UNIVERZITET U BEOGRADU

Vanja M. Korać

DIGITALNA FORENZIKA U FUNKCIJI ZAŠTITE INFORMACIONOG SISTEMA BAZIRANOG NA LINUX I WINDOWS PLATFORMAMA

doktorska disertacija

Beograd, 2014.

УНИВЕРЗИТЕТ У БЕОГРАДУ

Вања М. Кораћ

ДИГИТАЛНА ФОРЕНЗИКА У ФУНКЦИЈИ ЗАШТИТЕ ИНФОРМАЦИОНОГ СИСТЕМА БАЗИРАНОГ НА LINUX И WINDOWS ПЛАТФОРМАМА

докторска дисертација

Београд, 2014.

UNIVERSITY OF BELGRADE

Vanja M. Korać

DIGITAL FORENSIC IN SECURITY OF INFORMATION SYSTEM BASED ON LINUX AND WINDOWS PLATFORMS

PhD thesis

Belgrade, 2014.

Komisija:

_____

(prof. dr. Žarko Mijajlović, redovni profesor, PMF, Univerzitet u Beogradu – mentor)

_____

(dr. Miodrag Mihaljević, naučni savetnik, Matematički institut SANU, Beograd – mentor)

_____

(dr. Dragan Prlja, naučni saradnik, Institut za uporedno pravo, Beograd - predsednik)

_____

(prof. dr. Stevan Lilić, redovni profesor, Pravni fakultet, Univerzitet u Beogradu)

_____

(dr. Zoran Ognjanović, naučni savetnik, Matematički institut SANU, Beograd)

_____

(prof. dr Dejan Vučković, RGF, docent, Univerzitet u Beogradu)

_____

(datum odbrane)

ZAHVALNICA

Želeo bih da izrazim duboku zahvalnost profesorima dr Gojku Gruboru i dr Draganu Prlji, za njihovo vođstvo, podršku, stručnu pomoć i angažovanje tokom čitavog rada. Posebno se zahvaljujem prof dr Žarku Mijajloviću, dr Miodragu Mihaljeviću i dr Zoranu Ognjanoviću, na ukazanom poverenju, razumevanju i dragocenoj pomoći u "brušenju" i "poliranju teze", kao i za pronicljive sugestije, komentare i korisna rešenja koja su mi pomogla u usmeravanju istraživanja i pisanja ove disertacije.

Specijalnu zahvalnost dugujem dragom prijatelju i kolegi Zoranu Davidovcu, bez čije dragocene pomoći sprovođenje eksperimentalnog dela i obrada rezultata iz oblasti ispitivanja ranjivosti računarskih sistema, ne bi bilo moguće.

Veliku zahvalnost dugujem prof. dr Milanu Milosavljeviću, jer su mi njegova objašnjenja otvorila vrata fascinantnog sveta digitalne forenzike.

Izuzetnu zahvalnost bih uputio profesorima dr Stevanu Liliću i dr Dejanu Vučkoviću, za prihvatanje učešća u Komisiji za ocenu i odbranu doktorske disertacije. Članovi komisije za ocenu i odbranu doktorske disertacije, mnogo su mi pomogli u svim fazama izrade ove teze, kako korisnim savetima, tako i u komentarisanju pojedinih rezultata.

Tokom čitavog procesa izrade disertacije, imao sam podršku kolektiva Matematičkog instituta SANU u Beogradu, u kome sam zaposlen, a naročito podršku direktora Instituta, dr Zorana Markovića.

Svojoj porodici i prijateljima dugujem bezgraničnu zahvalnost za njihovu svesrdnu podršku koju su mi pružali sve vreme tokom rada na ovoj tezi, kao i ohrabrenje pri važnim životnim odlukama u profesionalnom i privatnom segmentu života. Njihovo znanje i iskustvo, pomoć, pažnja, i strpljenje bez izuzetka, su značajno doprineli mom usavršavanju.

Beograd, 7. april, 2014.

Naslov. Digitalna forenzika u funkciji zaštite informacionog sistema baziranog na Linux i Windows platformama

Rezime. Digitalna forenzika je multidisciplinarna nauka koja podrazumeva spoj razlicitih naučnih disciplina (računarske nauke, pravo, kriminologija) sa brojnim izazovima u uslovima masovnog generisanja digitalnih podataka (*Big Data*), virtuelizacije klijentske i serverske strane (*Cloud Computng*), neusaglašenosti standardizacionih tela i opšteg nedostatka brojnih standarda i eksperata u svim disciplinama. Kako se digitalna forenzika odnosi na sve digitalne uređaje, uža naučna oblast uključuje brojne aplikacije digitalne forenzike, kao što su računarska forenzika, forenzika mobilnih uređaja, forenzika na sistemima savremenih automobila, senzorskih mreža itd. U ovom radu je analizirana i primenjena uža naučna oblast računarske forenzike. Opisana je digitalna forenzika računarskih sistema baziranih na Windows i Linux platformi, sa fokusom na određena mesta u implementiranom sistemu proaktivne digitalne forenzike koja mogu ukazati na forenzički relevantne događaje kritične za bezbednost sistema. Opisane su brojne metodologije, tehnologije i tehnike istrage visokotehnološkog kriminala. Proces prikupljanja podataka i digitalne forenzičke analize „uživo“, detaljno je razmatran. Izvršena je kratka revizija karakteristika i tipično zahtevanih funkcionalnosti softverskih forenzičkih alata, za inicijalni odgovor i oporavak podataka i particija magnetnih diskova. Opisani su i najvažniji digitalni forenzički kompleti alata i njihove osnovne funkcionalnosti. U radu se ističu i najznačajniji elementi kojima treba posvetiti posebnu pažnju prilikom digitalne forenzičke analize u virtuelnom okruženju. Takođe su objašnjeni i najvažniji segmenti samog virtuelnog okruženja i način na koji oni mogu biti značajni alati, za postupak digitalne forenzičke analize. U poslednjem delu ovog rada, fokus je usmeren na ranjivosti Windows i Linux platformi sa prikazanim načinima zlonamernog proboja sistema. Opisane su opšte ranjivosti i specifične ranjivosti koje se odnose samo na Windows, odnosno samo na Linux platforme. Takođe, navedeni su i najčešći načini zlonamernog iskorišćavanja sistema. Ranjivosti računarskih sistema i mreža mogu se odnositi na programe, hardver, konfiguraciju i ljude. Isključujući ljude kao najznačajniji i istovremeno najkritičniji faktor u zaštiti informacija, programske ranjivosti se tipično koriste za *online* direktne napade, ili napade malicioznim programima. Otkrivanje i otklanjanje ranjivosti sistemskih programa je jedan od glavnih ciljeva digitalne forenzike. Pored skupljanja forenzički relevantnih digitalnih podataka i izgradnje čvrstih digitalnih dokaza o kompjuterskom incidentu ili kriminalu za potrebe pravosudnog sistema, cilj digitalne forenzičke analize je da se iskorišćene ranjivosti trajno otklone i da se incident/protivpravna aktivnost takve vrste više nikada ne ponovi. U tom smislu je doprinos ovog rada veoma značajan. Praktičan primer ispitivanja ranjivosti servisa na Windows i Linux platformama obuhvatio je 80 operativnih sistema. Od tog broja, 51 se odnosi na Windows operativne sisteme, a 29 na Linux operativne sisteme. Dobijeni rezultati su rezultat dvogodišnjeg istraživanja, jer je ispitivanje sistema vršeno u 2011. i 2013. godini. Kroz skeniranje i prikaz ranjivosti difoltno instaliranih Windows i Linux sistema preventivno se otkrivaju ranjivosti koje potencijalno mogu biti iskorišćene od strane bezbednosnih pretnji (maliciozni programi ili zlonamerni napadači) i time ugroziti računarske sisteme i informacije. Proaktivnim otklanjanjem ovih ranjivosti realizuje se preventivna zaštita. Uspostavljanjem sistema proaktivne forenzike, obezbeđuje se logovanje forenzički relevantnih događaja, tj. tragova pokušaja napada u realnom vremenu, čime se bitno olakšava forenzička istraga u slučaju incidenta ili protivpravne aktivnosti.

Ključne reči : Zaštita sistema, ispitivanje ranjivosti, visokotehnološki kriminal, digitalna forenzika, forenzički alati, forenzička analiza „uživo“

Naučna oblast : Digitalna forenzika

Uža naučna oblast : Računarska forenzika

UDK broj :

Title. Digital forensic in security of information system based on Linux and Windows platforms

Abstract. Digital forensics is a multidisciplinary science which includes different scientific disciplines (computer scineces, law, criminology) with numerous challenges in conditions of digital data mass generating (*Big Data*), clients and servers virtualisation (*Cloud Computng*), incompatibility of standardizing bodies and general lack of numerous standards and experts in all of the disciplines. Since digital forensics applies to all of the digital devices, a focused scientific field includes numerous applications of digital forensics, like computer forensics, mobile devices forensics, forensics on modern cars systems, sensor networks etc. The focused scientific field of computer forensics was analyzed and applied in this paper. Digital forensics of computer systems based on Windows and Linux platforms was described, focused on certain points within the implementing system of proactive digital forensics, which can indicate forensically relevant data critical for system's security. Numerous methodologies, technologies and techniques of investigating cyber crime are described. The process of collecting data and "live" digital forensic analyses were considered in detail. A short revision of features was made, as well as of typical demanded functionality of software fonensic tools for an initial answer and recovery of data and partitions of magnetic discs. The most important sets of digital forensic tools and their basic functionalities were also descibed. In the paper, most important elements were listed which need special attention while performing digital forensic analysis in a virtual environment. The most important segments of virtual environment itself were also explained, as well as ways in which they can represent important tools for performing digital forensis analysis. The last chapter of this paper is focused on vulnerabilities of Windows and Linux platforms, with listed ways of malicious system intrusion. General and specific vulnerabilities were described regarding only Windows or only Linux platforms. The most common ways of malicious system abuse were also listed. Computer systems vulnerabilities can be applied on programs, hardware, configuration and staff. Disregarding staff as the most important, but at the same time the most critical factor in protecting information, program vulnerabilities are typically used for *online* direct attacks or attacks with malicious programs. Detecting and removing vulnerabilities of system programs is one of the digital forensics main goals. Beside collecting forensically relevant digital data and constructing strong digital evidence about computer incident or criminal for the purposes of law, the goal of digital forensic anlysis is to permanently remove abused vulnerabilities and to prevent incidents/illegal actions from repeating. In this sense, this paper is of utmost importance. A practical example of investigating system vulnerabilities on Windows and Linux platforms included 80 operating systems. Out of that, 51 regards Windows operating systems and 29 of them Linux operating systems. The obtained results derive from a two-year research, since system scanning was performed in 2011 and 2013. Through scanning and displaying vulnerabilities of Windows and Linux systems installed by default, vulnerabilities which could potentially be used by security threats (malicious programs or malicious attacks) and potentially endanger computer systems and information, are precautionally removed. By proactive removing of these vulnerabilities, preventive protection is being performed. By establishing the system of proactive forensics, logging of forensically relevant events, i. e. clues for potential attacks within real time are being secured, making it much easier to perform forensic investigation in case of an incident or illegal action.

Key words : Security of systems, vulnerability scanning, cyber crime, digital forensic, forensic tool, live forensic

Science area : Digital forensics

Field of Academic Expertise : Computer forensics

UDC number :

SADRŽAJ

1. METODOLOGIJA ISTRAŽIVAČKOG PROJEKTA

1.1. UVODNE NAPOMENE I OBRAZLOŽENJE RADA

Sa pojavom računarskih mreža, njihovom ekspanzijom i integracijom u sistem globalne mreže - Interneta, dolazi do njene zloupotrebe u smislu narušavanja njene prvobitno osmišljene funkcije - prenos informacija i komunikacija. Tehnologija je, sa jedne strane, postala moćan alat, međutim ona može biti i zloupotrebljena jer je postala globalno dostupna, pa samim tim raste i broj potencijalnih rizika od napada sa Interneta. Internet je uvećao lakoću i brzinu kojom se sprovode protivpravne aktivnosti, uklanjajući fizička ograničenja i smanjujući fizički napor za prevaru. Protivpravne aktivnosti mogu biti izazvane najrazličitijim oblicima malicioznih programa ili direktnim napadom zlonamernog napadača.
Razlozi za pojavu ovih napada su različiti i generalno se mogu podeliti na materijalno i nematerijalno motivisane. Na prvom mestu razlog je sticanje finansijske dobiti. Kao drugi motivi za napade na računarske sisteme ističu se izazov, znatiželja, samopotrvđivanje, krađa podataka, špijunaža i drugi. Pod kompjuterskim kriminalom u najširem smislu podrazumevaju se krivična dela prema Krivičnom zakonu nacionalne države, u kojoj su na bilo koji način uključeni računarski sistemi i mreže [132]. Glavni cilj istrage visokotehnolškog kriminala je, kao i u slučaju klasičnog kriminala, izgraditi za pravosudne organe neoboriv, ili čvrst dokaz, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela [131]. Da bi se obezbedio takav dokaz, u slučaju visokotehnološkog kriminala, neophodno je, uz pomoć niza posrednih dokaza, pronaći informacije u digitalnom obliku koje imaju verodostojnu vrednost, a koja je uskladištena ili prenešena u takvom obliku. Takve informacije su digitalni dokazi.
Bilo da je reč o zvaničnoj ili korporativnoj istrazi, u toku prikupljanja, analize i prezentacije digitalnih dokaza moraju se poštovati određeni principi. Kada je reč o visokotehnološkom kriminalu najčešće se zahteva i svedočenje ili veštačenje eksperta.
U prvom i trećem delu drugog poglavlja, opisan je tok forenzičke istrage. Navedene su i opisane definicije koje se najčešće pojavljuju u vezi sa visokotehnološkim kriminalom, njihovim pojavnim oblicima i štetnim posledicama koje ostavljaju, da bi se ukazalo na izuzetan značaj digitalne forenzike računarskih sistema, baš zbog otkrivanja ovih krivičnih dela. Činjenično stanje je sledeće :

a. gotovo da ne postoji nijedna veća organizacija na svetu koja nije pretrpela kompromitovanje svojih sistema od strane napadača;
b. većina outsourced[1] (eng. outsourced) programa se pravi za backdoor-ovima[2], što može napadaču da omogući upad u sistem;
c. *firewalls*, sistemi za detekciju napada na sistem (eng. intrusion detection system - IDS) i antivirusi nisu rešili bezbednosne probleme;
d. postoji veliki broj umreženih računara (tzv. *botnet* mreža) namenjenih distribuciji nelegalnih sadržaja ili piraterije;
e. dok se ovaj rad piše postoje na stotine neobjavljenih exploita koji se upravo koriste;

Zato bavljenje digitalno forenzičkim procesima postaje nezaobilazna disciplina kada je reč o otkrivanju digitalnih protivpravnih aktivnosti i računarskih incidenata, kako sa aspekta zvanične istrage, tako i sa aspekta korporacijske istrage.

[1] Outsourced programi su programi koji se prave za ime i račun određene kompanije od strane neke druge kompanije.
[2] Backdoor ili zadnja vrata predstavlja metod zaobilaženje normalne autentifikacije, neprimećeno obezbeđivanje daljinskog pristupa računaru.

Drugi deo drugog poglavlja, detaljno opisuje pojedinačne metodologije odnosno modele sa kojim se definiše, oblikuje i standardizuje proces digitalne istrage. Određeni modeli koji su prikazani u radu prilaze digitalnoj istrazi sa naučno-tehničkog aspekta, a neki sa netehničkog aspekta. Takođe, neki od prikazanih modela su detaljniji u odnosu na druge po pitanju korespondencije fizičke i digitalne istrage, a opet kada je reč o istražnom procesu neki modeli imaju veći okvir u metodološkom smislu.

Cilj prikaza istražnih metoda, predstavlja presek trenutnog stanja istražnih metoda. Takođe, ovo može biti od pomoći istražiteljima jer na osnovu preseka stanja, mogu u skladu sa specifičnostima istrage, primeniti odgovarajući model. Nadalje opisane su prednosti i nedostaci obuhvaćenih modela.

Četvrti deo drugog poglavlja, posvećen je digitalnoj forenzici u virtuelnom okruženju. Opisani su najznačajniji elementi kojima treba posvetiti posebnu pažnju prilikom digitalno forenzičke analize u virtuelnom okruženju. Takođe su objašnjeni i najvažniji segmenti samog virtuelnog okruženja i na koji način oni mogu biti značajni za postupak digitalne forenzičke analize. U radu se razmatraju dva aspekta virtuelnog okruženja. Sa prvog aspekta posmatra se virtuelno okruženje kao digitalno mesto krivičnog dela. Drugi aspekt posmatra virtuelno okruženje kao okruženje za digitalno forenzičku analizu podataka.

U trećem poglavlju opisano je prikupljanje, analiza i očuvanje podataka na Windows i Linux platformama na "živom" sistemu, sa ciljem utvrđivanja da li postoji određena incidentna/protivpravna aktivnost. S obzirom na izuzetan značaj prikupljenih podataka u forenzičkoj istrazi u radu su opisani alati i načini prikupljanja podataka od značaja kako onih sa privremenim karakterom (eng. volatile data) tako i postojanih podataka od značaja. S obzirom da forenzička praksa zahteva da forenzičar raspolaže setom raznovrsnih alata za određene namene, ali i specificnim namenskim alatima koji su generalno bolji za rešavanje namenskih zadataka, ovo poglavlje posvećuje tome posebnu pažnju. U tom smislu, opisani su najznačajniji programski forenzički alati za inicijalni odgovor, alati za oporavak podataka i particija kao i digitalno forenzički kompleti alata namenjenih za Windows i Linux sisteme. Na kraju ovog poglavlja, dat je prikaz trendova u razvoju odgovora na protivpravne aktivnosti i primećenih nedostataka u vezi sa forenzičkim odgovorom „uživo“.

Četvrto poglavlje posvećeno je ispitivanju ranjivosti na Windows i Linux platformama. Opisane su opšte ranjivosti i ranjivosti koje se odnose samo na Windows odnosno samo na Linux platforme. Takođe, navedeni su i najčešći načini zlonamernog iskorišćavanja sistema. U praktičnom primeru izvršeno je ispitivanje ranjivosti servisa na Windows i Linux platformama.

1.2. PREDMET ISTRAŽIVANJA

U ovom projektnom zadatku predmet istraživanja je digitalna forenzika računarskih sistema baziranih na Windows i Linux platformi, sa fokusom na određena mesta u implementiranom sistemu proaktivne digitalne forenzike koja mogu ukazati na forenzički relevantne događaje kritične za bezbednost sistema. Opisan je proces prikupljanja podataka i digitalne forenzičke analize „uživo“ i izvršena je kratka revizija karakteristika i tipično zahtevanih funkcionalnosti softverskih forenzičkih alata za inicijalni odgovor i oporavak podataka i particija. Opisani su i najvažniji digitalno forenzički kompleti alata i njihove osnovne funkcionalnosti. U poslednjem poglavlju fokus je usmeren na ranjivosti Windows i Linux platformi sa prikazanim načinima zlonamernog iskorišćavanja sistema iz forenzičke prakse. Praktičan primer ispitivanja ranjivosti servisa na Windows i Linux platformama obuhvatio je 80 operativnih sistema. Od tog broja 51 se odnosi na Windows operativne

sisteme a 29 na Linux operativne sisteme. Dobijeni rezultati su rezultat dvogodišnjeg istraživanja jer je ispitivanje sistema vršeno u 2011. godini i 2013. godini.

1.3. CILJEVI I ZADACI ISTRAŽIVANJA

Naučni cilj ovog projekta jeste praktična verifikacija efekata implementacije digitalne forenzike u sistem zaštite informacione imovine organizacija. Teoretski su poznate koristi od primene forenzičkih znanja, tehnika i alata u otkrivanju uzroka, a ne samo posledica, napada na računarske mreže i sisteme i trajno sprečavanje ponavljanja istog ili sličnog napada. Ovaj istraživački rad, kroz analizu ranjivosti operativnih sistema i implementaciju infrastrukture proaktivne digitalne forenzike, obezbeđuje potrebne smernice za preventivnu zaštitu informacione imovine organizacija.

Glavni cilj ovog istraživačkog projekta je opisati metode prikupljanja, kako onih podataka koji utiču na bezbednosnost sistema tako i forenzički relevantnih podataka, u realnom vremenu ("uživo") sa Windows i Linux sistema sa tačno određenih sistemskih mesta, na kojima se mogu pronaći potencijalni dokazi povrede sistema bezbednosti, ili incidentne odnosno protivpravne aktivnosti.

Poseban cilj ovog rada je da se detaljnije i sveobuhvatno prikaže stanje iz oblasti metoda i tehnika digitalne forenzike računarskih sistema koje otkrivaju ovakvu vrstu kriminala i preventivno deluju kao vid zaštite računarskih sistema. U praktičnom primeru biće prikazana analiza ranjivosti Linux i Windows operativnih sistema sa alatom Rapid 7 Nexpose, na osnovu servisa koji ovi sistemi sadrže. Ova analiza je obuhvatila gotovo sve najbitnije Linux i Windows platforme čiji je broj 80 (51 Windows operativnih sistema i 29 Linux operativnih sistema).

Zadatak ove analize treba da pokaže stanje sistema, tj. koliko je sistem ranjiv posle njegove instalacije na računaru. Na taj način detektovane su ranjivosti na sistemu, i predložene su mere za prevazilaženje ovih bezbednosnih problema, čime se preventivno deluje protiv mogućeg forenzički relevatnog događaja. U tom smislu, ovo sveobuhvatno istraživanje se može posmatrati i kao jedna proaktivna digitalna forenzika u smislu spremnog dočekivanja, ali i otkrivanja forenzički relevatnog događaja.

1.4. OKVIR ISTRAŽIVAČKE HIPOTEZE

Opšta hipoteza:

Istraživanje incidentnih/protivpravnih aktivnosti podrazumeva prikupljanje digitalnih podataka (potencijalnih dokaza) sa računarskih sistema i mrežnih uređaja utvrđivanje autentičnosti i njihovu analizu. Pre svake istrage podrazumeva se ispitivanje potrebnih preduslova kao što su: postojanje dovoljnog broja obučenih profesionalaca, forenzičke radne stanice i forenzičke laboratorije za oporavak podataka, saradnja sa javnim tužilaštvom i definisana metodologija. U zavisnosti od tipa istrage (zvanična ili korporativna) zavisi i ko će dati prvi odgovor na incidentnu/protivpravnu aktivnost. Koliku važnost ima forenzički odgovor i koliko je on osetljiv, možda najslikovitije prikazuje opis o potrazi za digitalnim podacima koji je dao Fridman u sledećim rečenicama svoje knjige[3] :
"*Svi podaci ostavljaju trag. Potraga za podacima ostavlja trag. Brisanje podataka ostavlja trag. Odsustvo podataka pod određenim okolnostima može da ostavi najjasniji trag od svih.*"

[3]C.S.Friedman, This Alien Shore, DAW BOOKS, INC, New York 1998, dostupno na http://rose.digitalmidnight.org/temp/books/CS_Friedman/C.%20S.%20Friedman%20-%20This%20Alien%20Shore.pdf

Prema tome, digitalni podaci generisani ili uneti u računar ostavljaju brojne tragove u operativnim sistemima. Pretraga za podacima podrazumeva priključivanje forenzičkog alata, što znači ostavljanje tragova na digitalne podatke (Lokardov zakon). Izbrisani podaci ostavljaju tragove u nealociranim i slek prostorima diska, a odsustvo podataka ukazuje na antiforenzičku aktivnost i predstavlja jaku osnovu za sumnju u protivpravne aktivnosti. Virusi na primer ostavljaju svoj kod u zaraženim programima. Tragovi kompromitovanja mogu biti prisutni u različitim oblicima na primer u izvornim fajlovima programskog jezika, u objektnim fajlovima (eng. Object files), u izvršnim kodovima, u šel skriptama, u izmenama nad postojećim programima ili čak u tekstualnim fajlovima pisanim od strane napadača. Za istragu je vrlo značajno ukoliko bi se ovi delovi informacija mogli iskoristiti za utvrđivanje izvora napada [180]. Prikupljanje podataka može da podrazumeva prikupljanje podataka iz živog sistema (eng. live) da bi se sakupile osetljive tj. nestabilne informacije ili se vrši post-mortem prikupljanje podataka bez izmene ili oštećenja i u tom slučaju se vrši preuzimanje fizičkih dokaza (kao na primer hard diskovi, diskete ili drugi mediji). Nakon preuzimanja fizičkih dokaza vrše se forenzička dupliranja – uzimanje softerskog imidža ili kloniranje diska računarskih dokaza i utvrđuje se autentičnost između originalnog digitalnog dokaza sa forenzičkom kopijom. Post-mortem analiza ili kako se još u literaturi naziva statička analiza ima određena ograničenja jer ne može da pruži potpunu sliku događaja. U novijim radovima opisuju se glavni ograničavajući faktori post-mortem analize [83]. Paralelno se vrši istraživanje i nadzor mreže za dobijanje dodatnih informacija. Pored toga, za dobijanje dodatnih informacija vrše se i intervjui sa odgovarajućim ljudima koji imaju određene detalje u vezi sa incidentnom odnosno protivpravnom aktivnošću .

Alternativa post-mortem analizi jeste analiza uživo. U ovom slučaju digitalni dokazi se prikupljaju dok sistem radi. Kada se podaci prikupljaju iz "živog" operativnog sistema važno je znati koji su podaci lako promenljivi tj. podaci privremenog karaktera (eng. volatile), a koji podaci su postojanog karaktera (eng. non-volatile). Na prvom mestu "lako izmenljivi" podaci odnosno volatile podaci, su sistemski detalji koji istražiteljima pružaju uvid u način i prirodu kompromitovanja sistema i nekada mogu biti podaci od krucijalnog značaja. Od podataka koji neće lako biti izmenjeni na sistemu, na prvom mestu su oni koji daju informacije o statusu, setovanjima, konfiguraciji sistema i istorijske informacije na osnovu kojih se mogu utvrditi način i priroda kompromitovanja sistema. U skladu sa navedenim ciljem forenzičkog odgovora, ovaj rad će biti orijentisan ka prikupljanju podataka "uživo " sa Windows i Linux sistema, sa određenih mesta na sistemu koji mogu ukazati na one forenzičke relevantne događaje koji utiču na bezbednost sistema. Prikupljanje podataka, kao što je pomenuto podrazumeva prikupljanje podataka sa računarskih sistema i prikupljanje podataka sa mreže. S obzirom da je fokus ovog rada usmeren ka računarskim sistemima baziranim na Windows i Linux platformama, biće prikazani alati i tehnike za prikupljanje dokaza sa pomenutih računarskih sistema (eng. host based evidence). Prikupljanje dokaza sa mreže i sa mrežnih uređaja (eng. network based evidence) nisu predmet ovog rada.

Treba napomenuti, da ono na šta forenzički odgovor "uživo" ne može dati adekvatne rezultate, ali može dati dobru predstavu o onom šta se desilo, dodatne analize moguće je uraditi sa mrežnom forenzikom, a kasnije forenzičkom duplikacijom, post-mortem analizom (analiza fajlova: dumpa memorije, slika, audio video fajlova, arhiva i dokumenta), post-mortem analizom uz pomoć virtuelnog okruženja [16] [134], što izlazi iz okvira ovog rada.

Radna hipoteza:

Skeniranjem ranjivosti Windows i Linux operativnih sistema u eksperimentalnom delu istraživačkog rada istovremeno se otkrivaju ranjivosti koje mogu ugroziti bezbednost sistema i omogućava se izbor adekvatnih mera zaštite, tako da se te ranjivosti više ne mogu iskoristiti za napade na sisteme. Kroz skeniranje i prikaz ranjivosti difoltno instaliranih

Windows i Linux sistema [poglavlje 4.] preventivno se otkrivaju ranjivosti koje potencijalno mogu biti iskorišćene od strane bezbednosnih pretnji (maliciozni programi ili hakeri), a time ugroziti računarske sisteme i informacije. Na taj način realizuje se preventivna zaštita. Zaštita sistema upravo obuhvata prevenciju sa detekcijom i odgovorom na incidentnu/protivpravnu aktivnost. Prevencija podrazumeva procenu rizika, kontrolu pristupa, šifrovanje i fajervole, dok odgovor na incident podrazumeva detekciju upada i rukovođenje protivpravnim aktivnostima od strane forenzičara. U tom smislu, ovaj rad opisuje komplementarnost digitalne forenzike, proaktivne digitalne forenzike, prvog odgovora na incident i oblasti zaštite operativnog sistema. Rezultati istraživanja proistekli iz ovog rada, mogu bitno uticati na smanjenje vremena potrebnog za realizovanje kompleksnih zadataka zaštite.

1.5. METODI ISTRAŽIVANJA I TOK ISTRAŽIVAČKOG PROCESA

U radu je primenjena osnovna metodologija prirodnih nauka - eksperimentalna metodologija primenjena u istraživačkom procesu kroz *istraživanje* i *prezentaciju rezultata istraživanja*. U toku istraživačkog procesa primenjene su četiri faze: *postavljanje problema, formulisanje hipoteze, proveravanje hipoteze i potvrđivanje (verifikacija) hipoteze*.

U prvom delu istraživačkog rada primenjen je *desk* metod istraživanja literaturnih podataka o digitalnoj forenzičkoj istrazi, akviziciji i analizi, sa posebnim osvrtom na forenzički odgovor "uživo" na Windows i Linux platformama. Opisane su lokacije potencijalnih dokaza forenzički relevantnih događaja koji utiču na bezbednost sistema i koji mogu potvrditi ili osporiti postojanje incidentne ili protivpravne aktivnosti. Detaljno su opisani forenzički alati komandne linije, zatvorenog i otvorenog programskog koda sa kojima je moguće prikupljanje potencijalnih dokaza i njihova analiza. Zatim su primenjeni metodi *sinteze i generalizacije*, kao i osnovni logički metodi *indukcije i dedukcije*, te *analitičko-deskriptivni metod* istraživanja funkcionalnosti forenzičkih alata.

U eksperimentalnom delu rada primenjen je eksperimentalni metod verifikacije ranjivosti operativnih Windows i Linux sistema na kontrolisanom slučaju i predložene su korektivne mere. Izvršeno je skeniranje i analiza ranjivosti Linux i Windows operativnih sistema sa alatom "Rapid 7 Nexpose" na osnovu servisa koji ovi sistemi sadrže. Stvoreni su određeni laboratorijski uslovi za potrebe istraživanja koje je realizovano u sklopu "Vmware ESX" 5.1.0 platforme, "IBM x3650 M3" servera i "EMC VNX5300" sistema. Na taj način ostvarena je centralizovana konsolidacija svih virtuelnih računarskih sistema namenjenih ispitivanju. Time je obezbeđena stabilna platforma za efikasno ispitivanje ranjivosti uz visok nivo sigurnosti. Ova analiza je obuhvatila gotovo sve najbitnije Linux i Windows platforme čiji je broj 80 (51 Windows operativnih sistema i 29 Linux operativnih sistema). Zadatak ove analize treba da pokaže stanje sistema, tj. koliko je sistem ranjiv posle njegove instalacije na računaru. Na taj način detektovane su ranjivosti na sistemu i predložene su mere za prevazilaženje ovih bezbedonosnih problema. Rezultati istraživanja su beleženi i prezentovani u posebnom Prilogu na CD-u tabelarno, radi veće preglednosti.

2. VISOKOTEHNOLOŠKI KRIMINAL I DIGITALNA FORENZIKA

2.1 UVOD

Od pojave prvih digitalnih računara pa do danas prošlo je skoro 60 godina. Iako skromni po mogućnostima, a veliki po gabaritima, oni su na samom početku bili namenjeni da olakšaju i ubrzaju kompleksne proračune iz naučnih i tehničkih oblasti, kao i da obrađuju velike količine podataka kako u poslovnom tako i na administrativnom polju.

Pojava savremenih računara, široka rasprostranjenost i velike količine najrazličitijih korisničkih programa, uticala je na promene života ljudi širom sveta. Ova tehnologija nam pruža ogromne mogućnosti i u velikoj meri olakšava naše živote. Današnji računari koji postaju sve manji a istovremeno „snažniji" nalaze primenu gotovo u svim naučnim oblastima od planiranja, prikupljanja, proračuna i obrade podataka do analize i projektovanja procesa i vrednovanja istog. Na primer u računarskoj grafici, nastavi, obrazovanju, saobraćaju, komunikaciji, informisanju, edukaciji, umetnosti zabavi, upravljanju uređajima, bezbednosti veštačkoj inteligenciji itd. Međutim, mora se razumeti da savremena tehnologija sa sobom donosi i mnogo rizika.

Paralelno sa ovakvim razvojem računara razvile su se i računarske mreže, od kojih je najpoznatija tzv. svetska mreža – Internet. Nastanak računarstva, i njihovo međusobno umrežavanje i stvaranje jednog informacionog i globalnog okruženja, vezuje se za jednu sjajnu i pozitivnu ideju koja se odnosi na međusobnu komunikaciju na svetskom nivou. Kolika je upotreba Interneta u svetu (na dan 30. Juna 2012. godine[4]) možda najbolje odslikava sledeća tabela (Tabela 1.):

Tabela 1: Statistika upotrebe Interneta na svetskom nivou u odnosu na populaciju iz Juna 2012. godine

Svetski regioni	**Populacija (2012 Est.)**	**Internet korisnici Dec. 31, 2000**	**Internet Korisnici** Poslednji podaci	**Penetration (% Populacija)**	**Rast 2000-2012**	**Korisnici %** prema tabeli
Afrika	1,073,380,925	4,514,400	167,335,676	15.6 %	3,606.7 %	7.0 %
Azija	3,922,066,987	114,304,000	1,076,681,059	27.5 %	841.9 %	44.8 %
Evropa	820,918,446	105,096,093	518,512,109	63.2 %	393.4 %	21.5 %
Middle East	223,608,203	3,284,800	90,000,455	40.2 %	2,639.9 %	3.7 %
Severna Amerika	348,280,154	108,096,800	273,785,413	78.6 %	153.3 %	11.4 %
Latinska Amerika / Karibi	593,688,638	18,068,919	254,915,745	42.9 %	1,310.8 %	10.6 %
Okeania / Australija	35,903,569	7,620,480	24,287,919	67.6 %	218.7 %	1.0 %

[4] Statistika upotrebe interneta u odnosu na svetsku populaciju odnosi se na 30. jun, 2012. Demografska populacija bazirana je na osnovu podataka od strane US Census Bureau (http://www.census.gov). Informacije o upotrebi Interneta publikovane su od strane Nielsen Online (http://www.nielsen.com/us/en.html), International Telecommunications Union (http://www.itu.int/en/Pages/default.aspx), GfK (http://www.gfk.com/Pages/default.aspx).

SVET UKUPNO	**7,017,846,922**	**360,985,492**	**2,405,518,376**	**34.3 %**	**566.4 %**	**100.0 %**

Izvor : InternetWorldStats - http://www.internetworldstats.com/stats.htm, statistika je bazirana na osnovu obuhvaćenih **2,405,518,376 Internet korisnika.** Copyright © 2001 - 2013, Miniwatts Marketing Group

S obzirom da novu tehnologiju koristi **2,405,518,376** (podatak iz tabele 1.) mora se razumeti da ona sa sobom donosi i mnogo rizika. Tehnologija sa jedne strane, može postati moćno oružje u našim rukama, međutim isto tako ono može biti usmereno i protiv nas jer je postala globalno dostupna. Nažalost, možemo da konstatujemo da je ovakav tehnološki progres pratilo i razvijanje ideje o korišćenju novih tehnologija u protivpravne svrhe [151]. Internet je uvećao lakoću i brzinu kojom se sprovode kriminalne radnje, uklanjajući fizička ograničenja i smanjujući fizički napor da bi se neko prevario. Na primer iz banke mogu biti ukradene milijarde dolara u "online" okruženju za nekoliko minuta, za razliku od vremena pre pojave Interneta kada su razbojnici fizički pljačkali banke i bili ograničeni i vremenom i količinom novca koji mogu da iznesu van banke, uz ogromnu količinu utrošene fizičke energije.

Za razliku od prvih računara koji su bili izolovani od uticaja ostalih računara, nakon početka njihove masovnije proizvodnje osmišljene su računarske mreže i to u vrlo kratkom vremenskom periodu, sa ciljem da bi se podaci, koji se nalaze na različitim računarima, mogli deliti (eng. share) i distribuirati pojedinim ili svim korisnicima određene mreže. Danas se primeri ovakvih mreža mogu naći praktično u svakoj organizaciji čiji zaposleni koriste računare u svom poslu, umrežene u jedinstveni sistem radi lakše i brže međusobne komunikacije. Nažalost, takav sistem je dvostruko ranjiv – kako spolja tako i iznutra.
Fantastičnim razvojem informaciono-komunikacionih tehnologija (u daljem tekstu IKT) i računarskih mreža, već sedamdesetih godina prošlog veka dolazi do pojave visokotehnološkog kriminala.

Globalnom ekspanzijom korisnika Interneta [5] (31. Decembra 2000 godine je bilo 360,985,492 korisnika a 31.marta 2011 taj broj je 2,095,006,005) čiji se godišnji rast meri geometrijskom progresijom [6] imalo je za posledicu i globalni talas krivičnih dela koja su povezana sa računarskim tehnologijama.

Visokotehnološki kriminal je tako postao svakodnevnica, a razvoj tehnologija je uslovio i neverovatnu diferencijaciju vrsta nedozvoljenih dela koja se mogu izvršiti njihovim korišćenjem od onih naivnih i bezopasnih koja se uglavnom vezuju za reklamiranje različitih proizvoda, do veoma opasnih ponašanja koja spadaju među teška (ponekad čak i najteža) krivična dela u mnogim nacionalnim zakonodavstvima [151]. U stvari on podrazumeva korišćenje Interneta, računara, mreža i srodnih tehnologija u izvršenju krivičnog dela uključujući kako tehnološki specifična krivična dela, tako i tradicionalna krivična dela uz pomoć IKT. U otkrivanju i sankcionisanju visokotehnološkog kriminala, digitalna forenzika je nezamenljiv alat. Ova teza je usmerena na digitalnu forenziku informacionih sistema baziranih na Windows i Linux platformama. S obzirom da je informacioni sistem izuzetno širok pojam i da bi se izbegla greška njegovog poistovećivanja sa računarskim sistemom, naslov teze je upravo suzio ovaj pojam ograničavajući se na računarske sisteme pod Windows i Linux operativnim sistemom kao podskupom informacionog sistema. U daljem tekstu biće navedene i definicije koje se najčešće pojavljuju u vezi sa visokotehnološkim kriminalom, njihovim pojavnim oblicima i štetnim posledicama koje ostavljaju, da bi se ukazao na izuzetan značaj digitalne forenzike računarskih sistema baš zbog otkrivanja ovih krivičnih dela. Činjenično stanje je sledeće :

[5] Izvor: http://www.internetworldstats.com/stats.htm , pristup 16.11.2011

[6] Broj redovnih korisnika Interneta je u 2009. godini premašio jednu milijardu, a u Srbiji dva miliona. Izvor: Dragan Prlja, Mario Reljanovic Pravna informatika

a. gotovo da ne postoji nijedna veća organizacija na svetu koja nije pretrpela kompromitovanje svojih sistema od strane napadača;
b. većina outsourced[7] (eng. outsourced) programa se pravi za backdoor-ovima[8], što može napadaču da omogući upad u sistem;
c. firewall-i, sistemi za detekciju napada na sistem (eng. intrusion detection system - IDS) i antivirusi nisu rešili bezbednosne probleme;
d. postoji veliki broj računara namenjenih distribuciji nelegalnih sadržaja ili služi za distribuciju piraterije;
e. dok se ovaj rad piše postoje na stotine ne objavljenih exploita koji se upravo koriste;

Zato bavljenje digitalno forenzičkim procesima postaje nezaobilazna disciplina kada je reč o otkrivanju digitalnih protivpravnih aktivnosti i računarskih incidenata, kako sa aspekta zvanične istrage, tako i sa aspekta korporacijske istrage.
Kao krajnji cilj ovog rada je da se pruži prikaz stanja iz ove oblasti, da se baci svetlo na metode i tehnike digitalne forenzike računarskih sistema (jer je teza usmerena na računarske sisteme) koji otkrivaju ovakvu vrstu kriminala i preventivno deluju kao vid zaštite računarskih sistema. U praktičnom primeru biće prikazana analiza ranjivosti Linux i Windows operativnih sistema sa alatom Rapid 7 Nexpose na osnovu servisa koje ovi sistemi sadrže. Ova analiza je obuhvatila gotovo sve najbitnije Linux i Windows platforme čiji je broj 80 (51 Windows operativnih sistema i 29 Linux operativnih sistema). Ova analiza pokazuje stanje sistema, tj. koliko je sistem ranjiv posle njegove instalacije na računaru. Na taj način se detektuju ranjivosti na sistemu, dobijaju se preporuke za prevazilaženje ovih bezbednosnih problema, čime se preventivno deluje protiv mogućeg forenzički relevatnog događaja. Tako da se ovo sveobuhvatno istraživanje može posmatrati i kao jedna proaktivna digitalna forenzika u smislu spremnog dočekivanja, ali i otkrivanja forenzički relevatnog događaja.

2.1.1 Visokotehnološki kriminal-sajber kriminal-računarski kriminal

Sinonimi koje najčešće srećemo u literaturi povodom ove vrste kriminala su Internet kriminal, eKriminal, računarski kriminal, mrežni kriminal, tehnološki kriminal, informacioni kriminal, elektronski kriminal, digitalni kriminal i termin koji se koristi u našem zakonodavstvu visokotehnološki kriminal. Iako ne postoji zvanična i opšteprihvaćena definicija ovog pojma kriminaliteta, termin sajber kriminal je u literaturi dominantno zastupljen u Americi, a naše zakonodavstvo ga definiše kao visokotehnološki kriminal pa će se u daljem tekstu ova vrsta kriminala nazivati visokotehnološkim kriminalom.

S obzirom da ne postoji opšteprihvaćena definicija koja se vezuje za ovu vrstu kriminala u daljem tekstu bih izložio one definicije koje su najzastupljenije u svim relevatnim literaturama koja se bavi ovom oblašću.

Postavlja se pitanje, šta tačno znači visokotehnološki kriminal, ili sajber kriminal (američki naziv za ovu vrstu kriminala koji se odomaćio u mnogim svetskim jezicima) ? Jedinstveni odgovor na ovo pitanje još ne postoji, ali ono što je zajedničko za mnoge definicije koje određuju ovaj pojam, može se uočiti zajednički element – *korišćenje računara ili računarske mreže i Interneta*. U svetu istraživanja visokotehnološkog kriminala ovakvo usko tumačenje ovog termina nalazimo u velikom broju Internet enciklopedija i rečnika, pa je sajber kriminal definisan kao „kriminalna aktivnost počinjena korišćenjem računara i Interneta“.[9]

[7] Outsourced programi su programi koji se prave za ime i račun određene kompanije od strane neke druge kompanije.
[8] Backdoor ili zadnja vrata predstavlja metod zaobilaženje normalne autentifikacije, neprimećeno obezbeđivanje daljinskog pristupa računaru.
[9]Izvor: Internet adresa: http://www.techterms.com/definition/cybercrime, pristupano 21.11.2011.

Profesor dr Dragan Prlja, naučni saradnik Instituta za uporedno pravo, ističe da se u praksi može dogoditi da počinilac koristi mnogo drugih sredstava za izvršenje krivičnog dela, pa je očigledno da ovako uska definicija nikako ne zadovoljava sve potrebe percipiranja ove vrste kriminaliteta, koje je od velike važnosti za njihovo dalje suzbijanje. Identifikovati šta predstavlja krivično delo visokotehnološkog kriminala i kako se ono razlikuje od drugih vrsta nepoželjnog ponašanja koje nije uvek društveno opasno, osnovni je problem koji nijedna definicija još uvek nije uspela da prevaziđe. I pored velikih napora da se ovaj problem što jednostavnije, a opet što preciznije odredi, završava se identifikacijom sajber kriminala kao vršenje krivičnih dela upotrebom računara ili računarskih mreža.[10] Iako naizgled suviše jednostavna, ova definicija veoma dobro pokriva široko polje mogućeg kriminalnog delovanja. Ono što se uzima kao zamerka koncepcijske prirode, odnosi se na činjenicu da nisu samo računari moguća sredstva zloupotrebe novih tehnologija. Ukoliko se ona uopšti i ispravi tako da pod sajber kriminalom obuhvati i one protivpravne aktivnosti preduzete nekim drugim digitalnim uređajima i Internetom, ta bi definicija zbog svoje širine bila sveobuhvatna. Na ovaj način obuhvaćeno je sve od nelegalnog preuzimanja raznih vrsta muzičkih i video fajlova pa do velikih finansijskih zloupotreba sa on-line bankovnih računa. Ostala dela se moraju inkriminisati u okviru postojećih krivičnih dela, kao njihovi specifični oblici. Pri tome se mora voditi računa o činjenici da savremene tehnologije napreduju daleko brže od mogućnosti zakonodavca da vrši izmene krivičnog prava, kao i o činjenici da u mnogim od ovih oblasti ne postoje utvrđeni međunarodni standardi, niti nedvosmislena praksa [11].

Takođe izdvojio bih jednu najpotpuniju, mada možda ne i najprecizniju definiciju o kompleksnom pojmu sajber kriminala predstavljenu na UN-a sa Desetom kongresu Ujedinjenih Nacija, posvećenog Prevenciji od kriminala i tretmanu počinioca od aprila 2000. Godine [12]:

"*Sajber kriminal je kriminal koji se odnosi na bilo koji oblik kriminala koji se može izvršavati sa računarskim sistemima i mrežama, u računarskim sistemima i mrežama ili protiv računarskih sistema i mreža*"

To, zapravo, podrazumeva neku kriminalnu radnju koja angažuje računarski sistem ili mrežu kao sredstvo ili kao cilj izvršenja krivičnih dela ili koja se realizuje u elektronskom okruženju. Karakteristika sajber kriminala je ta, što je on učinjen sa namerom a ne slučajnošću.

U Konvenciji o sajber kriminalu (Convention on Cybecrime [13]) Saveta Evrope računarski sistem je definisan kao svaki uređaj ili grupa međusobno povezanih uređaja kojima se vrši automatizivana obrada podataka. To dalje implicira da bez istih i bez računarskih mreža nema ovog oblika kriminala.

Ovako predstavljen sajber kriminal pokriva veliki broj različitih kriminalnih aktivnosti uključujući napade na računarske podatke i računarske sisteme, napade vezane za računare, sadržaje ili intelektualnu svojinu pa se u literaturi najčešće navodi kao jedan opšti termin – kišobran (eng. umbrella) termin.

Dr. Gojko Grubor, profesor na katedri za Bezbednost i zaštitu informacionih sistema i profesor dr. Milan Milosavljević rukovodilac doktorskog programa Napredni sistemi zaštite na Univerzitetu Singidunum, u najširem smislu pod računarskim kriminalom podrazumevaju

---

Izvor Internet adresa: http://www.crime-research.org/analytics/702, pristupano 21.11.2011.

Izvor: Internet adresa: http://www.thefreedictionary.com/cybercrime, pristupano 21.11.2011.

Izvor: http://www.webopedia.com/TERM/C/cyber_crime.html, pristupano 21.11.2011.

Izvor: http://www.pcmag.com/encyclopedia_term/0,2542,t=cybercrime&i=40628,00.asp, 21.11.2011.

[10]Izvor: Internet adresa: http://www.webopedia.com/TERM/C/cyber_crime.html, 21.11.2011.

[11] Dragan Prlja, Mario Reljanović, Pravna informatika, Pravni fakultet Univerziteta Union u Beogradu, 2010, strana 54.

[12] Tumačenje i razmere ovog kriminala i njegove opasnosti opisane su u dokumentu *Kriminal vezan za kompjuterske mreže* (eng. *Crime related to computer networks*) Izvor: http://www.uncjin.org/Documents/congr10/10e.pdf, 10.12.2011

[13] http://conventions.coe.int/treaty/en/treaties/html/185.htm, 01.03.2012

krivična dela prema krivičnom zakonu nacionalne države, u koja su na bilo koji način uključeni računarski sistemi i mreže. U računarskom i kibernetičkom (sajber kriminal) kriminalu, računari se koriste kao predmet napada i krađe, izmene ili uništavanja podataka, kao alat za izvršavanje tradicionalnih oblika kriminala i za skladištenje kompromitujućeg materijala. Glavni cilj istrage računarskog kriminala je, da se kao i slučaju klasičnog kriminala, izgradi za pravosudne organe neoboriv ili čvrst dokaz krivice, i/ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Ključnu metodologiju istrage i dokazivanja računarskog kriminala obezbeđuje metodologija istrage klasičnog kriminala, sa specifičnostima istrage osetljivih, lako promenljivih i po svojoj prirodi posrednih digitalnih dokaza [132] [14] a najvažnije metodologije biće prikazane u narednim poglavljima.

Dr Linda Volonino profesor Informacionih sistema Canisius i predsednik FBI Infragard ISSA (Infomation system security association – udruženja za bezbednost informacionih sistema) definiše termin sajber kriminal, prema načinu izvršenja krivičnih dela koje uključuju računare, u dve kategorije [199][15]:

- **računar kao cilj** - računar ili podaci su meta ove vrste kriminala. Zločine protiv računara uključuju i napade na mrežama koje mogu da prouzrokuju obaranje mreže, kao na primer napadi crva, neovlašćen pristup računaru, ili zloupotreba informacionih sistema, računara, programa ili podataka. Najčešći primeri su virusi, crvi, trojanski konji, industrijske špijunaže, softverska piraterija, i hakovanja (zlonamerni upadi na računare)
- **računar kao sredstvo** – u ovom slučaju računar se koristi da bi se izvršila neka protivpravna aktivnost. Mnogi zločini počinjeni sa računarom su tradicionalni zločini, kao što su krađe, prevare, falsifikovanja, uhođenje ili distribucija dečije pornografije. Razlika je u tome, da su ovi tradicionalni zločini počinjeni koristeći informaciono komunikacione tehnologije. U novije vrste krivičnih dela koje spadaju u ovu kategoriju mogu se svrstati ugrožavanje e-maila, krađu identiteta, spam, fišing (eng. phishing) [16], farming (eng. pharming) [17] kao i sve aktivnosti planiranja, rukovođenja, izvršenja i prikrivanja protivpravnih aktivnosti. Fišing predstavlja najdrastičniji atak na privatnost ličnosti, jer se počinilac, nakon što je prevarom ili na drugi način došao do vitalnih podataka za preuzimanje nečijeg identiteta (Internet i druge šifre, brojevi platnih kartica, i sl.) predstavlja u njegovo ime, zaključuje poslove ili ostvaruje društvene kontakte [152].

[14]Milan Milosavljević, Gojko Grubor, Istraga kompjuterskog kriminala - metodološko tehnološke osnove, Singidunum 2009. Strana 4.

[15] Linda Volonino, Computer forensics principles and practices, Pearson Education, Inc Upper Saddle River, New Jersey, 2007 strana 6.

[16] Fišing na mreži predstavlja način prevare korisnika računara u cilju otkrivanja ličnih ili finansijskih informacija putem lažne e-poruke ili Web lokacije. Uobičajena phishing prevara na mreži počinje e-porukom koja izgleda kao zvanično obaveštenje iz pouzdanog izvora, kao što je banka, preduzeće koje se bavi kreditnim karticama ili ugledni prodavac na mreži. Primaoce e-poruka upućuje na lažnu Web lokaciju gde se od njih zahteva da unesu lične podatke, kao što su broj računa ili lozinka. Ove informacije se nakon toga obično koriste za krađu identiteta. Izvor : http://Windows.microsoft.com/sr-Latn-CS/Windows-vista/What-is-phishing, 02.03.2012

[17] Farming je isto što i fišing, predstavlja sistem krađe poverljivih informacija, brojeva računa ili kreditnih kartica koristeći se lažnim web sajtovima. Predstavlja sofisticiraniji vid prevare od phishinga. Razlikuje se po tome što kod pharminga nema 'mamca' na koji treba kliknuti (vec se realizuje samovoljnim odlaskom na web adresu). Dovoljno je da se otvori neki e-mail i na taj način će se računar zaraziti nekim zlonamernim programom (virus, trojanac, keylogger) koji će krasti informacije sa računara. Na primer ukoliko korisnik želi da ode na sajt svoje banke, instalirani zlonamerni program će korisnika redirektovati na lažni sajt (a da korisnik toga nije svestan) koji izgleda isto kao i sajt banke i ukoliko korisnik ne prepozna da je redirektovan na lažni sajt uneće sve svoje podatke. Kako funkcioniše farming ? Web sajtovi koriste imena domena kao svoje adrese na internetu, dok je njihova stvarna lokacija određena IP adresom. Kada korisnik unese ime domena u svom web pretraživaču, ime domena se preslikava u neku IP adresu putem DNS servera. Tada se web pretraživač povezuje na server sa tom IP adresom i prezuma podatke sa Web strane. Ukoliko je korisnik posetio određeni sajt, podaci o DNS ulazu se pamte u DNS kešu korisničkog računara tako da se ne mora ponovo pristupati DNS serveru svaki put ukoliko korisnik želi da poseti taj isti određeni sajt. Zlonamerni program (koji se instalirao putem e-maila zaraženog virusom) koji služi za farming, u stvari vrši izmenu DNS ulaza ili host fajla na korisničkom računaru i time se postiže automatsko prelikavanja određenog sajta u zlonamernu (farming) web adresu. Još veća opasnost je ukoliko se zaraze DNS serveri jer za posledicu može da se ima zlonamerno preusmeravanje velikog broja korisnika. Izvor : http://www.baguje.com/tag/pharming, 03.01.2012

To znači da računar može biti sredstvo ili cilj izvršenja ovih krivičnih dela, što podrazumeva da je na neki način ostvarena u krivičnopravnom smislu kažnjiva posledica, s tim što posledica može biti ispoljena na nosiocima IKT (računari, mreže i ostali digitalni uređaji). Međutim, računar može biti i posrednik u izvršavanju krivičnog dela sajber kriminal, na primer, u slučaju korupcije tuđeg računara i izvršenja krivičnog dela sa tog računara.

U vezi sa ovakvom kategorizacijom ove vrste kriminala postoji i definicija koja određuje sajber kriminal kao oblik kriminalnog ponašanja, kod koga se korišćenje računarske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela, ili se računar upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično-pravnom smislu relevantna posledica[18].

Naravno, sajber kriminal može biti u obe ove kategorije. Na primer, ako bi neko koristio računar da upadne u bazu podataka zdravstvene ustanove sa namerom promeni lek pacijentu ili da izmeni laboratorijske rezultate ili da prikrije medicinske greške, to predstavlja razlog za tužbu zbog zloupotrebe.

Odeljenje za pravosuđe SAD (DOJ The department of Justice) sajber kriminal definiše u širem smislu kao svako kršenje krivičnog zakona koji uključuju dobro poznavanje i korišćenje računarske tehnologije za njihovo izvršenje. Takođe potrebno je dobro poznavanje računarskih tehnologija kako bi se uspešno sprovela istraga i dalje procesuiranje takvih krivičnih dela.

Na osnovu svih navedenih definicija o sajber kriminalu može se uočiti da se u stvari sajber kriminal odnosi na bilo koji zločin koji je u vezi sa informaciono komunikacionim tehnologijama.

2.1.2 Tipovi visokotehnološkog kriminala

Kada se spomenu tipovi sajber kriminala (visokotehnološkog kriminala), onda se govori o aktivnostima na osnovu kojih je izvršen napad zajedno sa različitim oblicima tehničkih i informacionih pomagala. To mogu biti različiti hardverski uređaji ili softverska rešenje, koja napad mogu da olakšaju nanoseći štetu fizičkim ili pravnim licima.

Profesor na Franklin Pierce Centru za prava (nekadašnji naziv University of New Hampshire School of Law) Ronald Standler sajber kriminal prema obliku, odnosno vrsti krivičnog dela deli u tri kategorije [19]: 1. neautorizovano korišćenje računara, 2. stvaranje i distribucija štetnih računarskih programa, 3. uznemiravanje i uhođenje u sajber prostoru.

Računarski kriminal se može definisati kao što to definiše prof. dr Milan Škulić : „Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja, kod koga se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivično pravnom smislu relevantna posledica.“[20]

Prof. Dr Đorđe Ignjatović definiše kompjuterski kriminalitet u čijem je fokusu računarski sistem i glasi : "Kompjuterski kriminalitet predstavlja poseban vid inkriminisanih ponašanja kod kojih se računarski sistem (shvaćen kao jedinstvo hardvera i softvera) pojavljuje ili kao sredstvo izvršenja ili kao objekat krivičnog dela, ukoliko se deo na drugi način, ili prema drugom objektu, uopšte ne bi moglo izvršiti ili bi ono imalo bitno drugačije karakteristike[21]."

[18] Dragan Prlja, Mario Reljanović, Pravna informatika, Pravni fakultet Univerziteta Union u Beogradu, 2010, strana 54.

[19] http://www.rbs2.com/ccrime.htm

[20] Škulić Milan, Aleksić Živojin (2002.) — Kriminalistika-Dosije, Beograd, str.*396*

[21] Đorđe Ignjatović (1991.) — Pojmovno određenje kompjuterskog kriminaliteta– Anali Pravnog fakulteta u Beogradu, str.*142*

Definicija iz zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala države Srbije: visokotehnološki kriminal predstavlja vršenje krivičnih dela kod kojih se kao objekat ili sredstvo izvršenja dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom i elektronskom obliku[22].

Razlog nepostojanja univerzalne definicije je i taj, što je broj krivičnih dela koja se mogu podvesti čak i pod najrestriktivnije i najuže definicije računarskog kriminala, skoro u svakodnevnom rastu. Klasifikacija takvih ponašanja je teška zato što se ne mogu utvrditi kriterijumi koji će određena dela svrstati isključivo u jednu kategoriju, dok sa druge strane, pojave novih načina zloupotrebe nužno iziskuju i proširenje pomenute liste kriterijuma [144].

Profesor dr. Predrag Dimitrijević kada govori o ovom obliku kriminala podrazumeva ga kao jednu uopštenu formu kroz koju se ispoljavaju različiti vidovi protivpravnog postupanja. Ovaj vid kriminala je usmeren protiv bezbednosti informacionih sistema u celini ili u njenom pojedinačnom delu (mrežni ili računarski sistemi i drugi elektronski uređaji)[23]. Ispoljava se na različite načine, različitim sredstvima i motivisan je koristoljubljem i/ili nanošenjem štete drugome.

Tipovi sajber kriminala, navedeni u materijalu za "radionicu" o kriminalu, na mreži sa desetog kongresa UN, navedeni su kroz definicije u užem i širem smislu [187]:

1. Sajber kriminal u užem smislu predstavlja svako ilegalno ponašanje obavljeno elektronskim putem usmereno ka bezbednosti računarskih sistema i podacima koje oni obrađuju;
2. Sajber kriminal u širem smislu (kriminal vezan za računarsku tehnologiju) je svako ilegalno ponašanje obavljeno pomoću ili u vezi sa računarskim sistemom ili računarskom mrežom, uključujući i takve aktivnosti kao što su ilegalno posedovanje i/ili nuđenje i distribucija informacija pomoću računarskog sistema ili računarske mreže[24]. Naravno, najveći problem prilikom definisanja ovog termina predstavlja razlika u zakonskoj regulativi u većini zemalja;

U istom dokumentu navode se i konkretni oblici kompjuterskog kriminaliteta, u skladu sa Preporukom Saveta Evrope [47] i listom OECD-a [84] iz 1989., odnosno 1985. godine. To su :

- neovlašćen pristup (upad) računarskom sistemu ili mreži (onesposobljavanje zaštitnih mera na sistemu ili mreži),
- oštećenje računarskih podataka ili programa,
- računarska sabotaža,
- neovlašćeno presretanje komunikacija u/od kompjuterskim sistemima i mrežama
- računarska špijunaža.

Ono što treba napomenuti je da u praksi, uglavnom, dolazi do ukrštanja ovih oblika kriminala. Na primer, prilikom neovlašćenog upada u računarski sistem ili mrežu, uglavnom, on može obuhvatiti i računarsku špijunažu ili postavljanje malicioznih programa sa svrhom presretanja komunikacija ili uništavanje podataka.

Kada je reč o sajber kriminalu u širem smislu, najčešće se pojavljuju sledeći pojavni oblici:

1) računarski falsifikati,
2) računarske krađe,
3) tehničke manipulacije uređajima ili elektronskim komponentama uređaja,

[22]Zakon o organizaciji i nadrežnosti državnih organa za borbu protiv visokotehnološkog kriminaliteta, ,Sl. Glasnik R.C. бр.61/2005, 23. 10. 2011.

[23] Predrag Dimitrijević, Kompjuterski kriminal, Izvor : http://www.prafak.ni.ac.rs/files/nast_mat/Kompjuterski_kriminal.pdf 25.11.2011

[24]Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders Vienna, 10-17 April 2000, dostupno na http://www.uncjin.org/Documents/congr10/10e.pdf

4) zloupotrebe sistema plaćanja (manipulacije i krađe elektronskih kreditnih kartica ili korišćenje lažnih šifri u nezakonitim finansijskim aktivnostima).

Evropska konvencija o sajber kriminalu [46] grupiše ova dela u 4 kategorije:

1. dela protiv poverljivosti, integriteta i dostupnosti kompjuterskih podataka i sistema – tu spadaju nezakoniti pristup, presretanje, uplitanje u podatke ili sisteme, korišćenje uređaja (proizvodnja, prodaja, uvoz, distribucija), programa, šifri;
2. dela vezana za računare – tu spadaju krađe i falsifikovanje kao oblici napada;
3. dela vezana za sadržaje – tu spada dečija pornografija obuhvatajući posedovanje, distribuciju, transmisiju, čuvanje ili činjenje dostupnim i raspoloživim ovu vrstu materijala, njihova proizvodnja radi distribucije i obrade u računarskom sistemu ili na nosiocu podataka;
4. dela vezana za kršenje autorskih i srodnih prava obuhvataju reprodukovanje i distribuciju neautorizovanih primeraka pomoću računarskih sistema (ili pomoću mreže).

U Enciklopediji Sajber kriminala čiji je urednik profesor na Ročesterovom Tehnološkom institutu dr. Samuel McQuade, prikazani su i prepoznati sledeći oblici nedozvoljenog ponašanja koje FBI i Nacionalni centar za kriminal belih kragni SAD (*National White Collar Crime Center*) otkrivaju i prate [124]: upadi u računarske mreže; industrijska špijunaža; softverska piraterija; dečija pornografija; zatrpavanje elektronskom poštom; „njuškanje“ lozinki (eng. sniffing); pharming (imitiranje drugog računara radi neovlašćenog upada), i prevare sa kreditnim karticama.

Zavisno od tipa učinjenih dela, sajber kriminal može imati političku ili ekonomsku pozadinu. U politički motivisan sajber kriminal spadaju sledeća dela [54] :

a. sajber špijunaža,
b. upad na računare i mreže (hakovanje),
c. sajber sabotaža,
d. sajber terorizam,
e. sajber ratovanje.

U ekonomski motivisan sajber kriminal spadaju sledeća dela [54]:

a) sajber prevare,
b) neovlašćeno upadanje na računare i mreže (hakovanje),
c) krađa Internet usluga i vremena,
d) piraterija programa, mikročipova i baza podataka,
e) sajber industrijska špijunaža,
f) prevarne Internet aukcije (neisporučivanje proizvoda, lažna prezentacija proizvoda, lažna procena, nadgrađivanje cene proizvoda, udruživanje radi postizanja veće cene, trgovina robom sa crnog tržišta, višestruke ličnosti),
g) proizvodnja i distribucija nedozvoljenih i štetnih sadržaja (dečija pornografija; pedofilija; verske sekte; širenje rasističkih, nacističkih i sličnih ideja i stavova; zloupotreba žena i dece, pružanje nedozvoljenih usluga (kockanje prostitucija),
h) manipulacija zabranjenim proizvodima, supstancama i robama (drogom, ljudskim organima, oružjem),
i) povrede sajber privatnosti (nadgledanje e-pošte; spam, phishing prisluškivanje, njuškanje lozinki tj. sniffing praćenje e-konferencija, prikačinjanje i analiza “cookies”),
j) distribucija zlonamernih programa (virusi, crvi, trojanci, phishing, pharming).

Dakle, štete prouzrokovane visokotehnološkim kriminalom, mogu se podeliti na :

- **materijalne** – za posledicu imaju objektivno učinjenu finansijsku štetu, bilo da je učinilac izvršio delo sa ili bez namere sticanja imovinske koristi.

- **nematerijalne** – odnose se na neovlašćeno otkrivanje nečijih poverljivih informacija, ili neko drugo "indiskretno zlonamerno ponašanje"
- **kombinovane** – kod kojih izvršenje krivičnog dela kao posledicu stvaraju i materijalnu i nematerijalnu štetu na primer, zloupotrebom mreže ili računara izvršena je krađa autorskog dela i javno objavljena pod tuđim imenom.

Prema prikazanim različitim kategorijama ove vrste kriminala mogu se uočiti različiti interesi koje motivišu ljude da počine zakonom nedozvoljene radnje. U praksi, naravno, postoje i slučajevi kada je u pitanju radoznalost, samodokazivanje ili hvalisavost pred drugim licima. Zato se nikada ne može sa sigurnošću govoriti o jedinstvenom profilu učinilaca računarskog kriminala, jer se oni svrstavaju u različite kategorije prema pojavnim oblicima dela koja čine, ali i prema motivima, koji ih pokreću u vršenju kriminalnih aktivnosti.

Prema profesoru Prlji, učinioci ovih dela mogli bi se podeliti na dve grupe na:

a. zlonamerne učinioce, koji mogu da deluju radi ostvarenja imovinske koristi, ili samo u cilju nanošenja štete ili osvete ;
b. učinioce koji nisu motivisani ni ostvarenjem koristi, niti prouzrokovanjem štetnih posledica, već jednostavno traže zadovoljstvo u neovlašćenom prodiranju u neki dobro obezbeđen informacioni sistem ili radi zabave.

Zlonamerni učinioci računarskih delikta najčešće su motivisani koristoljubljem, a smatra se da podaci iz prakse ukazuju na određeni skup osobina koje čine njihov kriminalni profil. Oko 80% delikvenata čini delo prvi put, a 70% je zaposleno više od pet godina u oštećenoj kompaniji. Njihovo starosno doba je u proseku između 19 i 30 godina, pretežno su muškog pola, veoma su inteligentni; imaju uglavnom više godina radnog iskustva i važe kao savesni radnici koji prilikom obavljanja radnih zadataka ne prouzrokuju nikakve probleme. U većini slučajeva su tehnički kvalifikovaniji nego što to zahteva radno mesto na koje su raspoređeni. Ovi učinioci sebe po pravilu ne smatraju kradljivcima ili uopšte kriminalcima, već samo pozajmljivačima.

Kada je reč o drugoj grupi tu se radi o tzv. hakerima[25], koji koriste svoje računarsko znanje da upadaju u tuđe računarske sisteme. Oni zadovoljstvo mogu pronći u samom činu upada u višestruko obezbeđene informacione sisteme. Što su računarski sistemi i mreže bolje čuvani, to je za njih veći izazov. Iako neki od njih nisu zlonamerno motivisani, oni mogu svesno ili nesvesno da prouzrokuju ogromne štete.

Sa druge strane, kada je reč o statistici oštećenih, prema izveštaju Internet Crime Complaint Center (IC3) iz 2009. godine više od polovine oštećenih, zbog Internet zloupotreba su stariji od 40 godina. Izveštaj je pokazao da su 76% cyber kriminalaca muškarci, a da polovina kriminalaca živi na šest lokacija: California, Florida, New York, Texas, Washington i District of Columbia [200].

Dakle, pored posledica finansijske prirode, koje mogu da nastanu kada učinilac vrši delo u cilju sticanja protivpravne imovinske koristi, pa tu korist za sebe ili drugo lice zaista i stekne, ili je ne stekne, ali svojim delom objektivno pričini određenu štetu, ili kada učinilac ne postupa radi sticanja koristi za sebe ili drugoga, ali objektivno učini finansijsku štetu, postoje i posledice nematerijalne prirode. One se ogledaju u neovlašćenom otkrivanju tuđih tajni, narušavanju ugleda, povredi moralnog prava ili drugom sličnom postupanju, kao i kombinovane posledice, koje postoje kada se otkrivanjem određene tajne, ili povredom

[25] Treba napomenuti da nisu svi hakeri zlonamerno motivisani i kao takve razlikuju se nekoliko vrsta hakera. *White hat* hakeri ili kako se još mogu naći u literaturi etički hakeri, "penetration testers", "sneakers", "red teams" i "tiger teams" hakeri, svoje znanje i sposobnosti koriste da bi istražili računarske sisteme i programe, i u njima našli propuste i upozorili proizvođače programa. Na primer, ukoliko pronađu neki sigurnosni propust neće nanositi štetu već će zakrpiti taj sigurnosni propust ili javiti vlasniku da to uradi. Za razliku od njih Black hat hakerima (crackers), fokus je usmeren na činjenje štete na račun drugih. Na primer ukoliko pronađu neki propust na informaciono komunikacionom sistemu iskoristiće ga da od njega napravr neki profit, ili će naneti neku štetu. Gray hat hakeri se bave radnjama koje su na granici sa nelegalnim, npr ako pronađu neki sigurnosni propust neće nanositi štetu već će ostaviti javnu poruku da se zakrpi taj sigurnosni propust (što daje vremena i black hakerima da reaguju !!!). Script Kiddies, predstavljaju hakere bez iskustva koji iskorišćavaju tuđe programe kako bi provalili u računarske mreže i sisteme.

autorskog prava, putem zloupotrebe kompjutera ili informatičke mreže nanese određeni vid nematerijalne štete, a istovremeno prouzrokuje i konkretna finansijska šteta [122].

Svrha detaljnije klasifikacije podrazumeva razdvajanje sajber kriminala od ostalih oblika kriminala. Direktor Kriminološkog instituta Australije Adam Graycar, pokušao je da prevaziđe upravo ovaj problem navođenjem devet kategorija sajber kriminala.

Te kategorije sortirane su na sledeći način [26]: dela protiv telekomunikacionih službi, komunikacija u cilju zločinačkog udruživanja, telekomunikaciona piraterija, rasturanje neprikladnog sadržaja, pranje novca i evazija poreza, elektronski vandalizam terorizam i iznuda, prevare u vezi sa prodajom investicija, nezakonito presretanje telekomunikacija, prevare vezane za elektronsko poslovanje. Međutim, iako je Graycar svojim širokim definicijama zaista gotovo uspeo da pokrije sve oblike neželjenog i nezakonitog ponašanja, u nekim slučajevima one nisu upotrebljive. Kao na primer, analiza rasturanja materijala neprikladnog sadržaja – jer bi u ovu grupu spadale kako reklamne poruke čije slanje u principu nije kažnjivo, tako i slanje rasističkih poruka, pornografskog materijala (uključujući i dečiju pornografiju), uputstva za pravljenje eksplozivnih naprava itd… primera ima mnogo

Pavan Duggal, predsednik međunarodne organizacije „Cyberlaws“, koja se bavi istraživanjem sajber kriminala, sa druge strane izneo je jednu jednostavniju kategorizaciju ovakvih krivičnih dela, ali ona ne zadovoljava po pitanju detaljnije klasifikacije. On navodi da se sva krivična dela iz ove grupe mogu svrstati na[27] :

1. dela protiv ličnosti,
2. dela protiv imovine,
3. dela protiv države.

U pojavne oblike krivičnih dela iz grupe **dela protiv ličnosti** Alice Hutchings, istraživač i analitičar programa za Globalni ekonomski i elektronski kriminal Australijskog instituta za kriminologiju[28] posmatra ovu grupu kroz sledeće pojavne oblike :

- **sajber manipulacija** (eng. Cyber grooming), vrsta psihološke manipulacije koja se obavlja na Internetu preko sinhronih i asinhronih komunikacionih platformi (javne chat pričaonice, Internet sajtovi za upoznavanje, instant messenger-i i VOIP servisi tipa ICQ i Skype) i u novije vreme putem socijalnih mreža (facebook, twitter, myspace) . Žrtve manipulacije su uglavnom deca tj. maloletna lica od 11-17 godina i kao krajnji cilj ove manipulacije je sastanak koji se obično pretvara u seksualno zlostavljanje, fizičko nasilje, dečiju prostitucije i pornografije [29] [100];
- **sajber uznemiravanje**, **uhođenje** (eng. cyber stalking) primer je bombardovanje sms porukama, uznemiravanje e-mail porukama, uznemiravanje telefonskim pozivima, neželjena pažnja – pokloni, slanje različitih poruka putem instant messenger-a čata i voip tehnologije putem društvenih mreža, pa čak i postavljanja web strana i blogova u cilju izazivanja straha kod žrtve. Žrtve ove vrste kriminala su uglavnom poznate ličnosti [30] [101]. U Americi postoje organizacije koje se bave suzbijanjem ovog problema kao na primer WHOA (Working to Halt Online Abuse)[31] ;
- **sajber nasilje – maltretiranje** (eng. cyber bullying). Dok se tradicionalno maltretiranje može izraziti kroz fizičke ili psihičke napade, cyber bullying se odvija

[26] Izvor :http://www.crime.hku.hk/cybercrime.htm, 22.11.2011.

[27]http://www.crime-research.org/analytics/702, 27.10.2011.

[28] Dostupno na http://www.aic.gov.au/events/aic%20upcoming%20events/2011/~/media/conferences/2011-studentforum/alice_hutchings.pdf, 22.11.2011.

[29] Kamil Kopecký, Cyber grooming danger of cyberspace, study, Olomouc, 2010, dostupno na http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=15%3Acybergrooming-danger-of-internet 22.11.2011.

[30] Kamil Kopecký, Stalking a kyberstalking nebezpečné pronásledování, studie Olomouc, 2010, dostupno na http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu 22.11.2011

[31] http://www.haltabuse.org/about/about.shtml, 22.11.2011

na mentalnom planu kao vrsta psihološkog šikaniranja koja se manifestuje kroz slanje uznemirujućih, ponižavajućih, uvredljivih i neprikladnih poruka ili sadržaja. Napadi ovog tipa mogu biti toliko intenzivni i ponavljajući, da žrtva može da doživi mentalni slom, a posledice mogu da dovedu i do samoubistva[32] [205]. I ovaj oblik krivičnih dela, takođe se realizuje putem informaciono komunikacionih tehnologija na već opisan način.

Na osnovu konsultovanja obimne literature realizacija ove vrste kriminala vezane za dela protiv ličnosti može se ilustrovati kroz uglavnom četiri koraka :

a. identifikovanje i lociranje žrtve (tipovanje),
b. uspostavljanje kontakta sa žrtvom,
c. prikupljanje svih relevantnih informacija potrebnih napadaču,
d. sprovođenje protivpravne aktivnosti.

U **dela protiv imovine** spadaju :

- **neovlašćen pristup** – ova dela se obično realizuju uz pomoć phishing-a, pharming-a, malware-a, wifi ranjivostima, i socijalnim inženjeringom;
- **Internet prevare** – vezuju se za zahtevom za transfer novca, spam, clickjacking[33] prevare kroz sajtove za upoznavanje[34]
- **krađa identiteta** - predstavlja još jedan oblik visokotehnološkog kriminala koji se manifestuje kroz krađu identiteta druge osobe u kojima zlonamerna osoba pretenduje da se predstavi kao neko drugi u cilju pristupanju resursima od materijalne koristi (npr. kredita) i drugih privilegija u ime te druge osobe. Žrtva krađe identiteta (znači lice čiji identitet pribavlja zlonamerni napadač) može trpeti štetne posledice, ako se smatra odgovornim za postupke počinioca. Organizacije i pojedinci koji su prevareni na ovakav način od strane lopova, takođe mogu imati štetne posledice i gubitke u istoj meri kao i osobe čiji je identitet kompromitovan.
- **zlonamerni programi** - predstavljaju programe (npr. programski kod, skripta, aktivni sadržaj[35]) koji za cilj imaju određenu zlonamernu aktivnost (da ometaju ispravan rad informaciono komunikacionih sistema, programa ili da ga onemoguće, da prikupljaju takve informacije (ili njihova eksploatacija), čime se dovodi do kršenje propisa o zaštiti privatnosti). Prema Johny Aycocku profesoru informatike sa univerziteta Calgary, ovde spadaju [10] : logičke bombe[36] (eng. logic bomb),

[32] Veronika Krejčí, Kyberšikana kybernetická šikana,(studie), Olomouc, 2010 Izvor : http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-studie 22.11.2011

[33] Clickjacking predstavlja tehniku prevare web korisnika iskorišćavajući neki sigurnosni propust na sistemu ili iskorišćavajući ranjivost nekog web pretraživača sa ciljem otkrivanja poverljivih informacija ili preuzimanja kontrole nad računarom. To se realizuje tako što korisnik klikne na naizgled bezazlenu stranicu i počinje da se izvršava neki kod ili skripta bez znanja korisnika. Zapravo „dugme“ odnosno link koji je bio kliknut počinje da obavlja neku drugu funkciju, a ne onu za koju je korisnik bio obavešten. Na primer, korisnik može da primi mail sa linkom za neki video zapis, ispod koje stoji skrivena druga stranica npr ebay.com. Kada korisnik pokuša da klikne na „play“ zapravo kliknuće na „buy“ na ebay aukciji. Isto tako dešavale su se ove vrste prevara čime se omogućavalo uključivanje web kamera i mikrofona kroz Adobe Flash Player za koji je ubrzo objavljena sigurnosna zakrpa.
Izvor: http://www.adobe.com/support/security/advisories/apsa08-08.html.

[34] Radi se o psihološkim trikovima da bi se namamile potencijalne žrtve kroz sajtove za upoznavanje. Koristeći lažne profile na tim sajtovima za upoznavanje pretvarajući se da savršeno odgovaraju potencijalnoj žrtvi korišćenjem takođe lažne fotografije koja je ukradena sa neke od društvenih mreža. Ljudi na tim fotografijama su takođe žrtve. Akcenat je stavljen na što većem zbližavanju sa potencijalnom žrtvom kroz korišćenje poezije, poklona i drugih „romantičnih trikova“, tako da se žrtvi učini da može da im veruje. Nakon uspostavljanja poverenja krajnji cilj je traženje od žrtve da pošalje novac , ček ili neki drugi oblik načina plaćanja, kako bi se napadaču pomoglo zbog navodnih finansijksih poteškoća kako su predstavili svojoj žrtvi. Kao način borbe protiv ovakve vrste kriminala jesti i obrazovanje što većeg broja ljudi po pitanju ovog načina prevare. Sajt http://www.romancescam.com/ je jedan od sajtova koji doprinose borbi protiv ovakve vrste prevare.

[35] Aktivni sadržaj (eng. active content) predstavlja interaktivni ili animirani sadržaj koji se koristi na Web lokacijama. On uključuje ActiveX kontrole i dodatne uređaje Web pregledača koji predstavljaju male programe čija je upotreba na Internetu rasprostranjena. Pregledanje Weba može postati zabavnije zahvaljujući aktivnom sadržaju jer on obezbeđuje trake sa alatkama, podatke o akcijama, video zapise, animirani sadržaj itd. Dostupno na :
http://Windows.microsoft.com/sr-Latn-CS/Windows-vista/What-is-active-content-and-why-does-Internet-Explorer-restrict-it, 01.03.2012

[36] Logičke bombe – predstavljaju deo koda nekog programa koji pokreće zlonamernu funkciju (akciju) u određeno vreme ili datum ili kada određeni uslovi budu ispunjeni. Sastoji se od dva dela payloada i okidača (eng. trigger). Payload predstavlja nosioca komponente gde se

trojanski konji[37] (eng. trojan horse), zadnja vrata[38] (eng. backdoor), virusi[39] (eng. virus), crvi[40] (eng. worm), zečevi[41] (eng. rabbit), spajveri[42] (eng. spyware), adveri[43]

---

definišu akcije koje će biti izvedene. Drugi deo čini funkciju za okidanje koja je definisana vremenom ili događajem prilikom kojeg će biti izvršena nosiva komponenta. Logičke bombe su uglavnom delovi nekog virusa, jer predstavljaju principe delovanja a ne celokupan mehanizam.

[37]Trojanski konji – Predstavlja program koji se na prvi pogled čini kao koristan, ali tajno obavlja i neke zlonamerne operacije (da ukrade informacije ili šteti sistemu). Jednom kad se instalira omogućuje zlonamernom korisniku udaljeni pristup računarskom sistemu da bi mogao da obavi kriminalne aktivnosti. Mogu služiti za krađu osetljivih informacija, da simuliraju proxy (eng. trojan proxy). Mogu se pojaviti i u formi trojan dialer-a (eng. dialers, zlonamerni programi koji pomoću modema pozivaju „premium-rate“ (veoma skupa uspostava veze i cena impulsa) telefonske brojeve da bi se time ostvarila materijalna korist. Naravno postoje i špijunske forme trojanaca koji špijuniraju računarski sistem (eng. trojan spy), obaveštavaju napadača o aktivnostima korisnika na računaru (eng. trojan notifiers), mogu i da evidentiraju aktivnost na tastaturi (eng. keylogging samo što ovaj tip keylogging-a nije samostalan kao kod spajvera). Karakteristika im je da se ne kopiraju sami i ne vrše zarazu fajlova, već to izvodi osoba koja ih je stvorila i preuzela kontrolu nad kompromitovanim računarom. Mogu se ukloniti ručno ili pomoću antivirusnog programa.

[38] Zadnja vrata predstavljaju mehanizam koji zaobilazi autentifikaciju (bezbednosna provera identiteta). Kao i kod logičkih bombi mogu biti kao deo koda ili kao samostalni programi. Koriste ih programeri da bi uštedeli vreme potrebno za autentifikaciju prilikom otklanjanja grešaka (eng. debbuging). Takođe, mogu da služe da obezbede daljinski pristup računaru ili omogućavanje pristupa otvorenom tekstu (eng. Access to plaintext). Jedna posebna vrsta zadnjih vrata je RAT alat za daljinsku administraciju (eng. Remote access trojan). Ovaj alat omogućuje daljinsko nadgledanje i upravljanje i pristup računaru. Mogu biti instalirani od strane korisnika (za daljinski pristup od kuće ili da se dozvoli help desk-u) ili neprimetno od strane nekog malicioznog programa (da se nanese šteta ili ukradu informacije).

[39] Frederick B. Cohen je 1983 skovao termin „računarski virus“ i odredio je možda i najbolju definiciju virusa u kojoj se kaže da virus predstavlja program koji može inficirati druge programe, modifikujući ih tako da uključuju kopiju njega samoga, koja takođe može biti modifikovana, tako da se virus može širiti u računarskom sistemu ili u mreži koristeći ovlašćenja svakog korisnika sa namerom da se inficiraju njegovi programi. Svaki program koji postane inficiran može delovati kao virus i na taj način se infekcija širi. Izvor : http://all.net/books/virus/part2.html 26.11.2011 Ova definicija je ključna jer određuje šta (zlonamerni) program čini virusom. Npr. dos program Format ili Linuxov program mke2fs imaju osobinu da formatiraju tj. brišu sve podatke sa neke particije, ali oni nisu virusi. Činjenica koja potvrđuje da li se oni šire infekcijom je ta koja određuje program, da li je virus ili ne. Virusi najčešće oštećuju ili modifikuju fajlove na ciljanom računaru, tako da mogu da dovedu sistem u stanje u kome ne može više da se normalno koristi. Ne koriste mrežne resurse za svoje širenje, ali mogu da se šire kroz mrežu kao deo nekog crva. Uglavnom se širi kao posledica delovanja ljudskog faktora. To znači da virus može postojati na računaru ali to ne znači da će sam računar biti zaražen. Računarski virusi mogu biti detektovani i uklonjeni antivirusnim ili antimalware programima.

[40] Crv je zlonamerni program koji ima samoreplicirajuću osobinu kroz računarske mreže. Za razliku od računarskih virusa kojima je neophodno da se prikače (eng. attach) na postojeći program, crv je samostalan i širi se od računara do računara kroz mrežu i ne oslanja se na druge izvršne kodove (ne treba program domaćin da bi radio). Mogu da se šire putem elektronske pošte (na primer ukoliko se e-mail adresar zarazi crvom, repliciraće se kroz sve kontakte iz adresara i izvršiće zarazu e-mail adresara tih kontakata), deljenih datoteka (eng. file sharing) ili internet servisa koristeći različite tipove protokole u komunikaciji (FTP, HTTP, P2P), a mogu da koriste i metode socijalnog inženjeringa zbog čega korisnik na prevaru može da ga pokrene, mada mogu i sami da se pokreću. Uvek izazivaju neku štetu na mreži kao na primer trošenje hardvereskih resursa što u nekim slučajevima može da preraste u obaranje servisa. Računarski crvi se mogu ukloniti korišćenjem alata za uklanjanje zlonamernih programa.

[41] Rabbit predstavljaju posebnu podgrupu crva. Naziv je dobijen po tome što mu je glavna osobina, neverovatno brzo umnožavanje. Postoje dve vrste ovih rabbita. Prva, zapravo, predstavlja program koji pokušava do potroši sve sistemske resurse kao na primer prostor na hard disku. Jedan od primera je i „forks bomb“ koja generiše veoma brzo veliki broj procesa (stvarajući procese sa beskonačim petljama) kako bi se iskoristio sav raspoloživ prostor na disku ili u memoriji. Kada se to desi postaje nemoguće pokrenuti novi program na sistemu. Druga vrsta zečeva je zapravo posebna vrsta crva koja predstavlja samostalan program koji se replicira mrežnim putem sa računara na računar, ali tako da briše svoj originalni primerak nakon replikacije. tj na mreži postoji samo jedna kopija zeca (retko su slučajevi u praksi).

[42] Spajveri ili špijunski programi predstavljaju oblike zlonamernih programa koji se instaliraju tajno (bez znanja korisnika) na računarski sistem. Prikupljaju i šalju informacije zlonamernom napadaču, o upotrebi i drugim poverljivim i ličnim podacima korisnika. Koje posledice i koje tačne informacije ovaj špijunski program može da prikuplja mogu varirati od tipa samog spajvera. Uglavnom predmet prikupljanja može biti bilo šta što potencijalno ima vrednost, a primera ima mnogo: korisnička imena, lozinke, e-mail adrese, brojevi kreditnih kartica, brojevi bankovnih računa, licence računarskih programa, praćenje posećenosti internet stranica, usporavanje internet veze, negativan uticaj na funkcionalnost programa računarskih sistema, izmene vezane za podešavanja bezbednosnih parametara računara (postavljajući ih na najniže vrednosti ili onemogućavanja istih), menjanje početne stranice web pretraživača u novu najčešće zaraženu, kao i mnoge druge osetljive i privatne informacije. Računar se može zaraziti spajverom na različite načine kao što su besplatna online skeniranja sistema, razni dodaci web pretraživaču u vidu pluginova ili add-ona, kroz pristup sumnjivim sajtovima ili slikama pa čak i preko nekih pretraživača, a mogu biti prikačeni kao deo nekog programskog paketa pri instaliranju na sistem. Nisu isto što i virusi (koji takođe mogu da prikupljaju ovakve informacije), zato što nemaju osobinu samo repliciranja. Pojavljuju se i u obliku keyloggera kao podvrsta špijunskih programa, koji pasivno snimaju aktivnost na tastaturi (kucanje na tastaturi). Znači pored toga što rade sve dosad navedeno, u stanju su da vrše i periodična snimanja ekrana (eng. screenshot) definisana vremenski ili na korisnikov klikom miša (što korišćenje virtuelnih tastatura kao vid zaštite od špijuniranja nije adekvatan jer se snima svaki klik po virtuelnim tipkama i to se beleži snimkom ekrana), pregledanje sadržaja međumemorije (eng. clipboard, deo memorije u koji se privremeno smešta isečeni ili kopirani tekst ili grafički objekat), praćenje unosa u web pretraživače, praćenje konverzacije messaging programa (Windows messenger, skype i dr.), praćenje svih otvaranih prozora na sistemu kao i datoteka i to sve praćeno snimkom ekrana. Uklanjaju se korišćenjem antispajver alatima ili nekim antivirusnim programima koji imaju integrisanu antyspaware pretragu.

[43] Adware ili oglašivački softver ima velike slličnosti sa spajverom iz razloga što se obe vrste programa baziraju na prikupljanju informacija o korisniku u njegovim navikama. Razlika je u tome što je advere više marketinški orijentisan. Prikupljene informacije se šalju kompanijama koje se bave posebnom vrstom marketinga (engl. *behavioural marketing*) koja se bavi analizom i praćenjem korisničkih

(eng. adware), hibridi[44], kapalice (eng. droppers) i zamke[45] i zombiji[46] (eng. zombies) [10].

U **dela protiv države** - spadaju ona dela koja su usmerena protiv vlade i vojske. Najzastupljenija vrsta u ovoj kategoriji je sajber terorizam. Sajber terorizam se može definisati kao što to čini profesor Clay Wilson direktor programa Politika Sajber bezbednosti (eng. Cyber Security Policy Program) "*kao političko motivisano korišćenje računara kao oružje ili kao cilj, pod-nacionalnih grupa ili tajnih agenata sa namerom da izazovu nasilje, da utiče na javnost ili na vladu da promeni svoju politiku*.[205][47]" Cilj ovog kriminala je da se napadne kritična infrastruktura u pokušaju da se nanese velika šteta u smislu gubitka života ili materijalne štete. Takvi napadi imaju za cilj da onesposobe informacione sisteme (npr vladine ili vojne web sajtove ili servise) koji su sastavni deo javne bezbednosti, kontrole saobraćaja medicinske i hitne službe i javne radove [117]. Uglavnom se radi o grupama ili pojedincima koji prete međunarodnim vladama i terorišu građane u zemlji.

Sve ove iznete informacije o tipovima napada i zlonamernim programima koji se koriste za njihovu realizaciju, digitalni forenzičar mora da prepoznaje i da bude informisan o njihovim novijim verzijama. Ti zlonamerni programi, o kojima je bilo reči u prethodnom delu rada, predstavljaju alate zlonamernih pojedinaca sa ciljem sprovođenja protivpravnih aktivnosti ili čak anti-forenzičkim delovanjima vezanih za uklanjanje potencijalnih dokaza o protivpravnoj aktivnosti. To, za posledicu može imati nanošenje velike štete, kako kompaniji, tako i pojedincu, ali i državi.

---

navika prilikom Web pretraživanja i oglašavanja. Javlja se u obliku iskačućih prozora (eng. pop-ups) kao reklamni oglas ili preusmeravajući web browser na određene web lokacije sa namerom da korisnika navedu na kupovinu. Ova vrsta programa će praćenjem korisničkih navika pokušati da se uklopi u kontekst onoga što korisnik radi. Na primer, ako korisnik pretražuje na internetu reč potter, rezulatat može biti neželjena reklama za knjigu o Harry Potteru. Neki adveri su nepošteni i zbog toga mogu da se klasifikuju kao špijunski program. Razlog je što ova vrsta programa osim što prikuplja podatke može i dalje da prenosi informacije o korisnicima, što može biti deo opet marketinške svrhe. Instaliraju se uglavnom kao samostalni programi i uglavnom dolaze uz besplatne programe, tako što većina korisnika ne čita uslove upotrebe programa (eng. EULA ili End User Licence Agreement – predstavlja ugovor o licenci softvera, za krajnjeg korisnika) kojeg instalira i prihvata dalju instalaciju po predloženim uslovima što prouzrokuje instaliranje i adware programa. Često dolazi sa integrisanim spajverom ili drugim malicioznim programom koji ugrožava privatnost korisnika (špijunirajući korisnički osetljive podatke). Takođe, kao i spajver programi, prisustvo adwera utiče na performanse računarskog sitema i oni nemaju samo-replicirajuću osobinu. Uklanjaju se sa računara alatima za uklanjanje malicioznih programa ili pomoću naprednijih antivirusnih programa.

[44] Tačni tipovi zlonamernih programa koji mogu u praksi da se pronađu, ne mogu sa sigurnošću da se utvrde kom tipu zlonamernog programa pripadaju. Razvojem programerskih paketa olakšava se stvaranje hibridnih malicioznih programa koji imaju karakteristike takve da odgovaraju karakteristikama različitih tipova zlonamernih programa. Na primer, dešava se da neko isprogramira trojanskog konja, koji ima samoreplicirajuću osobinu kao virus a da stvara backdoor.

[45] Dropper ili kapalica je program koji sadrži neku zlonamernu komponentu koji je dizajniran da "instalira" neku vrstu malvare-a (virusa, spajvera, backdoora, itd) na određenom sistemu. Dropper može biti samostalan ili izveden iz dve faze. Kod samostalanih dropper-a maliciozni kod se nalazi u njemu samom na takav način da se izbegne njegovo otkrivanje antivirusnim ili antimalver programima. Kada se radi o dvofaznom dropperu u prvoj fazi dropper downloaduje malver na ciljni računar a u drugoj fazi ga aktivira.

[46] Zombi je vrsta zlonamernog programa koji računarski sistem stavlja pod kontrolu zlonamernog napadača bez znanja vlasnika tog računarskog sistema. Uglavnom se koriste za lansiranje zlonamernog DOS napada. DOS napad predstavlja napad ne neki servis informaciono komunikacionog sistema (najčešće web servis) sa ciljem da se korisnicima onemogući njegovo korišćenje. Pokretanje ove vrste napada sa jedne mašine nije dovoljno da se izgeneriše velika količina internet saobraćaja da bi mogao da se obori veliki sajt i lako se može izblokirati računar sa kog se to pokušava prostim prekidom konekcije sa tim računarom. Dos napad može se izvršiti na lokalnom računaru ili sa udaljene lokacije [3]. Međutim, ukoliko u napadu učestvuje veliki broj zombi računara na ciljani servis, može se desiti da se uspešno realizuje napad. Koordinisan DOS napad u kome učestvuju ogroman broj mreža zombi računara naziva se DDOS napad ili distribuiran DOS napad (eng. distributed denial-of-service, napad odbijanjem usluga). Te mreže zaraženih računara (zaraženih nekim zlonamernim programom npr. trojanskim konjem ili crvom ili backdoorom) nalaze se pod kontrolom zlonamernog napadača i mogu se zloupotrebiti na takav način da svi računari istovremeno pošalju veliki broj specifičnih zahteva na neku IP adresu čim uspešno mogu da realizuju napad npr. obaranje web servisa. Ovi napadi su vrlo problematični i u današnje vreme najčešće se izvode putem tzv. botneta. Takođe potrebno je istaći i činjenicu da je veliki broj instalacija Operativnih sistema ostao na onoj osnovnoj formi (sveža instalacija) bez instaliranja sigurnosnih zakrpa (eng. patch) i kao takva postaje podložna napadima, što govori o ozbiljnosti ovog problema. Koliko je jedan takav Operativni sistem, bez instaliranih sigurnosnih zakrpa ranjiv, biće prikazano u četvrtom poglavlju ovog rada. Iz prakse može se reći da su najugroženiji oni računari koji su neprekidno na Internetu i imaju stalnu IP adresu (eng. static IP). U takvim slučajevim treba preduzeti naročite mere opreza.

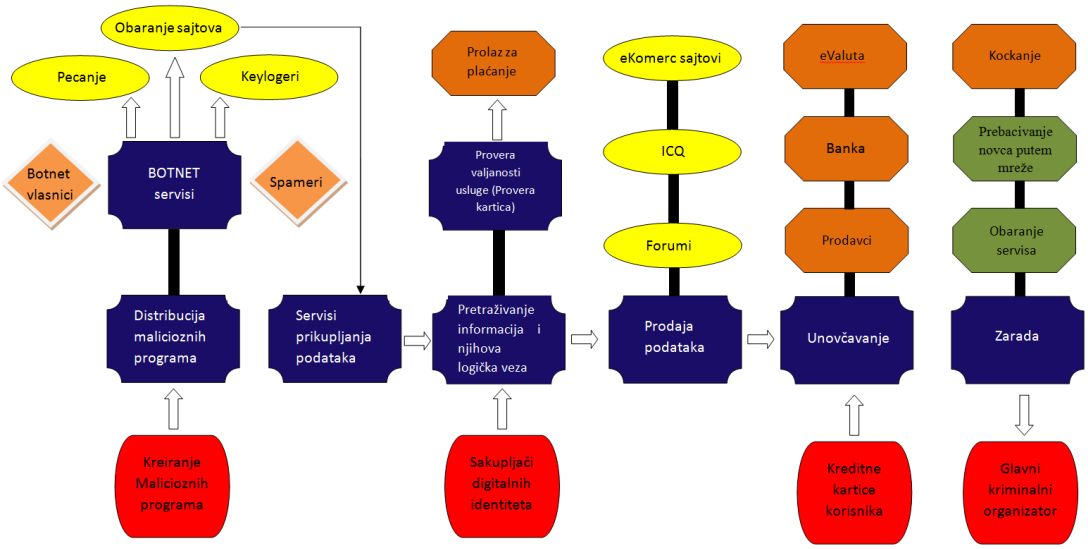
[47] Clay Wilson, Computer attack and cyber terrorism : Vulnerabilities and policy issues for Congress. Us Congressional Research Report RL32114, strana 4. Izvor : http://www.fas.org/irp/crs/RL32114.pdf. October 17 2003

Kada je reč o visokotehnološkom kriminalu u Srbiji, može se reći da obuhvata široku lepezu pojavnih oblika. Najčešći slučajevi su neovlašćen pristup računarima, računarskoj mreži ili bazama podataka, pravljenje i unošenje (širenje) računarskih virusa (kako bi se prikupili podaci o platnim karticama), krivična dela protiv ugrožavanja sigurnosti, povreda autorskih prava tzv. piraterija, zloupotrebe u vezi sa platnim karticama (zloupotreba ukradenih šifri), kompanijska odnosno industrijska špijunaža, napadi sa ciljem onemogućivanja serverskih servisa, zabranjeni pornografski materijali (npr. pedofilski materijali), iznuđivanje ili kompromitovanje, pljačke banaka, ali i svih ostalih krivičnih dela u kojima se koriste računari. Sama količina informacija koja se nudi na Internetu o kompromitovanju platnim karticama je prilična. Postoje određeni profesionalni sajtovi koji se bave prodajom potrebne opreme za ovaj vid kriminala. Koncept je sledeći : traži se preporuka najmanje dva člana, da bi se postao član unutar tog foruma. Po prijemu na forum postaje se običan korisnik. Da bi se došlo do pravih informacija mora se postati VIP korisnik, da bi se pronašlo ono što je tu najbolje. Da bi se postao VIP korisnik prate se aktivnosti i nakon određenog vremena, dopušta se pristup ozbiljnim ilegalnim stvarima (skimeri, dumpovi, 100% ispravni kradeni računi.). Isto tako nije redak slučaj, kada je reč i distribuciji i pristupu zabranjenim pornografskim materijalima, da se pristup specifičnim forumima ostvaruje kroz ostavljanje svojih ličnih podataka koji se proveravaju, zatim se od korisnika traži takođe da ostavi materijale koje im nisu bili poznati ili neke svoje "lično" napravljene (uglavnom kompromitujuće) slike ili video materijale kako bi bili sigurni u vašu iskrenost, i sve to da biste postali VIP član koji ima pristup velikom broju zabranjenog pornografskog sadržaja.

Praksa je pokazala, da jedan od najboljih vidova borbe protiv ovog tipa kriminala, predstavlja infiltraciju u takve grupe i forume da bi se došlo do organizatora.

Čuveni forum kriminalaca Dark Market razotkriven je upravo na takav način (uspešnom infiltracijom), prouzrokujući štetu od 700 miliona dolara zbog aktivnosti te grupe organizujući kupovinu i prodaju ukradenih kreditnih kartica[48].

Na slici 1. dat je ilustrativan prikaz načina na koje se realizuje ovakva vrsta kriminala i na koji način kriminalci ostvaruju zaradu.



Slika 1. *Način realizacije visokotehnološkog kriminala*

Kriminalci koji se bave ovim visokotehnološkim kriminalom pretežno deluju iz zemalja gde pravna regulativa iz ove oblasti nije dobro definisana. Uglavnom biraju zemlje poreskog raja i u njima formiraju off-shore firme. Postoje određene ostrvske zemlje gde

[48] Izvor: http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley

postoji više servera nego stanovnika i ti kriminalci odatle deluju, kako bi sakrili svoje tragove i dokaze.

Kao što se moglo primetiti iz svega prethodno izloženog u pitanju je ogroman broj različitih klasifikacija ove vrste kriminala što nam govori o tome kolika je raznovrsnost ovih dela i koliko su kompleksni njihovi pojavni oblici. Stvar se prilično usložnjava i zbog različitih kriterijuma koji se koriste po pitanju njihove klasifikacije, što samo potvrđuje o kakvom se problemu radi.

Ovom vrstom kriminala se bave pripadnici svih starosnih grupa - od maloletnih lica, studenata, pa sve do penzionera. Od samog znanja i veština učinioca, tipovi krivičnih dela mogu da variraju od ilegalnog kopiranja filmova, muzike, računarskih programa i njihove distribucije na ulici ili na veliko, kao i distribucija zabranjenih pornografskih materijala, pa do upadanja u informacione sisteme kako državnih tako i velikih korporacija.

Visokotehnolški kriminal je stvorio potrebu za angažovanjem posebno tehnički obučenih stručnjaka, kao i za reorganizacijom državnih organa (Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[49]). Glavni nosioci sistema za efikasno suzbijanje visokotehnološkog kriminala su nadležni državni organi koji predstavljaju : policija tužilaštvo, sudstvo, kao i njihove specijalizovane službe, ali i organi državne odbrane, ukoliko se učinjenim delom nanosi šteta ne samo pojedincu nego i celokupnoj državi. U Srbiji se ovom problemu poslednjih godina pristupilo veoma ozbiljno i postoje ohrabrujuća iskustva u radu specijalizovanih organa kao što su : posebne jedinice policije, bezbednosne agencije¸ Specijalno tužilaštvo i Specijalno odeljenje Viših sudova. Krivična dela iz oblasti visokotehnološkog kriminala su u isključivoj nadležnosti tih organa što ujedno predstavlja i institucionalni oblik za borbu protiv visokotehnološkog kriminala u Srbiji. [153].

Za postupanje u predmetima krivičnih dela na osnovu Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala nadležno je Više javno tužilaštvo u Beogradu za teritoriju Republike Srbije. U Višem javnom tužilaštvu u Beogradu obrazovano je posebno odeljenje za borbu protiv visokotehnološkog kriminala tj. Posebno tužilaštvo. Radom Posebnog tužilaštva rukovodi Posebni tužilac za visokotehnološki kriminal. Posebnog tužioca postavlja Republički javni tužilac iz reda zamenika javnih tužilaca koji ispunjavaju uslove za izbor za zamenika višeg javnog tužioca, uz pismenu saglasnost lica koje se postavlja. Prednost imaju zamenici javnih tužilaca koji poseduju posebna znanja iz oblasti informatičkih tehnologija.

5. avgusta 2011 godine Republički javni tužilac Zagorka Dolovac je postavila zamenika Višeg javnog tužioca, Branka Stamenkovića za rukovodioca Posebnog odeljenja za visokotehnološki kriminal, tj. Posebnog tužioca za visokotehnološki kriminal. U Posebnom tužilaštvu pored rukovodioca, angažovana su još dva zamenika Višeg javnog tužioca specijalizovana za ovu oblast kao i dva tužilačka savetnika uz prateće administrativno osoblje. Od osnivanja početkom 2006. godine zaključno sa 1. oktobrom 2011. godine, Posebno tužilaštvo za visokotehnološki kriminal je postupalo ili postupa u preko 1700 predmeta u okviru svoje nadležnosti.

Prethodno navedene informacije o visokotehnološkom kriminalu su veoma važne i moraju se shvatiti krajnje ozbiljno, ukoliko postoji bilo kakva indicija o njihovom postojanju. Da bi država mogla efikasno da suzbija ovaj vid kriminala, neophodno je postojanje razvijenog pravnog sistema kao i zakonskih propisa (do sada se na tome dosta uradilo) koji se moraju poštovati i dosledno primenjivati.

Ono što posebno zabrinjava je i činjenica da se sudije, tužioci i advokati zbog niskog nivoa, čak i elementarnog, znanja informatike, susreću sa mnogobrojnim problemima u postupku procesuiranja osumnjičenih, odnosno okrivljenjih za izvršenje ovih tipova krivičnih dela. Ovo je i jedan od razloga što se umnogome otežavaju i produžavaju postupci, koji zbog

[49] Izvor: http://www.ipc.rs/Arhiva/Download/1010-241.pdf, 03.01.2012

same prirode digitalnih dokaza, iziskuju brzinu i sposobnost, da bi se za veoma kratko vreme spasli digitalni dokazi i identifikovali izvršioci.

Takođe, treba istaći da je proces suzbijanja ovog tipa kriminala nerazdvojivo povezan sa prevencijom i edukacijom u ovoj oblasti, a na tim poljima se do sada nije mnogo uradilo i da treba očekivati da se one realizuju kroz organizovani, sistematizovani i kontinuirani rad.
Na osnovu navedenog, može se zaključiti da postoji velika potreba za dodatnom edukacijom iz informatičkih oblasti koja bi bila prilagođena pravnicima koji se bave tom oblašću. Takođe, na taj način će se graditi svest državnih organa u istražnom i krivičnom postupku o potrebi izuzetno brzog i efikasnog postupanja radi blagovremenog pribavljanja relevantnih digitalnih dokaza, odnosno potrebno je postojanje brže i efikasnije saradnje istražnih i pravosudnih organa sa stručnjacima koji se bave upravo digitalnom forenzikom.

2.1.3 Zakonska regulativa sajber kriminala - istorijat

Kao odgovor na rast visokotehnološkog kriminala, pojavljuje se i Prvi zakon koji se bavi rešavanjem problema vezanih za računarske prevare i nedozvoljenog upada. Donet je na Floridi 1978. godine - „The Florida Computer Crimes Act“. Ubrzo nakon toga usvojen je i američki federalni zakon o računarskim prevarama i zloupotrebama 1984. godine (eng. The Computer Fraud and Abuse Act - CFAA[50]), sa svojim izmenama i dopunama u 1986, 1988, 1989, i 1990. godini. Dok zakoni još nisu jasno definisali sajber kriminal odnosno visokotehnološki kriminal, tužioci su morali da se oslanjaju na tradicionalne krivične zakone.

U početku, CFAA je trebalo da štiti samo računare vlade i finansijske industrije računara od spoljnih krađa i upada. Godine 1986, CFAA iako dopunjen oštrijim kaznama, štitio je i dalje samo računare koje koristi vlada ili finansijske institucije. Konačno 1994, napravljena je značajna revizija CFFA u kome se prvi put pojavljuje građansko pravna komponenta i mogućnost vođenja građanskog parničnog postupka[51].

U Australiji je 1989. godine izvršena je izmena i dopuna „The Australian Crimes Act“ u vezi sa prekršajima koji se odnose na računare (član 76.). U Velikoj Britaniji 1990 usvojen je Zakon o računarskim zloupotrebama (eng. Computer abuse act), kojim se upad na računar smatra kriminalnom radnjom.[52] Takođe, u Holandiji 1993. godine usvojen je Zakon o računarskom kriminalu. Mnoge međunarodne organizacije su takođe donele preporuke u vezi sa izmenama zakonodavstva koja se tiču sprečavanja računarskog kriminala. Na primer, Ujedinjene nacije su se bavile problemom o sprečavanju zločina i postupanju sa delinkventima, na VIII kongresu UN, koji je održan u Havani 1990. godine. Doneta je rezolucija, koja od svih članica UN-a traži da pojačaju napore u pravcu suzbijanja manipulacija sa elektronskim računarima koje zaslužuju primenu kaznene sankcije, te da razmotre primenu različitih mera u tom pravcu. Tu spada modernizacija krivičnog prava i postupka, razvijanje javne svesti o opasnosti novog kriminala i potrebi njegovog suzbijanja, obrazovanja i stručnog usavršavanja službenika državnih organa koji se s njim susreću, razrada pravila profesionalne etike o postupanju sa kompjuterizovanim informacionim sistemima, i unapređenje svih oblika zaštite računarskih delatnosti.[53]“

Paralelno sa donošenjem raznih zakona vezanih za sajber kriminal, krajem 80-tih i u ranim devedesetim godinama pojavljuju se agencije u Sjedinjenim Američkim Državama koje su se bavile ovom problematikom i radile na razvoju treninga i izgradnji kapaciteta da bi rešavale problem vezan za sajber kriminal. Centri kao što su „SEARCH, Federal Law

[50] Izvor: http://www.panix.com/~eck/computer-fraud-act.html
[51] Građansko pravo daje oštećenoj strani priliku da podnese tužbu protiv prekršioca, kako bi dobili nadoknadu za učinjenu štetu.
[52] Eoghan Casey, Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet, Second Edition, Academic Press 2004, poglavlje 2, strana 19.
[53] Vladica Babić, Kompjuterski kriminal, RABIC, Sarajevo, 2009, str. 71

Enforcement Center (FLETC), i National White Collar Crime Center (NW3C)", pokrenuli su inicijativu za sprovođenje programa treninga za agencije reda i zakona [34]. NW3C u saradnji sa FBI osnivaju "Internet Crime Complaint Center" (IC3)[54]. IC3 prihvata i prosleđuje žalbe koje se odnose na visikotehnološki kriminal odgovarajućim agencijama na ispitivanje. Takođe IC3 vodi statistiku o količini i tipu ovih žalbi [109].

U Americi da bi se računari i javnost zaštitili protiv neželjene pošte, postoje zakoni protiv neželjene pošte. 1. Januara 2004. godine, stupio je na snagu zakon Kontrola Napada neželjene pornografije i marketinga, ili CAN-SPAM 55.Prema tom zakonu za krivično delo se smatra svako slanje komercijalnog e-maila sa lažnim ili obmanjujućim zaglavljima poruke ili obmanjujućim naslovom poruke.

Kada je reč o Evropi, prema dr. Mirjani Drakulić, možda najznačajnija aktivnost kojom se pokušava operacionalizovati saradnja u borbi protiv visokotehnološkog kriminala je formiranje EU Foruma [44] koji obuhvata razne agencije, provajdere Internet usluga, operatore telekomunikacija, organizacija za ljudska prava, predstavnike korisnika, tela za zaštitu podataka i sve druge zainteresovane koji žele da se uspostavi saradnja u borbi protiv visoko tehnološkog kriminala na evropskom nivou[56].

U Srbiji institucionalizovana borba protiv visoko tehnološkog kriminala tj. utvrđivanje krivično pravne zaštite počinje od 2005 godine. Tada je donet prvi zakon o organizaciji nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, a njegova primena je počela 2007. godine, nastavljajući se do danas. Ovim zakonom se propisuje formiranje posebnih organa u okviru Tužilaštva, MUP-a i Suda. Uloga i zadatak ovih organa je suzbijanje i borba protiv visokotehnološkog kriminala. Pri Višem javnom tužilaštvu i Višem sudu postoje odeljenja za borbu protiv visokotehnološkog kriminala. U MUP-u, u okviru službe za borbu protiv organizovanog kriminala, takođe postoji odeljenje za visokotehnološki kriminal. Specifičnost ovih organa je da su oni nadležni teritorijalno, dakle, za teritoriju čitave Srbije, dok je stvarna nadležnost određena posebnim zakonom i odnosi se na krivična dela za čije su otkrivanje procesuiranje i kasnije suđenje nadležni pomenuti organi. Nekadašnje rešenje u starom zakonu nije predviđalo određene grupe krivičnih dela kao npr. krivična dela protiv bezbednosti računarskih podataka, krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja. Poseban propust je bio taj što se u odredbe o organizovanom kriminalu nisu uvrstili i oblici sajber kriminala. Izmenama i dopunama koje su stupile na snagu januara 2010. godine ispravljeni su određeni propusti tako da se sada u nadležnosti ovih organa nalaze i krivična dela protiv privrede i krivična dela protiv ustavnog uređenja.

Krivična dela koja se tiču bezbednosti računarskih podataka definisana Krivičnim zakonikom iz 2005. godine su : računarska sabotaža, pravljenje i unošenje računarskih virusa, računarska prevara, neovlašćeni pristup zaštićenom računaru, računarskoj mreži, elektronskoj obradi podataka, različiti oblici falsifikovanja isprava, falsifikovanje novca, zloupotreba i falsifikovanje platnih kartica itd. Treba naglasiti da krađa identiteta nije definisana kao krivično delo, a trebalo bi biti definisana.

Jedan deo zakonskog okvira uspostavljen je izmenama ovog zakona (*Zakon o organizaciji nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala*), kojim se zaokružuje u materijalnom smislu ono što zovemo nedozvoljene društvene aktivnosti tj. radnje koje se smatraju krivičnim delom i koje se smatraju visikotehnološkim kriminalom i nalaze se u nadležnosti pomenutih organa.

Zatim, kao deo ovog zakonskog okvira je i Zakonik o krivičnom postupku. U njemu su opisani procesni mehanizmi kroz koje nadležni državni organi svake zemlje pružaju

[54] Internet crime Complaint Center. IC3 : http://www.ic3.gov/

[55] htpp://www.spamlaws.com/federal/can-spam.shtml

[56] Mirjana Drakulić, Ratomir Drakulić, Cyber kriminal, Fakultet Organizacionih nauka, Beograd, dostupno na http://www.ponude.biz/seminarski/0/49.pdf

mogućnosti, daju ovlašćenja i obaveze prikupljanja dokaza u svakom konkretnom krivičnom predmetu, kao i obezbeđivanje integriteta tih dokaza tj mogućnosti njihovog kasnijeg oporavljanja i izvođenja na sudu. Naš Zakonik o krivičnom postupku poznaje neke opšte dokazne radnje odnosno mehanizme kao što su privremeno oduzimanje predmeta, saslušanje itd… Takođe, naš Zakonik poznaje posebnu definiciju elektronskih dokaza koji se pojavljuju u vezi sa izvršenjem krivičnog dela kao podaci i informacije koji su značajni za istragu i smešteni ili preneti putem računara. Ti podaci imaju veliki značaj, a od presudne je važnosti način njihovog prikupljanja, s obzirom da su ti podaci izuzetno osetljivi, vrlo se lako mogu izmeniti, obrisati ili na neki drugi način uništiti, što zahteva posebnu pažnju i adekvatan pristup u postupku prikupljanja i obezbeđivanja ovakvih dokaza.

Dakle, zakonodavni okvir u zakonodavstvu Republike Srbije koji se odnosi na obezbeđivanje i pružanje krivičnopravne zaštite, dat je u Krivičnom Zakoniku, Zakoniku o krivičnom postupku, Zakonu o organizaciji nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala i u Konvenciji Saveta Evrope o sajber kriminalu koju je naša država ratifikovala u martu 2009. godine.

2.1.4 Visokotehnološki kriminal - primeri iz prakse

Internet ima i svoju drugu stranu medalje. Za organizatore i izvođače upada na računarske sisteme i prevara koje se odnose na visokotehnološki kriminal, Internet predstavlja platformu bez nadzora za podršku pri razmenjivanju informacija o novim otkrivenim ranjivostima, novim otkrivenim exploitima, izvornim kodovima novih exploita (i njihovom razvoju), listama ranjivih lokacija (mreža i sistema), ukradenih finansijskih podataka, i za razmenu zabranjenih sadržaja [39]. Neke od najpopularnijih baza exploita koji koriste i zlonamerni napadači su : The Exploit Database[57], SecurityFocus[58] i OSVDB[59]

Da bi se stekao bolji uvid u razmere specifičnosti i težine ovog vida kriminala, naveo bih u daljem tekstu neke od najinteresantnijih primera visokotehnološkog kriminala, koji su obeležile poslednje 2 decenije.

Između juna i avgusta 1994. godine Vladimir Levin iz Petrograda nakon osamnaest upada u sisteme Citybank izvukao je preko 10 miliona dolara. Sledeće godine je uhapšen u Londonu, 1997. je izručen američkim vlastima i osuđen je na 36 meseci zatvora i novčanu kaznu od 250.000 dolara.

Kevin Mitnik u SAD je uhapšen i osuđen 1995. godine nakon upada u velike računarske sisteme i krađa programa. Ono što je interesantno je da je on to uspeo da uradi sa vrlo malo hakerskog znanja. Zapravo, najviše se služio metodama socijalnog inženjeringa.

Takođe, poznati su i slučajevi gde su službenice Zavoda za penzije u Francuskoj, prebacile na svoje račune 6 miliona franaka na osnovu isplata penzija za osobe koje su davno pre toga umrle.

1998. godine se desio prvi masovni napad na Internetu, kada je u mrežu ubačen samoreplicirajući program koji uništava podatke na računarima i širi se samostalno po mreži (tzv. „crv“, eng. worm) koji je napravio veliku štetu i praktično uništio gotovo trećinu Internet sadržaja u SAD. Iste godine uhapšen je Robert Tappan Morris koji je napisao kod za crv Morris. On je tvrdio da je to uradio iz radoznalosti da vidi koliko je Internet velik.

[57] Dostupno na http://www.exploit-db.com/
[58] Dostupno http://www.securityfocus.com/
[59] Dostupno na http://osvdb.org/

Osuđen je na 3 godine uslovne kazne, 400 sati dobrovoljnog rada i 10.500 dolara novčane kazne.

Između avgusta 1999. i oktobra 1999. Jonathan Joseph James, kao maloletnik od 16 godina izvršio je upade na high-profile organizacije. Jedna takva meta je bila i Agencija Ministarstva odbrane gde je postavio svoj backdoor koji je omogućio da se vide osetljivi podaci kao što su elektronska pošta, korisnička imena i šifre zaposlenih. Takođe je upao i u NASA računare i ukrao program vredan 1.7 miliona dolara. Kao posledica NASA je bila prinuđena da privremeno isključi svoje računarske sisteme, čime je prouzrokovana velika finansijska šteta.

U narednim godinama gotovo da nije bilo Internet prezentacije važnije vladine institucije u SAD, multinacionalne korporacije, međunarodne organizacije i sl. koji nije „hakovan" (eng. hacked) – čiji sadržaj nije izbrisan, zamenjen nekim drugim sadržajem, ili sklonjen na izvesno vreme sa Interneta.

2003. godine pušten je do sada najdestruktivniji crv tzv. Slammer (poznati i kao Sapphire, Helkern or SQLExp), koji je u roku od deset minuta zarazio 90% računarskih sistema na planeti koji nisu imali (adekvatnu) zaštitu. Londonski Market intelligance (Mi2g) procenio je štetu koju je ovaj crv izazvao, na oko 1.2 milijarde dolara[60].

Prema rečima Davida Perry-a, direktora sektora za obrazovanje kompanije Trend Micro koja se bavi bezbednošću računara, napadi na računarske mreže postaju sve sofisticiraniji i teži za uočavanje i odbranu, ali i sve više okrenuti profitabilnoj dimenziji ove aktivnosti[61].

Kako vreme prolazi svedoci smo sve ozbiljnijih finansijski prevara, naročito nakon pojave elektronskog bankarstva, polovinom devedesetih godina prošlog veka i početkom masovnog korišćenja platnih kartica putem Interneta. Na taj način su stvorene pretpostavke za rađanje modernog visokotehnološkog kriminala[62]. Organizovani kriminal, odnosno terorističke grupe, pornografske i pedofilske mreže, grupe za ilegalnu trgovinu oružjem, narkotika, ljudi, uznapredovali su u korišćenju savremenih tehnologija. Procenjena šteta pričinjena od strane sajber kriminalaca u 2006. godini, iznosila je oko 200 milijardi evra na globalnom nivou. Na primer, ChoicePoint, Inc korporacija (kupljena od strane Reed Elsevier-a 2008. godine) je u 2006. godini morala da plati preko 15 miliona dolara kazne na osnovu tužbi građana i miliona potrošača zbog kompromitovanja ličnih finansijskih podataka [2].

Koliko štete ova vrsta kriminala može da prouzrokuje i koje metode, odnosno tehnike koriste kriminalci, naveo bih kroz neke primere Saše Živanovića, načelnika Odeljenja MUP-a za borbu protiv visokotehnološkog kriminala (služba za specijalne istražne metode u Srbiji koji su jedan od najbitnih faktora u borbi protiv visokotehnološkog kriminala), koji na ilustrativan način pojašnjavaju pojavne oblike ove vrste kriminala, a dešavaju se kod nas i u okruženju.

Primer 1 [153]
Prevare koje se odnose na bankomate ostvaruju se upotrebom lažnih maski ili Libanskih klopki koje se montiraju na otvor na bankomatu u koji ulazi kartica sa specijalnim štipaljkama u istoj boji kao i automat. Kada korisnik ubaci svoju karticu da podigne novac, ona ne ulazi u automat već upada u tu štipaljku. Pošto automat ne registruje karticu, korisnik ne uspeva da podigne novac ali ni da izvadi karticu. U tom momentu korisniku prilazi jedan građanin (kriminalac) koji počinje razgovor povodom problema na bankomatu koji je navodno i pomenutom građaninu napravio problem sa karticom, ali da zna kako da se

[60] http://malware.wikia.com/wiki/Slammer, 12.9.2011

[61] Izvor: Michael Coren, *Cyber-crime bigger threat then cyber-terror*, CNN International, 24.01.2005

[62] Koliko je „moderni" visokotehnološki kriminal opasan, može se videti iz napada koji se desio u februaru 2007. godine, kada je simultano napadnuto, sa ciljem potpunog onesposobljavanja, šest od trinaest tzv. „root servera" na Internetu. Da su uspeli u svojoj nameri, Internet bi kao takav u potpunosti prestao da funkcioniše. Na sreću, samo su dva servera pretrpela značajnije posledice. (Izvor: Internet adresa: http://www.crime-research.org/articles/threat-ti-Internet, 12.09.2011.).

problem reši samo mu je potreban pin od kartice. Lakoverni građani obično daju pin. Međutim i pored toga što je navodno ukucan pin, kartica ostaje i dalje u bankomatu bez izdatog novca. Zatim kriminalac daje predlog da se ode do centrale banke i da se tamo zatraži novac. I na kraju kad žrtva ode van vidokruga bankomata kriminalac skida štipaljku ubacuje karticu kuca pin i uzima novac.

Primer 2 [153] Kopiranje podataka sa kreditnih kartica
Ova prevara se uglavnom sprovodi u buticima, prodavnicama, restoranima i prevarant mora da ima saučesnika iznutra. Zadatak saučesnika, npr. konobara, je da karticu koju uzme od gosta, odnosno mušterije prilikom naplate provuče kroz specifičan mali uređaj (skimmer) i iskopira podatke sa kartice. Onda se ti podaci prenesu na magnetnu traku koja se zalepi na belu plastiku i to se onda koristi kao prava kartica. Zbog velikog obima krivičnih dela koje obuhvata visokotehnološki kriminal, širok je i dijapazon njihovih izvršilaca.

Primer 3
Bugarski recept: Korisnik banke stoji ispred bankomata. Izvršioci krivičnog dela obično se pozicioniraju da budu iza korisnika da bi videli pin broj koji se ukucava. Npr. Korisnik banke prilazi bankomatu i dok odabira parametre iz menija bankomata, oni mu neprimetno podmetnu neku novčanicu ili papir da izgleda kao da je nešto ispalo. Paralelno prate šta on kuca i fokusiraju se da zapamte pin tj. taj četvorocifreni broj. Čim ga ukuca obraćaju se korisniku da mu kažu da mu je nešto ispalo. U momentu kada se savije da podigne tu podmetnutu novčanicu, oni za to vreme izvlače karticu i beže. U tom momentu oni imaju podatke o pin kodu i vrše zloupotrebu dok mogu tj. dok se kartica ne blokira.

Primer 4
U jednoj od naših susednih država, kriminalci su napravili ugovor sa kućnim savetom o postavljanju jednog bankomata predstavljajući se kao radnici banke. Kao uslugu za postavljenje bankomata rekli su da će da im renoviraju zgradu (okreče ulaz vrše servisiranje i održavanje lifta). Bankomat je bio postavljen, ali nikada ni jednu novčanicu nije izbacio iz bankomata. To je bio lažni bankomat čiji je cilj bio da se uhvati što veći broj dump-ova (podaci sa kartice) sa kartica od građana koji su pokušali da iskoriste postavljeni bankomat.

Primer 5
Primer pharminga (ranjivost DNS servera), predstavlja redirekciju sa nekog sajta (za sada nije bilo primera u Srbiji). Ukoliko je korisnik pristupao nekom Internet portalu koji se bavi elektronskom trgovinom, kriminalci mogu da iskoriste ranjivost DNS servera tako što će da preusmere saobraćaj. To znači, kad korisnik pokuša da pristupi željenom serveru, vrši se redirekcija na neki server koji oni drže pod kontrolom. Uobičajeno je, da bi korisnik bio naveden, nude mu se povoljne akcije tipa (ovonedeljna akcija Računar i štampač za samo 100 evra). Oni zapravo daju primamljivu ponudu, a naivni korisnik kreće u jednu pravu kupovinu robe ili usluga, normalno unoseći sve one parametre sa svoje kartice. U ovom slučaju neće doći do zloupotrebe pin koda, ali će biti zloupotrebe podataka sa kartice, o broju kartici i o cvv2 broju da bi mogli dalje da je koriste. Uglavnom se koriste kombinovane tehnike phishinga pharminga i tehnike socijalnog inženjeringa [63].

Primer 6
Primer fišinga. Kriminalci su napravili lažnu web stranicu jedne banke. Zatim kriminalci su koristili spam metode ili mail bombere šaljući elektronske poruke na milione i milione

[63] Socijalni inženjering predstavlja upotrebu različitih psiholoških metoda sa ciljem uveravanja u lažni identitet napadača i iskorišćavanje situacije da se daju one informacije koje nikad ne biste dali.

adresa. Otuda i naziv fišing odnosno pecanje, i ko se upeca, upeca. U tom e-mailu postavljen je hyperlink ka toj određenoj stranici i kad se klikne na njega vodi vas do vaših podataka i traže vaš pin broj. U e-mail-u mogu biti navedeni različiti razlozi zbog čega vas banka kontaktira. Razlozi mogu biti od poboljšanja sigurnosti, pa do pretnji da ste u određenoj proceduri zbog nekorišćenja platne kartice, pa ukoliko ne sarađujete, ugasiće vam se račun. Kada klikne na taj hyperlink, korisnik ne ide na web stranicu svoje banke već na web stranicu koju su kreirali kriminalci. I na kraju, korisnik prateći njihova uputstva ostavlja svoje podatke o kartici. Ono što javnost treba da zna to je, da bilo koja banka da je u pitanju, nikada neće e-mailom od vas tražiti pin kod, vaše kartice !!!

Primer 7
Primer tehnike socijalnog inženjeringa korišćenjem telefoniranja. Korisnika neko pozove i predstavi se kao referent Banke i kaže „poštovani korisniče primetili smo da je došlo do tri uzastopna neuspešna pokušaja prilikom pristupa vašem bankovnom računu, a kako vaš račun nije bio siguran i da bi vaši privatni podaci bili zaštićeni banka je zaključala vaš račun, obavezni smo osigurati vaše transakcije putem Interneta i molimo vas da pozovete određeni broj telefona. Pozivom tog broja telefona otpočinje tačno razrađeni scenario. Javlja se sekretarica, koja daje obaveštenje o mogućnosti izbora tipa usluge koju možete da odaberete pritiskom određenog tastera, a kao glavni cilj je da vi izdiktirate svoje podatke o vašoj platnoj kartici.

Primer 8
Primer korišćenja tehnike socijalnog inženjeringa metodom phishinga za zloupotrebu sms servisa na mobilnim telefonskim aparatima. U Beogradu se dosta koristi sms servis prilikom plaćanje parkinga mobilnim telefonom. Time mobilni telefon sve više postaje radna kancelarija koja će biti u sve široj upotrebi. Za ovu kriminalnu radnju napravljen je lap top sa uključenim bluetooth uređajem na sebi i specijalno podešenim programom koji služi za sniffing tj. njuškanje. Na taj način vrši se uspostavljanje veze, preuzima se kontrola, vrši se širenje virusa, koji daje mobilnom telefonu naredbe za plaćanje u zavisnosti kako se to definiše. Većina korisnika, što je velika greška, ostavlja neke svoje podatke o platnim karticama, pin brojevima upravo u telefonskom imeniku svog mobilnog telefona ili na nekom drugom mestu u telefonu. Naravno u telefonu su pohranjeni i drugi podaci koje kriminalci mogu iskoristiti. Osim pomenutog lap-topa, na tržištu se može naći i tzv. „Bluetooth sniper“ puška koja skenira i napada bluetooth uređaje na udaljenosti koje mogu biti veće i preko 1 km. Prva verzija ove puške prikazana je još 2004. godine na sajmu u Las Vegasu.

Primer 9:
Još jedna od tehnika socijalnog inženjeringa :
Kriminalci su otvorili profil na facebooku koji se zove Dream team agencija. Ta agencija nudi mogućnost osvajanja 150 evra, radi promocije otvaranja agencije i mogu da dobiju 3 osobe. Ono što se očekuje od potencijalnog dobitnika je da se pozove još jedan prijatelj u ovu grupu i ako ste baš srećni, slučajnim izbornim sistemom dobićete 150 evra. Sledeći korak je da dobijate mail u kome se kaže da ste slučajnim izborom sistema dobili nagradu od 150 evra. Naravno, zamoljeni ste da popunite sledeće podatke kako bi vam nagrada bila uplaćena. Podaci koje se od vas traže su: broj kartice, cvv2 broj, datum i vreme isteka kartice, moraju sve cifre da se pišu sa naznakom da se ti podaci dostave na ovaj profil. Time ste im servirali sve informacije. Posle su dodali i poklanjanje kuće sa bazenom. Nažalost, građani na ovo nasedaju.

Primer 10

Korišćenje malicioznih programa bio je slučaj u Srbiji. Momak iz okoline Beograda sam je napisao Irc trojanca u Visual Basicu. Bio je oduševljen kako njegov virus funkcioniše u zemljama evropske unije jer je mislio da EU ima bolje sisteme zaštite. Primenom tehnike socijalnog inženjeringa, došao je do podataka o računu nemačkog državljanina. Svojim programom preuzeo je daljinsku kontrolu nad njegovim računarom. Praćenjem web kretanja ovog korisnika uvideo je da isti koristi on-line bankarstvo. Svojim programom pokupio mu je sve pristupne podatke o njegovoj banci. Uvideo je i jednu opciju da može da se vrši transfer novca van zemalja EU. Za tu svrhu je otvorio poseban račun u našoj zemlji da bi tu nameru mogao da sprovede. Paralelno je kreirao jednu lažnu stranicu njegove banke koju je upload-ovao (pohranio) na njegov računar. U međuvremenu mu je poslao jedno elektronsko pismo : „*Poštovani Gospodine, naša banka je uočila da ste vi u protekloj godini izuzetno dobro trgovali sa hartijama od vrednosti i sa tim u vezi mi smo odlučili da vas nagradimo sa 1300 evra, molimo vas da sledite dalja uputstva"*. Razlog za ova uputstva je bio taj da bi se dobio TAN kod (jedinstveni jednoznačni kod koji se koristi samo jednom) koji mu je bio potreban da izvrši transakciju. Međutim optuženi se nije najbolje snašao sa TAN kodom, što je doprinelo otkrivanju njegovog identiteta.

Primer 11
Opasni kriminalci koji se bave pljačkama iznudama i otmicama , takođe su uvideli koristi od sajber kriminala tako što su počeli da vrše otmicu nekog stručnjaka koji se sam bavio ilegalnim poslom i koji zna kako da donese pare iz daljine. Tako su jednog programera uhvatili, odveli ga u Budimpeštu, uzeli mu pasoš, i rekli da će ubuduće raditi za kriminalnu grupu, a ne za sebe. On je pristupio Australijskoj banci (koja nije tada koristila TAN brojeve) i pristupio je računu određene žrtve i izvršio transfer 5036 au$ na račun naše domaće banke. Podatke je nabavio sa posebnog foruma, sa kog je posle izbačen kada se pročulo da je uhapšen. Ovo je tipična manifestacija protivpravne imovinske koristi. Pripada jednom organizovanom obliku kriminala na Internetu i mimo Interneta gde svako ima određenu ulogu.Uključena su uglavnom lica mlađeg starosnog doba 20-30 godina.

Primer 12 : Internet prevara
Reč je o falsifikovanju SAD poštanskih markica. Naime, Ikar Dakota Feris je priznao da je u periodu od 2004 do 2009 godine bio umešan u izradi i štampanju falsifikovanih SAD poštanskih markica koje se legitimno prodaju preko stamps.com. Takođe je priznao da je nudio falsifikovane poštanske markice putem Interneta predstavljajući ih kao popust SAD poštarine. Ukupan profit koji je napravio je iznosio 345.000 $[64]

Primer 13 : Kršenje autorskih prava
Okružni sud u Beogradu na osnovu optužnice Posebnog tužilaštva za visokotehnološki kriminal oglasio je krivim G.M. Iz Beograda na zatvorsku kaznu od 6 meseci uslovno, zato što je od 2006. do 2008. u svom stanu u Beogradu neovlašćeno umnožavao primerke autorskih dela i oglašavao njihovu prodaju preko više Internet prezentacija. Nudio je 13.433 naslova autorskih dela i nakon elektronske porudžbine slao je CD i DVD diskove poštom i tako je stvorio imovinsku korist od 400.000 din[65].

Primer 14 : Internet prevara
Okružni sud u Beogradu na osnovu optužnice Posebnog tužilaštva za visokotehnološki kriminal oglasio je krivim J.Š. i njegovu devojku T.D. iz Novog Sada, zbog prevare počinjene preko Interneta, na zatvorsku kaznu od 6 meseci uslovno, zato što su od januara

[64] Dostupno na http://www.justice.gov/criminal/cybercrime/ferrisPlea.pdf
[65] Dr Dragan Prlja, Sajber criminal, Pravni fakultet Univerzitet Union, dostupnona http://www.prlja.info/sajberkriminal.pdf, 30.04.2012.

2007. do jula 2007. doveli u zabludu 29 britanskih državljana da će im obezbediti smeštaj tokom Exit-a u hotelu u Novom Sadu, što nisu činili, već su ih slali taksijem u hotel sa kojim nisu imali nikakav poslovan aranžman[66].

Primer 15 : Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka

Krivično delo Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz čl.302.st.1. Krivičnog zakonika. Posebno tužilaštvo podnelo je istražnom odeljenju Okružnog suda u Beogradu predlog za preduzimanje određenih istražnih radnji Kt.vtk.br. 56/07 protiv V.M. (31) iz Beograda zbog osnovane sumnje da je, dana 08.02.2007.godine, u vremenskom intervalu od 22:39:50 do 22:49:08 časova, u Kragujevcu, u hotelu „Stari Grad“, koji posluje u sastavu preduzeća „Tourist gamesstari grad“, neovlašćeno pristupio računarskoj mreži ošt. preduzeća „Yunicom“ sa sedištem u Beogradu. putem interne računarske mreže hotela u kojem je boravio - konektovao svoj računar na globalnu računarsku mrežu - Internet i pristupajući sa IP adrese broj: 87.116...., koja je u to vreme od strane Internet provajdera „SBB“ bila dodeljena preduzeću „Tourist gamesstari grad“, prekršio mere zaštite uspostavljene od strane ošt. preduzeća „Yunicom“ - unoseći u svoj računar web - adresu broj: 217.24..... dodeljenu ošt. preduzeću „Yunicom“ za pristupanje web - mail serveru „World Client for MDaemon“ preko kojeg su zaposleni iz ošt. „Yunicom-a“ ostvarivali poštanski saobraćaj, nakon čega je - znajući kao bivši radnik „Yunicom-a“ adrese elektronske pošte i lozinke zaposlenih lica, iste unosio i na svom računaru neovlašćeno pregledao sadržaj njihove elektronske pošte [67].

Iz prethodno navedenog i poglavlja koja se odnose na visokotehnološki kriminal mogu se uočiti određene specifičnosti:

- Protivpravne aktivnosti se uglavnom rade za novac, profit ili korist.
- Protivpravne aktivnosti (pogotovu napadi na računarske sisteme) postaju sve više sofitsticiraniji odnosno teži su za detekciju, analizu, brzo se šire i alati koji se koriste za tu namenu nisu javno dostupni.
- Krajnji korisnici postaju izloženiji sve većim rizicima (napadi su promenili fokusa sa servera na klijentske računare)
- Napadi su uglavnom pokreću iz inostranstva
- Velike razlike između sofictičiranih alata za napad i onih koji se koriste za njihovu detekciju i analizu

Prema APWG (Anti-Phishing Working Group)[68] izveštaju u trećem kvartalu 2012 godine[69] detektovano je preko 6 miliona malicioznih programa. Od toga 78.04% predstavljaju trojanci, 6.56% predstavljaju virusi, 6.53% predstavljaju crvi, 5.33% (Maliciozni programi za Internet prevare (eng. Rogueware), i ostali 3.33%. Procenat napada na finansijske usluge i usluge plaćanja iznosi čak 66.5% od svih napada. Primetan je porast napada na aukcijske sajtove i on iznosi 4.5%. Prema broju hostovanja fišing sajtova u trećem kvartalu 2012. Amerika je vodeća sa 73.04% iz razloga što se najveći procenat svetskih WEB sajtova i domenskih imena hostuje u Americi (a fišing se realizuje preko hakovanih ili kompromitovanih WEB sajtova). Države sa najvećim procentom zaraženih računara su Kina 53.17%, Južna Koreja 52.77%, Turska 42.51%, Slovačka 40.59% i Tajvan 40.20%. Norveška sa 20.16% i Irska sa 18.40% spadaju u zemlje sa najmanjim brojem zaraženih računara [8].

U tabeli 2. dati su statistički podaci koji pokazuju različite tipove napada na računarske sisteme i njihov ukupan procenat (prijavljenih slučajeva) u 2012 godini :

[66] Dr Dragan Prlja, Sajber criminal, Pravni fakultet Univerzitet Union, http://www.prlja.info/sajberkriminal.pdf, 30.04.2012.
[67] Dr Dragan Prlja, Sajber criminal, Pravni fakultet Univerzitet Union, http://www.prlja.info/sajberkriminal.pdf, 30.04.2012.
[68] http://www.antiphishing.org
[69] http://www.apwg.org/download/document/84/apwg_trends_report_q3_2012.pdf

Tabela 2 : Statistički prikaz prijavljenih napada [178]

TIP NAPADA	PRIJAVLJENI SLUČAJEVI
Data Theft	33%
E-mail abuse	22%
Unauthorized Access	19%
Data alteration	15%
Virus attacks	5%
DoS attacks	3%
Others	3%

Kada je u pitanju visokotehnološki kriminal digitalna forenzika je jedan od najznačajnih faktora u procesu otkrivanja istine o protivpravnim aktivnostima na osnovu svojih otkrića i rezultata. Međutim, cilj ovog rada je između ostalog da pokaže da digitalna forenzika, odnosno forenzika računarskih sistema deluje i preventivno, kad se govori o ovoj vrsti kriminala. Jer upravo njeni rezultati su ti koji pokazuju kako se neka protivpravna aktivnost desila, gde su bili propusti i na koji način su se oni desili, pa samim tim moguće je predupredi ti iste ili slične protivpravne aktivnosti. Dakle, učenjem od računarske forenzike kao podskupa digitalne forenzike i implementacijom tih saznanja u mehanizme zaštite IKT-a, ona postaje bitan elemenat proaktivne zaštite.

Trka između zakona i njegove primene sa jedne strane i novih tehnologija i njenih primena u zlonamerne svrhe na drugoj strani, i dalje traje.

2.2 ISTRAŽNE METODOLOGIJE - MODELI

Brzim tehnološkom razvojem, kao i razvojem programa, korisnici postaju digitalno znatno pismeniji, a kriminalne radnje postaju sve sofisticiaranije kada je u pitanju način izvršenja. Primena zakona je u stalnoj trci sa kriminalcima kada je reč o visokotehnološkom kriminalu. Jedan deo trke se odnosi na razvoj alata za prikupljanje i pretragu digitalnih dokaza, u odnosu na one kojima se vrši prikrivanje kriminalnih radnji, a drugi deo trke se odnosi na razvoj metodologije u digitalnoj forenzici. Metodologijom se obuhvataju forenzičke analize svih tipova digitalnih istraga kriminalnih radnji. Mora biti primenjiva na sve aktuelne digitalne zločine kao i na bilo koje nerealizovane zločine u budućnosti [159].

Svrha definisanja modela digitalne istrage je da informiše, oblikuje, i standardizuje proces digitalne istrage[70]. U ovom radu biće prikazani najznačajniji modeli digitalne istrage koji mogu da obezbede dosledan i standardizovan okvir koji podržava sve faze istrage. Neki od modela koji će biti prikazani prilaze digitalnoj istrazi sa naučno-tehničkog aspekta, a neki sa netehničkog aspekta. Takođe, neki od prikazanih modela su detaljniji u odnosu na druge po pitanju korespondencije fizičke i digitalne istrage, a opet kada je reč o istražnom procesu neki modeli imaju veći okvir u metodološkom smislu.

Cilj prikaza istražnih metoda, predstavlja presek trenutnog stanja istražnih metoda. Takođe, ovo može biti od pomoći istražiteljima, jer na osnovu preseka stanja, mogu u skladu sa specifičnostima istrage, primeniti odgovarajući model.

Za potrebe prikaza istražnih metoda, konsultovana je obimna relevantna literatura koja opisuje različite istražne metodologije u cilju traženja modela koji bi mogli biti primenjeni na digitalnu forenzičku analizu, kako u zvaničnom tipu istrage, tako i u korporacijiskom tipu i istrage uključujući i računarske incidente. Zajedničko za sve modele jesu 4 osnovne istražne faze: **Identifikacija/rukovanje (***skupljanje, prenos, integritet u lancu*

[70] Daniel A. Ray, Phillip G. Bradford, Models of Models: Digital Forensics and Domain-Specific Languages (Extended Abstract), http://www.ioc.ornl.gov/csiirw/07/abstracts/Bradford-Abstract.pdf, strana 1., 18.12.2011

istrage), **Forenzička akvizicija** (*otkrivanje, fiksiranje i izvlačenje),* **Forenzička analiza (***analiza DP i izgradnja čvrstog DD) i* **Prezentacija (***stručno svedočenje/veštačenje na sudu).*

2.2.1 The DFRWS model

DFRWS model razvijen je između 2001 i 2003 [71] pri digitalnoj forenzičkoj istraživačkoj radionici (eng. Digital Forensics Research Workshop). Razvijena od strane grupe istraživača i stručnjaka iz digitalno forenzičkih oblasti [53]. Ovim modelom su obuhvaćene digitalno istražne radnje, definisane klasama. Te klase, u stvari, služe za kategorizaciju istražnih radnji po grupama. Ovim modelom su predviđene liste radnji koje mogu da se izvršavaju a neke od njih su obavezne. Specifičnost ovog okvira je ta, što za svaku pojedinačnu istragu u velikoj meri model mora biti redefinisan. Okvir je predstavljen tabelom čije kolone predstavljaju klase radnji koje treba preduzeti u digitalnoj istrazi, a svaki red sadrži elemente te klase. Prema ovom modelu postoji ukupno sedam faza u procesu istrage digitalnih dokaza : identifikacija, čuvanje, sakupljanje, pretraživanje, analiza, prezentacija i odluka. Definisane klase ovih radnji i njenih elemenata predstavljene su u tabeli 3. [72]:

Tabela 3. DFRWS model digitalne istrage

1	2	3	4	5	6	7
IDENTIFIKACIJA	**ČUVANJE**	**PRIKUPLJANJE**	**ISPITIVANJE**	**ANALIZA**	**PREZENTACIJA**	**Odluka**
Otkrivanje događaja/vremena	Uprava slučaja	Čuvanje	Čuvanje	Čuvanje	Dokumentacija	
Potpis odluke	Tehnologija snimanja	Odobrene metode	Praćenje	Praćenje	Svedočenje stručnjaka	
Otkrivanje profila	Sled isključivanja	Odobreni softver	Tehnike validacije	Statistika	Pojašnjavanje	
Otkrivanje anomalije	Usklađivanje vremena	Odobreni hardver	Tehnike filtriranja	Protokoli	Izjava o delotvornosti misije	
Žalbe		Pravni autoritet	Uklapanje (poređenje) uzoraka	Izvlačenje podataka	Preporučena protivmera	
Posmatranje sistema		Kompresija bez gubitaka	Otkrivanje skrivenih podataka	Vremenski sled (hronologija)	Statistička interpretacija	
Audit analiza		Uzimanje uzoraka	Izvlačenje skrivenih podataka	Link		
		Redukovanje podataka		Prostor		
		Tehnike oporavka				

2.2.2 The Reith , Carr and Gunsch model ili The Abstract Digital Forensic Model

Ovaj model je razvijen 2002. godine i sastoji se od sledećih 9 koraka [73][159]:

1. **-Identifikacija** - prepoznavanje incidenta na osnovu pokazatelja i utvrđivanje njegovog tipa. Ovo ne spada eksplicitno u oblast forenzike, ali ima značajan uticaj na druge korake.
2. **Priprema - priprema alata**, određivanje tehnike, priprema naloga za pretres, praćenje ovlašćenja i podrška upravljanju.

[71] http://www.dfrws.org/2001/dfrws-rm-final.pdf, 18.12.2011

[72] http://www.dfrws.org/2001/dfrws-rm-final.pdf, strana 17, 18.12.2011

[73] M. Reith, C. Carr, and G. Gunsch. An examination of digital forensics models. *International Journal of Digital Evidence*, 1(3), 2002, strana 6, 25.12.2011.

3. -**Pristupna strategija** - formulisanje dinamičkog pristupa u čijem je fokusu primenjena specifična tehnologija u krivičnoj radnji i sprečavanje uticaja na potencijalne svedoke. Cilj strategije treba da bude maksimalno prikupljanje nepromenjenih dokaza, uz minimalni uticaj na žrtvu.
4. -**Očuvanje dokaza** - izolovati, osigurati i sačuvati stanje fizičkog i digitalnog dokaza. Ovo podrazumeva i sprečavanje ljudi da koriste digitalne ili neke druge elektromagnetne uređaje koji mogu u incidentnom okruženju uticati na dokaze.
5. -**Prikupljanje** - snimanje fizičkog mesta i dupliranje digitalnih dokaza koristeći standardizovane i priznate procedure.
6. -**Ispitivanje** - dubinsko i sistematsko pretraživanje dokaza koji se odnose na moguću krivičnu radnju. Fokus je na identifikovanju i pronalaženju dokaza, na mogućim potencijalnim lokacijama. Konstruiše se i detaljna dokumentacija za analizu.
7. -**Analiza** - utvrđuje se značaj, vrši se rekonstrukcija fragmenata podataka i donose se zaključci na osnovu pronađenih dokaza. Broj ponavljanja postupka ispitivanja kao i same analize razlikuje se od slučaja do slučaja. Postupak obavljanja analize ne zahteva visoku tehničku sposobnost i na taj način veći broj ljudi može da radi na slučaju.
8. -**Prezentacija** - vrši se obrazloženje zaključaka. Takva obrazloženja treba da budu prilagođena i manjoj stručnoj javnosti uz korišćenja apstraktne terminologije koja se odnosi na pojašnjene zaključaka.
9. -**Vraćanje dokaza** - obezbeđenje da se fizička i digitalna svojina vrate pravom vlasniku kao i definisanje načina na koji moraju biti uklonjeni krivični dokazi. Ovo ne spada eksplicitno u forenzički korak tako da nije zastupljen u nekim drugim forenzičkim modelima istrage.

Ovaj model sličan je DFRWS modelu i slično su definisane klase Očuvanja, Prikupljanja, Ispitivanja i Prezentovanja. U modelu je dodata podrška za pripremu alata i dinamičke formulacije istraživačkog pristupa [158]. Ovaj model predstavlja jedan apstraktni model koji može da se primeni na bilo koju tehnologiju ili vrstu visokotehnološkog kriminala za različite tipove incidenata. U stvari, njegov značaj je da se on iskoristi kao osnova za razvoj detaljnijih metoda prilikom istraživanja odredjenih vrsta visokotehnološkog kriminala. Prednosti ovog modela su sledeće :

- kreiranje doslednog i standardizovanog okvira za digitalno forenzički razvoj;
- primenjivost predloženog mehanizma za buduće digitalne tehnologije;
- metodologija je generalizovana na takav način da omogući sudu da pojasne tehnologiju ne tehničkim posmatračima:
- identifikuje se potreba za specifičnim tehnološkim alatima kao i uvid u prethodno definisane alate;
- potencijal za obuhvatanje elektronskih tehnologija ne digitalnim pristupom kroz apstrakciju.

Mane ovog modela :

- definisane kategorije mogu biti previše uopštene za praktičnu primenu
- nema lakog načina za testiranje ovog modela;
- svako dodavanje potkategorija ovom modelu učiniće ga težim za korišćenje;
- model ne ističe značaj lanca očuvanja integriteta (eng. chain of custody), već se u njemu samo navodi da, ukoliko je lanac očuvanja jak, on će se održati tokom trajanja istrage.

2.2.3 The Ciardhuain model

Ciardhuain model je razvijen 2004. godine od strane Seamus O. Ciardhuáin. Bazira se na prethodnim modelima, ali sa proširenom "vodopad" (eng. waterfall) arhitekturom[74]. Koraci ili faze u ovom modelu definisani su kao aktivnosti. Ovaj model se realizuje kroz sledećih 13 koraka tj. aktivnosti[75] [40]:

1. **Svesnost -** Stvaranje svesti o tome da je potrebno sprovesti istragu. Svest može biti stvorena kako spoljašnjim događajima (na primer krivično delo prijavljeno policiji) tako i unutrašnjim (na primer sistem za detekciju napada na OS upozorava sistem administratora da je bezbednost sistema ugrožena).
2. **Autorizacija -** Dobijanje ovlašćenja za sprovođenje istrage. Forma ovlašćenja može znatno da varira u zavisnosti od tipa istrage. Na primer sistem administrator može zahtevati jedno usmeno odobrenje od strane menadžmenta kompanije za detaljnu istragu računarskih sistema te kompanije, ukoliko se radi o korporacijskoj istrazi. Kao druga krajnjost, nadležni državni organi moraju dobiti formalno zakonsko ovlašćenje kojim se tačno precizira šta je u istrazi dozvoljeno (sudski nalozi ili garancije).
3. **Planiranje-** Planiranje aktivnosti u velikoj meri će zavisiti od informacija koji potiču, kako iz same organizacije (politike procedure i saznanja o prethodnim istragama), tako i od onih informacija koje od spolja imaju uticaj (propisi i zakoni koji postavljaju opšti kontekst za istragu i koji nisu pod kontrolom istražitelja).
4. **Obaveštavanje-** Odnosi se na informisanje o predmetu istrage i informisanje drugih zainteresovanih strana da je istraga u toku, da bi bili svesni istrage. Ova aktivnost nije primenjiva u nekim istragama gde je potreban faktor iznenađenja da bi se sprečilo uništavanje dokaza.
5. **Pretraga i identifikovanje dokaza -** Ova aktivnost se bavi pronalaženjem dokaza i na osnovu toga identifikuje potrebe za sledeću aktivnost. Na primer u jednostavnijim slučajevima aktivnost može da podrazumeva, pronalaženje računara koji se koristi od strane osumnjičenog, i potvrdu da je to od interesa za istražitelje. U složenijim okruženjima, ova aktivnost nije jednostavna jer može zahtevati otkrivanje računara kroz veći broj Internet pružaoca usluga (eng. ISP - Internet service provider) ili otkrivanje računara u drugim zemljama na osnovu podataka o IP adresi računara.
6. **Prikupljanje dokaza** - Predstavlja aktivnost kojom se dokazi prikupljaju u obliku koji može da se sačuva i analizira, na primer kreiranje slike (eng. image) hard diska ili zaplena celog računara. Ova aktivnost veoma je značajna za dalji tok istrage i fokus je većine rasprava u literaturi. Razlog tome su greške koje mogu da nastanu, a loša praksa u ovoj fazi može za posledicu da ima nevažeći dokaz ili čak može da dođe i do uništenja samog dokaza. Ovo se naročito odnosi na istrage za dela koja su inkriminisana zakonom kao krivična.
7. **Transport dokaza** - Nakon aktivnosti prikupljanja, dokazi moraju biti transportovani na odgovarajuću lokaciju za dalja ispitivanja. To može biti jednostavan fizički prenos zaplenjenih računara na bezbednu lokaciju, ali može da podrazumeva i prenos podataka preko mreže. U ovoj fazi bitno je obezbediti integritet samih dokaza pri transportu.

[74] Vodopad način istrage podrazumeva da aktivnosti prate jedna drugu u nizu.

[75] Seamus O. Ciardhuáin, : An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2004, dostupno na https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

8. **Smeštaj dokaza** - Prikupljeni dokazi u većini slučajeva moraju da se čuvaju, jer ispitivanje nad njima se ne može uvek odmah odvijati. Prilikom skladištenja potrebno je takođe, kao i u prethodnoj aktivnosti, voditi računa da se očuva integritet dokaza.
9. **Ispitivanje dokaza** - Uključuje korišćenje potencijalno velikog broja tehnika za pronalaženje i tumačenje podataka značajnih za istragu. Na primer, može se zahtevati popravka oštećenih podataka na način koji podrazumeva očuvanje integriteta istih. U zavisnosti od rezultata prikupljanja pretrage i identifikacije koji može predstavljati veliku količinu podataka koje treba ispitati, neophodno je korišćenje i automatizovanih tehnika koje mogu pomoći istražiteljima.
10. **Hipoteza** - Nakon ispitivanja, istražitelji definišu hipotezu o tome šta se desilo. Stepen formalnosti ove hipoteze zavisi od vrste istrage. Na primer, kao rezultat policijske istrage biće detaljna hipoteza, sa detaljnom propratnom dokumentacijom o ispitanom dokaznom materijalu, koja će biti pogodna za korišćenje na sudu. Za razliku od policijske istrage, interne istrage u kompaniji, od strane sistem administratora, kao rezultat imaju manje formalan izveštaj koji je namenjen menadžmentu kompanije.
11. **Prezentovanje hipoteze** - Osim istražiteljima, hipoteza može biti prezentovana i trećim licima odnosno nadležnim organima. Kada je u pitanju zvanična istraga hipoteza se predstavlja sudu, a u slučaju korporativne istrage predstavlja se menadžmentu.
12. **Dokazivanje hipoteze** - Hipoteza mora da pretrpi dodatne provere i kontra argumente . Na primer, sudu će biti prezentovani kontra teza i suprotni dokazi. Ako kontra teza ima čvršćih argumenata to će značiti da se istraga mora vratiti korak unazad, da bi se pribavili i analizirali dodatni dokazi sa ciljem izgradnje čvršće i argumentovanije hipoteze.
13. **Diseminacija** - Širenje informacija ili aktivnosti koje mogu uticati na buduće istrage ili neka buduća pravila i procedure (ukoliko sud dozvoli nakon završetka istrage). Primer diseminacije opisali su profesori sa Univerziteta Arizona Tucson, Hauck, Chau i Chen njegove kolege 2002. godine, kroz kreiranje sistema "COPLINK"[76] [81] koji pruža podršku nadležnim državnim organima u svojstvu istražitelja u realnom vremenu u vidu alata za analizu koji sadrže veliko broj prikupljenih informacija iz prethodnih istraga. Ekspert računarske forenzike i glavni urednik naučnog časopisa "IEEE software", Harrison, sa svojim kolegama 2002. godine [79] predstavili su prototip sistem koji ne funkcioniše u realnom vremenu, ali omogućuje funkciju arhiviranja iskustava i stečenih znanja istražitelja.

Takođe, ovaj model uključuje i pojam "protok informacije" (eng. information flows), čime se omogućuje dublje razumevanje izvora dokaza i drugih podataka. Podrazumeva se da ovi tokovi informacija moraju biti definisani na organizacionom nivou i mogu se primeniti na različite istrage u okviru iste organizacije.

2.2.4 The Beebe i Clark model

Model Bebbe i Klark[14] ne grupiše aktivnosti, već ih struktuira kroz faze koje se sastoje od više podfaza. Sastoji se od šest faza :

1. **Priprema** - Ideja pripreme je predstavljena u kontekstu poboljšanja kvaliteta i dostupnosti digitalnih dokaza koji se prikupljaju uz minimalne troškove. Ova faza podrazumeva sve one korake koji utiču na povećanje identifikacije i dostupnosti digitalnih dokaza kao podrška detekciji, odgovoru na incidentnu/protivpravnu

[76] Izvor: http://www.fbe.hku.hk/~mchau/papers/coplink.pdf, 0103.2012

aktivnost i krivičnoj istrazi visokotehnološkog kriminala. Cilj ove faze je postavljanje organizacije u forenzički spreman položaj [163].

2. **Odgovor na incidentnu/protivpravnu aktivnost** - Ova faza podrazumeva otkrivanje i inicijalne predistražne radnje. Ukoliko postoji sumnja da se radi o visokotehnološkom kriminalu kao na primer ugrožavanje bezbednosti računara, korišćenje računara za prikazivanje zabranjenih materijala (dečije pornografije). Cilj ove faze je da se otkriju, potvrde, procene i definišu strategije odgovora na bezbednosni incident.
3. **Prikupljanje podataka** - Prikupljanje podataka i informacije koje su potrebne da bi se potvrdio incident i njegov značaj. Kada se donese odluka da se istraži incident odnosno protivpravna aktivnost, formalno se započinje faza Prikukupljanja podataka. Kao cilj ove faze je prikupljanje digitalnih dokaza kao podrška istražnom planu i strategiji.
4. **Analiza podataka** - Predstavlja najsloženiju i najdužu fazu u procesu digitalne istrage. Svrha analize podataka je da potvrdi ili opovrgne sumnje u vezi sa protivpravnim aktivnostima. Takođe, može dati odgovore na pitanja u vezi sa rekonstrukcijom događaja (ko, šta, gde, kada i kako [133]).
5. **Prezentacija nalaza** - Svrha ove faze je prezentovanje relevantnih nalaza različitoj publici uključujući menadžment, tehničko osoblje, pravna lica kao i nadležne organe. Prezentovanje nalaza može biti usmeno, pismeno ili može da podrazumeva obe forme. Prezentacija treba da obezbedi detaljnu obrazloženu rekonstrukciju događaja, na osnovu informacija koje su dobijene iz podataka tokom faze Analize podataka.
6. **Okončanje i zaključak istrage** - Fokus ove faze je na zatvaranju istrage. Važno je istaći da se u ovoj fazi ne realizuje samo okončanje istrage (i postupa po rešenjima u vezi sa njom), već se i radi na očuvanju stečenog znanja za poboljšanje narednih digitalnih istraga.

Sve faze i podfaze ovog modela pokrivene su principima digitalne istrage i direktno zavise od nje. Podfaze su orijentisane više ka cilju nego prema aktivnostima. Krajnji cilj svake podfaze se predstavlja ciljevima u širem smislu, a ne kao konkretni pojedinačni zadaci. Zadaci istrage su direktno zavisni od specifičnosti slučaja i tipa visokotehnološkog kriminala. Kao nedostatak ovog modela se ističe da je nepotpun i da je previše sveobuhvatan. Takođe prilagođavanje modela novim tehnologijama ili specifičnim operativnim sistemima povećava kompleksnost ovog modela stvarajući nove podfaze.

2.2.5 Kruse i Heiser model

Kruse i Heiser u svom modelu predstavljenom 2002. godine, navode da se proces forenzičke istrage sastoji iz 3 koraka [108]:

1. **Sticanje dokaza** (eng. acquiring)- Podrazumeva rukovanje dokazima, prikupljanje dokaza, identifikovanje i označavanje dokaza, transport dokaza, skladištenje dokaza, uz poštovanje lanca očuvanja integriteta dokaza.
2. **Utvrđivanje autentičnosti dokaza** - Cilj ovog koraka je pokazati da su prikupljeni dokazi identični onima koje je ostavio osumnjičeni za izvršenje protivpravne aktivnosti. Uglavnom se koriste timestamping (vremenske oznake koje dokazuju postojanje dokaza u specifičnom trenutku) ili kriptografske tehnike (dobijajući heš (eng. hash) vrednost koja predstavlja fingerprint dokaza) sa ciljem da se dokaže validnost i originalnost dokaza.

3. **Analiza podataka** - obezbediti digitalnu kopiju originalnog dokaza, napraviti minimum 2 bekapa originalnog diska. To se radi bit-to-bit (eng. bit stream imaging ili eng. disk imaging) programima čime se dobija forenzički bekap odnosno klon originalnog diska uključujući slobodan i slek prostor (o njima će biti više reči u poglavlju 2.3.5). Ovo je jako važno napomenuti, jer normalan bekup ne kopira obrisane fajlove i određene delove hard diska koji mogu sadržati informacije od velike važnosti za digitalnu istragu. Sa analizom treba početi nakon pravljenja heš vrednosti image-a hard diska koji će se analizirati, i izvršiti dokumentovanje. Obavezno je nad svim pronađenim digitalnim dokazima održati lanac očuvanja integriteta digitalnih dokaza (eng. chain of custody). Posle analize smestiti ih na sigurno mesto, gde ne mogu biti oštećeni ili uništeni. Na kraju ovog koraka ostaje prezentovanje sudu šta je urađeno sa dokazima, zašto i da li su izvršene radnje nad dokazima bile prihvatljive.

2.2.6 America's department of justice - **DOJ model**

Ovaj model (DOJ model[77])je predložilo američko pravosuđe 2001. godine u "Vodiču za istragu digitalnog mesta krivičnog dela" (eng. Electronic Crime Scene Investigation Guide)[135] i veoma je sličan prethodnom modelu (Kruse i Heiser model) i isto tako nezavistan je od tehnologije. Razlika je u tome što je istaktnuta posebna faza Izveštaj. Ovaj model orijentisan je više ka fizičkom mestu krivičnog dela, a manje ka forenzičkoj analizi i ispitivanju digitalnog sistema. Model se sastoji od sledećih faza :

- **Priprema** – U ovoj fazi vrši se pripremanje opreme i alata koji će biti neophodni u istrazi ;
- **Prikupljanje dokaza** – U ovoj fazi vrši se pretraga i prikupljanje elektronskih dokaza koje se realizuje kroz sledeće podaktivnosti : obezbeđenje mesta krivinog dela[78], dokumentacija mesta krivičnog dela[79] i sakupljanje dokaza[80];
- **Ispitivanje** - Obezbeđuje prepoznavanje dokaza objašnjavajući njegovo poreklo i značaj kao i pregled skrivenih i nejasnih informacija uz pravljenje odgovarajuće dokumentacije u vezi sa ispitivanim dokazima ;
- **Analiza** -Cilj ove faze je da se, na osnovu rezultata faze ispitivanja, ukaže na značaj i dokaznu vrednost koju mogu posedovati pronađeni dokazi ;
- **izveštaj** - ovaj korak podrazumeva pisanje izveštaja sa akcentom na proces analize dokaza i oporavka važnih podataka tokom cele istrage. Svaki slučaj računarskog kriminala obavezno prati izveštaj.

2.2.7 Model "Odgovor na incident"

Prosise i Mandia su 2001. godine predstavili digitalno istražni model "Odgovor na incident" [156][155]. Ova metodologija je adekvatna za korporacijski model istrage i fokusirana je na incidentni odgovor kada su u pitanju kritični sistemi koji mogu biti kompromitovani. Model se sastoji od sledećih 11 faza :

- **Priprema za incident** - Podrazumeva sve one radnje koje će potpomoći da se forenzički relevantan događaj spremno dočeka. Omogućava se jednostavnija

[77] https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[78] Obezbediti mesto krivičnog dela radi bezbednosti lica i integriteta podataka kao i zbog identifikacija potencijalnih dokaza. Treba napomenuti da profesionalana radoznalost ljudi koji nisu deo istražnog tima (policajci i drugi profesionalci) mogu ugroziti dokazni materijal.

[79] Podrazumeva se dokumentovanje fizičkog opisa mesta krivičnog dela, kao na primer fotografisanje računara

[80] Podrazumeva konfiskovanje računarskog sistema ili pravljenje kopije podataka na forenzičkom sistemu

koordinacija između kadra zaduženog za odgovaranje na incidentnu radnju. Priprema podrazumeva identifikovanje i klasifikovanje kritične informacione imovine, implementaciju računarskih i mrežnih protivmera koje podstiču efikasniji odgovor na incident, posedovanje programskih i hardverskih alata za odgovor na incident (kao na primer alati za pronalaženje i eliminisanje virusa i pretnji), uspostavljenje efikasnije politike koja podstiče odgovor na incidentnu radnju uz odgovarajuća interna dokumenta i kontrolnih listi (koja imaju za cilj brži oporavak sistema i mreže od incidentne radnje)[81]. Ulaganje u razvoj kapaciteta za incidentne odgovore u okviru organizacije zavisi od procenjenog rizika. Takođe, podrazumeva se organizovanje obuke IT kadra u okviru organizacije i nabavka neophodne infrastrukture.

- **Detektovanje incidentne radnje** – Podrazumeva identifikaciju sumnjive radnje.
- **Inicijalni odgovor na incident** - U ovoj fazi se vrši potvrđivanje da se desila incidentna radnja i skupljaju se nestabilni dokazi tj. lako promenjivi dokazi (dokazi, odnosno podaci koji mogu lako da se izgube na primer podaci iz RAM memorije).
- **Izrada strategije za odgovor na incident** – Predstavlja određivanje odgovora na incidentnu radnju u skladu sa poznatim činjenicama.
- **Duplikacija** – Predstavlja pravljenje bekapa, odnosno mirror-ovanje postojećeg sistema.
- **Istraga** – Predstavlja istraživanje sistema da se identifikuje ko, zašto i na koji način se realizovala incidentna aktivnost.
- **Realizacija sigurnosnih mera** - Ova faza podrazumeva izolovanje sumnjivog sistema.
- **Posmatranje mreže** - Ova faza podrazumeva posmatranje mreže radi potencijalne detekcije novih odnosno ponovljenih napada.
- **Oporavak** – Predstavlja vraćanje sistema u njegovo originalno stanje sa pridodatim merama zaštite.
- **izveštavanje** - Podrazumeva izradu dokumentacije u vezi sa odgovorom na incidentnu radnju.
- **revizija** – Predstavlja razmatranje odgovora i prema potrebi adekvatno prilagodjavanje.

2.2.8 Eoghan Casey model

Casey model je predstavljen 2000. godine [36][37] i u početku je bio zamišljen kao model koji se primenjuje isključivo na nezavisne računare (eng. standalone computers) da bi se vrlo brzo počeo primenjivati i u umreženom okruženju. Istražnom procesu prilazi sa pravnog stanovišta i ima nešto veći okvir. Veoma je primenjiv, kako na korporativnu istragu tako i na zvaničnu istragu. Predstavljene kategorije su opšteg karaktera. Model omogućava ispitivačima i istražiteljima principe na osnovu kojih može da se formira argumentovana hipoteza koja je zasnovana na činjenicama uzimajući u obzir pravni kriterijum za prihvatljivost. Ti principi su sledeći [35]:

- **Prihvatljivost** – Koriste se metode i koraci koje su stekle konsenzus u relevatnim krugovima.
- **Pouzdanost** – Korišćeni metodi su lako proverljivi i dokazivi kako bi otkrića bila potkrepljena.
- **Ponovljivost**- Postupak je nezavistan prostorno i vremenski i može se ponoviti.
- **Integritet** – Postojanje mogućnosti provere neporemenjenosti stanja dokaza.

[81] Kao na primer kreiranje spiska za proveru eng. notification checklist, kreiranje načina označavanje (eng. tag) i obeležavanje (eng. label) digitalnih dokaza, kreiranje početne kontrolne liste odziva na incidentnu radnju prilagođenu okruženju), obuka zaposlenih koji će učestvati u odgovorima na incidentne radnje/protivpravne aktivnosti.

- **Uzročno posledični sled** – Logičan sled događaja koji povezuje dokaze sa osumnjičenim.
- **Dokumentacija** – Ceo istražni postupak je pokriven dokumentacijom uključujući i ekspertska svedočenja.

Koraci Casey modela su sledeći [35]:

- **Sumnje ili incidentna upozorenja** - Svaki proces ima neki svoj početni korak. Početni korak može, na primer, da bude signaliziran od strane alarma nekog sistema za zaštitu (sistem za detektovanje napada eng. intrusion detection ili sistem za detektovanje zlonamernih aktivnosti eng. proactive threat protection), senzora zaštite na mreži, administratora sistema nakon pregleda log fajlova. Takođe, može biti iniciran na tradicionalan način, u slučaju da građanin prijavi moguću kriminalnu aktivnost, što za posledicu ima izlazak istražnog tima na fizičko mesto krivičnog dela. U slučaju da se na tom mestu nalaze i elektronski uređaji (računari, telefoni, mrežna oprema i ostali digitalni izvori) deo istrage će se odvijati i u digitalno forenzičkom pravcu. U ovoj fazi se vrši prikupljanje inicijalnih činjenica pre pokretanja potpune istrage, da bi se razmotrio izvor i pouzdanost informacije. Na primer, pojedinac se žali na uznemiravanje zbog pretećih poruka na ekranu, uzrok može biti virus, ili "proactive threat protection" prijavljuje neuspešni upad u sistem, a može biti i lažan alarm. Zbog navedenog, ovaj prvi korak je izuzetno osetljiv (jer se donose zaključci o tome da li se desila protivpravna aktivnost ili ne) zbog toga što svaka intervencija na mestu zločina može uticati na promenu dokaza što može ugroziti ceo proces. Uglavnom je neophodno da se uđe na mesto zločina, u ovom slučaju, digitalno mesto da bi se prikupile inicijalne činjenice koje mogu sadržati relevatne informacije, ali se to mora obaviti na izuzetno pažljiv način. Naglasio bih da je iskustvo samog istraživača ili eksperta u ovoj fazi veoma bitno jer može pomoći u donošenju zaključaka da li se kriminalni akt dogodio ili nije, na osnovu malog broja dokaza. Ulazak u istragu prerano, odnosno bez odgovarajućeg ovlašćenja ili protokola, može dovesti do kompromitovanja celog slučaja.
- **Procena značajnosti** - Istražni resursi (osoblje koje je uključeno u istražne aktivnosti) su ograničeni (zbog angažovanja na više slučajeva istovremeno ili su slučajevi ekvivalentni po značaju) i kao takvi primenjuju se samo tamo gde su najpotrebniji. U zavisnosti od istražnih okruženja značaj ispitivanja sumnjivih kriminalnih aktivnosti varira. Kada je u pitanju zvanična istraga sve sumnjive kriminalne aktivnosti se moraju ispitati od strane nadležnih državnih organa. U civilnom i poslovnom okruženju sumnjive aktivnosti će biti predmet istrage, ali politika i kontinuitet poslovanja su češće u prvom planu po značaju u odnosu na legalni aspekt. Faktori koji utiču na značajnost su : pretnje fizičkim povredama, mogućnost značajnih gubitaka, rizik kompromitovanja ili ometanja sistema većih razmera. Ukoliko se problem može brzo zaustaviti ili ukoliko štete nema ili je minimalna, ukoliko nema faktora pogoršanja, potpuna istraga se ne mora sprovoditi. U ovom koraku donosi se odluka ili o nastavku primene istražnih resursa (na osnovu važnosti dokaza pregledanih do ovog koraka) ili o obustavljanju daljih akcija ukoliko podaci i informacije ukazuju da protivpravna aktivnost nije učinjena uz detaljno obrazloženje.
- **Protokoli incidenta i mesta zločina** - Ukoliko je potpuna istraga odobrena, glavni cilj ovog koraka je sačuvati mesto zločina u "netaknutom" stanju. To se postiže dokumentovanjem stanja i očuvanjem integriteta predmeta sa mesta zločina na osnovu protokola, procedura i prakse koji moraju da se primenjuju da bi se smanjio procenat greške, previda i povreda onih koji su odgovorni za osiguravanje mesta zločina (digitalni istražitelji ili lica koja su prva odgovorila na incidentnu radnju). Rezultat ove faze je obezbeđeno mesto zločina, gde je sav sadržaj dokumentovan i snimljen sa pratećim fotografijama i sa osnovnim dijagramima da bi se mapirale

važne oblasti i predmeti. Ovakvo obezbeđeno mesto zločina je dobar temelj za sve naredne aktivnosti i predmeti otkriveni u ovoj fazi ostaju nepromenjeni tokom cele istrage. U ovom koraku se ne prikupljaju dokazi i ne radi se analiza već se samo identifikuju dokazi koji su relevantni za slučaj.

- **Identifikacija ili konfiskacija** - Nakon što je mesto zločina osigurano, potencijalni dokazi zločina ili incidenta moraju biti konfiskovani. Od izuzetne je važnosti da procedure budu jasne, a da bi se one uspešno sprovodile, neophodno je razumevanje pravnih kriterijuma. Cilj ove faze je da se napravi dobar odabir objekata - trijaža, koje treba konfiskovati (fizičke i digitalne) uz što detaljnije dokumentovanje i obrazloženje svake sprovedene aktivnosti. Dokumentacija je prisutna u svim fazama istražnog postupka, ali je pri konfiskovanju digitalnih dokaza najvažnija zbog uspostavljanja lanca očuvanja integriteta zaplenjenih dokaza. Na primer, fotografisanje i snimanje serijskih brojeva, predmeta, dokumentovanje ko je rukovao dokazima, pomaže da se prati kretanje dokaza nakon prikupljanja. Za tu namenu postoje obrasci i definisane procedure koje pomažu da pri održavanju dokumentacije. U tradicionalnom kontekstu konfiskovanje podrazumeva "uzimanje predmeta", a u digitalnom kontekstu se vrši konfiskovanje predmeta, takođe ali sa tom razlikom što ti predmeti nose i "određena stanja"[82] koja mogu da se izgube nakon zaplene ili nestabilnosti elektronskih uređaja (npr. slaba baterija, prekid struje). Ova specifičnost je veoma bitna jer daje šansu istražiteljima da se prikupe informacije iz zatečenog stanja, pre nego što isključe napajanje i izvrše zaplenu. Iako se u ovoj fazi podrazumeva konfiskacija, treba uzeti u obzir i metode i tehnike koje omogućuju prikupljanje osetljivih sistemskih i mrežnih informacija. Takođe, treba skrenuti pažnju da digitalni dokazi mogu postojati u velikom broju različitih formi : logovi aplikacija, biometrijski podaci, aplikacijski metadata podaci, logovi Internet servis provajdera, firewall logovi, proxy logovi, logovi mrežnog saobraćaja, logovi sistema za detektovanje upada u sistem, sadržaji podataka iz baze podataka i logovi transakcija, logovi audit programa i mnogi drugi logovi. S obzirom na prethodno izneto identifikovanje i zaplena svih dostupnih digitalnih dokaza, nije nimalo lak zadatak. Da bi se proces zaplene što efikasnije sproveo, publikovani su i vodiči u kojima su dati praktični saveti i principi koji su od koristi onima koji se bave digitalnim dokazima. Jedan od njih je "*Electronic Crime Scene Investigation: A Guide for First Responders"*[83] publikovan od strane *US Department of Justice* 2001. godine u USA [9] kao i *„Forensic Examination of Digital Evidence: A Guide for Law Enforcement"*[84] publikovan 2004. godine u USA. Takođe dobar vodič je „*The Good Practices Guide for Computer Based Electronic Evidence"*, publikovan 2003. godine od strane "Association *Chief Police Officers - ACPO*" u Velikoj Britaniji [85]. Dokumenti su veoma korisni u smislu razvijanja standardnih operativnih procedura[86] i mogu da omoguće izvođenje jednostavnijeg tipa istrage sa manjim brojem računara (do 5). Što je bolje utrenirano i obučeno osoblje koje prvo

[82]Ta stanja su zapisana u RAM memoriji (eng. *Random Access Memory*) računara koja sadrže podatke o procesima, informacije o stanju mreže, konekcije sa udaljenim računarom kao i mnoge druge. Kada dodje do isključenja sistema trenutni sadržaj RAM memorije je izgubljen i može samo deo informacija da se povrati.

[83]U ovom vodiču opisani su različiti izvori digitalnih dokaza. Na slikovit način kroz ilustracije opisuje se kako se kojim digitalnim dokazom rukuje kako bi pomogle osoblju koje prvo odgovara na incident, dostupno na adresi https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[84] U ovom vodiču se opisuju opšti forenzički principi i procedure koje se primenjuju u radu sa digitalnom dokazima. Aktivnosti koje se preduzimaju sa ciljem prikupljanja i zaštite digitalnih dokaza ne smeju da utiču na integritet digitalnih dokaza. Ove aktivnosti sme da izvodi samo stručno lice uz dokumentovanje svih aktivnosti (zaplena, pregled, prenos, skladištenje i zaštita) [194]. „Forensic Examination of Digital Evidence: A Guide for Law Enforcement" dostupan je na adresi National Institute of Justice : http://www.nij.gov/pubs-sum/199408.htm , pristupljeno 21.05.2013.

[85] Ovaj vodič pruža polaznu tačku za inicijalne korake u rukovanju digitalnim dokazima.
Dostupno na http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

[86] Ove procedure služe da bi se smanjio rizik od greške, obezbeđuje korišćenje najbolje moguće metode i utiče na povećanje verovatnoće da se dva forenzička istražitelja da dođu do istih zaključaka nakon pregledanja dokaza.

odgovara na incident veće su šanse da se pronađe veliki broj dokaza i da se konfiskuju predmeti koji sadrže veliki broj relevantnih informacija.

- **Očuvanje** - Ova faza je odgovorna za preduzimanje potrebnih mera kako bi se očuvali integriteti fizičkih i digitalnih dokaza odnosno njihova nepromenjivost. Za uspeh ove faze bitnu ulogu imaju alati i metodi koji se koriste, kao i sama stručnost istražitelja jer se u krivičnom postupku, uglavnom, pokušava to osporiti od suprotne strane. Veliki broj stručnjaka koji se bavi digitalnom forenzikom tvrde da od ove faze počinje prava digitalna istraga. U ovoj fazi se pravi veći broj dupliranih kopija digitalnih dokaza iz svih izvora, dok se originalni materijal katalogizira i smešta u kontrolisano okruženje u neizmenjenom stanju. Kopija dobijena odgovarajućim forenzičkim alatima koji će takođe biti obrađivani u ovom radu, je identična kopija originalnog materijala koja služi za pregledanje ispitivanje i analize u daljim fazama digitalno forenzičke istrage.
- **Oporavak podataka** -Pre same analize podataka neophodno je izvršiti povraćaj podataka koji su ili izbrisani ili sakriveni ili prikriveni (zamaskirani) ili koji su iz nekih drugih razloga nedostupni za pregled, kao na primer, zbog postojanja nekog specifičnog operativnog sistema ili fajl sistema. Takođe, u ovoj fazi će možda biti neophodno da se vrši rekonstrukcija delova podataka, sa ciljem oporavka nekog objekta. Akcenat u ovoj fazi je proces oporavka i identifikacije svih nedostupnih podataka. Rezultat ove faze je učiniti dostupnim što veću količinu podataka za narednu fazu. Takođe, ova faza omogućuje najkompletniji uvid u vremenski okvir podataka, uvid u motiv i nameru prikrivanja protivpravne aktivnosti brisanjem, skrivanjem ili maskiranjem podataka različitim tehnikama od strane počinioca, ukoliko je konkretan dokaz pronađen ili snimljen. Tehnike prikrivanja podataka od strane malicioznih korisnika odnose se na manipulaciju sa fajlovima, manipulaciju sa diskom, šifrovanje i tehnike prikrivanja podataka (eng. steganography) [129]. Kada je reč o manipulaciji sa fajlovima, uglavnom se menjaju imena i ekstenzije i daju im se osobine skrivanja fajla (eng. hidden properties). Manipulisanje diskom podrazumeva skrivanje particija (PartitionMagic[87], Partition Commander[88], LILO) i skrivanje podataka u loše sektore. Kod enkriptovanja koriste se bit šifting (Hex Workshop[89]) i steganografija (S-tools[90], Anubis[91], MP3STEGO[92], OpenPuff[93]) i upotreba EFS(Encrypting File System)[94] fajl sistema. Prisustvo ovih alata (bez znanja administratora ili korisnika) na kompromitovanom računaru ukazuje forenzičaru da je maliciozni korisnik nameravao skrivanje potencijalnih dokaza ili tragova.
- **Pronalaženje značajnih podataka** - U ovoj fazi istražitelji imaju na raspolaganju sve potencijalne ditigalne dokaze koje su u vezi sa slučajem. Vrši se prikupljanje podataka i metadata podataka (podaci o podacima) iz očuvanog i oporavljenog izvora prema kategorijama dokaza, ne prema sadržaju ili kontekstu. Zapravo, istražitelj na osnovu poznavanja tehnologija i alata, utreniranosti i iskustva, pretražuje određene kategorije koje imaju određene klasne karakteristike za koje se zna da su ili izgledaju da su, u vezi sa relevantnim činjenicama iz slučaja. Ovo je faza gde konkretne činjenice dobijaju oblik koji potvrđuje ili opovrgava hipotezu izgrađenu od strane istražnog tima. Na primer, ukoliko se radi o optužbi koja ima

[87] http://www.symantec.com/press/powerquest/pq092302.html
[88] https://www.vcom.com/partition-commander
[89] http://www.hexworkshop.com/
[90] http://www.spychecker.com/program/stools.html
[91] http://sourceforge.net/projects/anubisstegano/
[92] http://www.petitcolas.net/fabien/steganography/mp3stego/
[93] http://embeddedsw.net/OpenPuff_Steganography_Home.html
[94] EFS može koristiti ugrađenu 128-bitnu enkripciju što se često sreće u praksi. http://www.oit.umn.edu/security/topics/Windows-efs/index.htm

veze sa dečijom pornografijom, zahtevaće se vizuelni digitalni dokazi u nekom od strandardnih grafičkoh formata kao na primer JPG, GIF, BMP, TIFF. U tom slučaju istražitelj će se fokusirati na pretragu fajlova koji sadrže određene karakteristike ovih grafičkih formata. Ukoliko se radi o incidentnoj radnji "upadanju u sistem" istražitelji će se fokusirati na pretraživanje fajlova ili objekata koji su u vezi sa rutkit alatima[95] (eng. rootkit), exploitima (grupe izvršnih fajlova ili skripti) koji pomaže napadaču da uspešno kompromituje sistem. Rezultat je uglavnom velika količina digitalnih informacija koji u sebi sadrže potencijalne dokaze.

- **Redukcija** - Ova faza je specifična po tome što se u njoj ciljaju specifični objekti koji su prikupljeni i povezani sa istragom ili se donosi odluka da se neki od njih eliminišu. U ovom koraku se izdvajaju nebitni podaci od bitnih, na osnovu eksternih atributa podataka (heš ili checksum vrednosti) ili tipova podataka, ne uzimajući u obzir sadržaj ili kontekst. Kriterijum, na osnovu kojeg se vrši eliminisanje određenih podataka je izuzetno važan i može biti preispitan od strane suda. Kao rezultat ove faze, dobija se najmanji skup digitalnih informacija koje imaju najveći potencijal da sadrže podatke sa dokaznom vrednošću.
- **Organizovanje i pretraga**- U ovoj fazi se vrši dobra priprema podataka za temeljnu analizu koja sledi u narednoj fazi. Savet je da se dobijena grupa materijala iz prethodne faze dobro ogranizuje kroz smisleno grupisanje i označavanje ili na neki drugi smislen način organizuju, da bi se ubrzala faza analize. Na primer, određeni fajlovi se mogu grupisati u grupe koristeći foldere ili eksterne medije za skladištenje podataka. Cilj ove faze je da se olakša istražiteljima da pronađu i identifikuju podatke tokom analize, koje će kasnije koristiti pri kreiranje finalnih izveštaja i za svedočenje pred sudom. Ova faza podrazumeva korišćenje različitih tehnologija pretraga kao pomoć istražiteljima za brzo lociranje potencijalnih dokaza. Na primer, podaci se mogu indeksirati[96] radi efikasnijeg pregleda materijala što će znatno pomoći istražiteljima pri identifikovanju materijala prema značajnosti (relevantni, nebitni). Rezultat ove faze su dobro organizovani atributi podataka koji moraju da omoguće ponovljivost i preciznost aktivnosti u narednoj fazi koja sledi.
- A**naliza** - Ova faza podrazumeva vrlo detaljnju pretragu padataka koji su identifikovani u prethodnim fazama. Vrši se detaljan pregled unutrašnjih atributa podataka kao što je tekst i njegovo značenje, specifični formati audio i video zapisa. Na osnovu individualnih i klasnih karakteristika pronađenih digitalnih dokaza, prave se veze između podataka, određuje se njihovo poreklo da bi na kraju locirali učinioca protivpravne radnje. Ova faza ima svoje podfaze :

[95] Rootkit je program koji omogućava privilegovan pristup računaru/serveru od strane zlonamernog korisnika, aktivno krijući svoje prisustvo od administratora, u cilju narušavanja standardne funkcionalnosti operativnog sistema ili drugih aplikacija. Termin rootkit nastao je spajanjem reči "root" (što u Linux terminologiji predstavalja tradicionalni naziv za privilegovanog korisnika računara/servera), a reč komplet (eng. kit) (koji se odnosi na programske komponente koje implementiraju ovaj alat) Izvor *:* http://download.nai.com/products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf*, 26.11.2010*. Neke od najkorišćenijih funkcija rootkit programa su sledećr : onemogućavanje logovanja aktivnosti, obezbeđivanje zadnjih vrata za ponovni ulazak na sistem, uklanjanje ili prikrivanje dokaza o inicijalnom ulasku u sistem, skrivanje sadržaja određenih fajlova, skrivanje fajlova i direktorijuma, prikupljanje informacija (šifre, korisnička imena, postojeći računari u mreži). Primer rootkit implementacije : napadač nakon iskorišćenja poznatih ranjivosti na sistemu (nekim od exploita) ili dobijanjem lozinke (razbijanjem zaštite ili putem socijalnog inženjeringa), dobija privilegovan pristup i mogućnost instaliranja rootkita. Rootkit omogućava napadaču da maskira tekući upad i održava privilegovan pristup računaru zaobilezeći mehanizme autentifikacije i autorizacije. Iako može da se koristi za različite namene termin "rootkit" ima negativne konotacije zbog njegove povezanosti sa zlonamernim programima koji utiču na sistem i sa krađom lozinki bez znanja administratora ili korisnika. Jako je teško otkrivanje rootkit-a jer je u stanju da zaobiđe program koji je namenjen da ga pronađe. Metode detekcije uključuju i korišćenje alternativnih operativnih sistema, poređenjem heš vrednosti samog sistema; skeniranje i analizu stanja memorije. Uklanjanje može biti komplikovano ili praktično nemoguće, naročito u slučajevima kada se rootkit implemetnira u samo jezgro, pa je jedino rešenje reinstalacija operativnog sistema. Jedan od projekata koji je usmeren ka pronalaženju rootkita pod Linux operativnim sistemima je i Rootkit hunter (Izvor : http://www.rootkit.nl/projects/rootkit_hunter.html, 26.11.2011)

[96] Indeksiranje je tehnika koja se koristi za brzo pretraživanje podataka. Indeksiranje prolazi kroz kompletno telo podatka i kreira mapu lokacija svih informacija. Ova mapa odnosno indeks ima funkciju kao na primer indeks u knjizi ili lisni katalog u biblioteci. Proces indeksacije može biti dugotrajan, ali kada se jednom uradi pretraživanje je izuzetno brzo.

- **Procena konteksta i sadržaja** - Sadržaje, čitljivih ili vidljivih digitalnih podataka, moguće je pregledati i na osnovu njih utvrditi faktore kao što su način (sredstva), motiv, i prilika.
- **Eksperimentisanje** – Predstavlja probanje novih i neisprobanih tehnika i metoda koje su zasnovane na naučnoj osnovi uz rigorozno dokumentovanje za potrebe testiranja. Rezultat eksperimenta može biti ili odbijen ili opšte prihvaćen.
- **Fuzija i povezanost** - Tokom istrage, podaci (informacije) se prikupljaju iz mnogih izvora (digitalnih i nedigitalnih). Sami za sebe podaci (informacije) ne mogu da prenesu priču o istraživanom događaju, već moraju da se fuzionišu da bi se sklopila cela priča. Primer fuzije može predstavljati vremenski okvir nekog događaja ili radnje koji se odnosi na određeni slučaj odnosno incident. Svaka protivpravna aktivnost ili incident poseduje hronološku komponentu gde događaji ili radnje traju tačno određeni vremenski period. Ovim se dobijaju odgovori na gde, kada i ponekad, kako se desio forenzički relevantan događaj [23]. Vremenski delovi svih predočenih aktivnosti biće fuzionisani sa različitih izvora (digitalnih i nedigitalnih) kao što su digitalni podaci, zapisi telefonskih kompanija, poruke elektronske pošte, izjave svedoka i izjave osumnjičenih. Korelacija se odnosi na uzročno posledičnu vezu između događaja uz hronološko praćenje.
- **Provera valjanosti** - Rezultat faze analize predstavlja podnošenje obrazloženih otkrića sudu ili drugim licima ovlašćenim za donošenje odluka kao dokaz za krivično gonjenje ili oslobađajuću presudu.
- **Izveštavanja**- Da bi se obezbedila transparentnost u istražnom postupku, konačni izveštaj treba da sadrži važne detalje o svakom istražnom koraku, uključujući protokole kojih su se istražitelji pridržavali, metode prilikom konfiskacije, dokumentacija, kolekcija, čuvanje, oporavak, rekonstrukcija, organizovanje i pretraga ključnih dokaza. U izveštaju je potrebno posvetiti najviše pažnje analizi na osnovu koje su se izveli zaključci ili na opisima dokaza koji podržavaju te zaključke. Ne donositi zaključke bez detaljno opisanih potkrepljujućih dokaza i analiza. Izveštaj mora biti objektivno napisan uključujući i iznošenje alternativne teorije koji su kontradiktorne ili nepotkrepljene dokazima.
- **Argumentovano uveravanje i svedočenje** - Cilj ove faze je da analitičari i/ili eksperti obuhvate sve tehničko-tehnološke i inženjerske detalje, kao i korišćene metode u istrazi i prenesu ih u jasnom obliku, razumljivo Sudu.

Ovaj model je široko primenljiv i nezavistan je od tehnologije. Faza analize u ovom modelu se zasniva na naučnim metodama.

2.2.9 Carrier i Spafford model

Carrier i Spafford model je predstavljen 2003. godine [27]. Ovaj model posmatra računar kao mesto protivpravne aktivnosti i naziva ga digitalno mesto krivičnog dela u kojem se primenjuju tehnike istrage fizičkog mesta krivičnog dela. Ovaj model može biti primenjen kako na zvaničnu istragu tako i na korporacijsku istragu. Mesto zločina predstavlja okruženje (fizičko ili virtuelno), dok incident predstavljaju protivpravne aktivnosti koje za posledicu imaju reakciju interventnog ili forenzičkog tima. Ovaj model sastoji se iz 17 podfaza organizovanih u pet faza :

1. Pripremna faza - Ova faza podrazumeva obezbeđivanje neophodne infrastrukture i operacija koje su u stanju da u potpunosti podrže proces istrage, jer dokazi i fizički i digitalni mogu biti izgubljeni, ukoliko se na adekvatan način nisu prikupljali i čuvali. Ova faza podrazumeva i dve podfaze : **faza operativne spremnosti** (u daljem tekstu FOS) i **faza infrastrukturne spremnosti** (u daljem tekstu FIS).

- **FOS** podrazumeva postojanje neophodne obuke i opreme za lica uključena u forenzičko istraživanje, kao na primer obuke interventnog tima za odgovor na incident, obuke forenzičkih laboratorijskih analitičara kao i lica koja primaju inicijalne izveštaje o incidentnoj radnji. Sva oprema (koja će biti upotrebljena na mestu krivičnog dela i ona iz forenzičkih laboratorija) koja će biti korišćena u digitalnoj forenzičkoj istrazi, mora da bude ispravna, održavana i tehnološki najsavremenija.
- **FIS** osigurava postojanje potrebnih podataka kako bi se izvršila potpuna istraga i odnosi se na one koji održavaju okruženje koje može biti meta kriminalnih aktivnosti odnosno mesto krivičnog dela. Od fizičkih primera ovde spadaju, instaliranje i raspoređivanja video kamera ili čitača kartica za snimanje potencijalnih fizičkih mesta krivičnih dela. Digitalni primeri ove faze podrazumevaju slanje log fajlova sa servera na određeni zaštićeni "log server", sinhronizovanje satova na serverima sa NTP serverom, heširanjem kritičnih izvršnih fajlova sa MD5 ili sa SHA kao vid osnovnog tipa zaštite.

2. Razvojna faza – Značajna je za uspostavljanje mehanizama za detektovanje i potvrđivanje incidenta. Zadaci koje se u ovoj fazi obavljaju razlikuju se od tipa istrage odnosno, da li je angažovan zvanični istražni tim ili korporacijski istražni tim. Ova faza podrazumeva dve podfaze :

- **Podfaza detekcija i obaveštavanje** - Podrazumeva detektovanje incidentne radnje i obaveštavanje nadležnih odnosno ovlašćenih lica. To može da podrazumeva različite načine obaveštavanja, kao na primer upućivanje poziva na 92, alarm mrežnog sistema za detekciju napada, a može doći i od strane ljudi koji istražuju ilegalne aktivnosti na mreži.
- **Podfaza potvrda i autorizacija** - Cilj ove faze je dobijanje ovlašćenja da se u potpunosti istraži incident i mesto krivičnog dela. U zavisnosti od tipa istrage ova faza ima svoj različit razvoj. Kada je u pitanju zvanična istraga, ova podfaza podrazumeva dobijanje naloga za pretres potkrepljeno dovoljnim dokazima. Kada je u pitanju korporacijska incidentna radnja, nisu potrebni nalozi za pretres, ukoliko nije došlo do kršenja prava privatnosti ili ukoliko slučaj ne prevazilazi kapacitete korporacijskog istražnog tima (na primer međunarodni incident, zahtev za prisluškivanje telefonskog aparata). U slučaju neovlašćenog upada u server, angažuje se interventni tim kao odgovor na incidentnu radnju koji preduzima potrebne aktivnosti kako bi proverili da li je sistem kompromitovan i to nadgledanje mreže u potrazi za sumnjivim aktivnostima, pretraživanje po sistemu, radi pronalaženja malicioznih programa, i/ili malicioznih alata. Bitno je naglasiti da, ukoliko se analiza sprovodi "uživo", prema sistemu se treba odnositi kao prema mestu krivičnog dela uz minimalan uticaj na sistem. Ukoliko se potvrdi da se desila incidentna radnja, neophodno je odobrenje nadležnih za preduzimanje daljih aktivnosti[97].

3. Faza istrage fizičkog mesta krivičnog dela [98] - U ovoj fazi se vrši prikupljanje i analiza fizičkih dokaza i vrše se rekonstrukcija događaja koji su doveli do incidentne/protivpravne aktivnosti. Kao najvažniji cilj digitalne forenzičke istrage je identifikovanje učinioca protivpravne aktivnosti ili incidentne radnje, a za to je neophodno postojanje fizičkih dokaza. Kada je u pitanju zvanična istraga, istražitelj fizičkog mesta krivičnog dela, odgovoran je za izvršenje većeg broja zadataka koji će biti navedeni. Kada je reč o korporacijskoj istrazi, te zadatke će vršiti interventni tim za odgovor na računarski incident ili tim za fizičku bezbednost. Sastoji se od 6 podfaza :

[97] Ukoliko se radi o serverima gde je vreme aktivnog rada kritično za kompaniju, odobrenje mora da se dobije od strane izvršnog nivoa kompanije.

[98] Faza istrage fizičkog mesta krivičnog dela, odvija se paraleleno sa fazom istrage digitalnog mesta krivičnog dela, a dobijeni rezultati iz istrage digitalnog mesta krivičnog dela koriste se u istrazi fizičkog mesta krivičnog dela.

- **Podfaza očuvanje** - Ova faza je ista za svaki tip protivpravne aktivnosti. Podrazumeva, osiguranje izlaza, pomoć povređenima, zadržavanje osumnjičenih kao i identifikovanje svedoka. Kada je reč o digitalnom incidentu, fizičko mesto zločina trebalo bi da se osigura koristeći iste procedure kao kod fizičkog incidenta. Ako je reč o istrazi vezanoj za upad u server, ova faza podrazumeva identifikaciju osobe iz računarskog centra i sprečavanje drugih lica da uđu u centar iz mogućeg razloga da je neko od zaposlenih odgovoran za incidentnu radnju. Ova podfaza ne čuva konkretne dokaze, već u stvari vrši očuvanje fizičkog mesta krivičnog dela od bilo kakvih izmena da bi se mogli prikupiti i identifikovati dokazi.
- **Podfaza pregled** - Podrazumeva opservaciju fizičkog mesta krivičnog dela od strane istražnog organa kao osoba koja prva odgovara na incident. U ovoj fazi vrši se identifikovanje delova fizičkih dokaza kao i osetljivih delova fizičkih dokaza (koji moraju brzo da se sakupe i dokumentuju da bi se izbeglo oštećenje), uz razvijanje hipoteze o protivpravnoj aktivnosti. Kada je reč o digitalnom incidentu, primeri bi bili sledeći : identifikacija fizičkih dokaza (broj računara, lokacija računara, koje mrežne konekcije poseduju računari, mobilni telefoni, optički mediji (CD-Rom, DVD-Rom, Blue ray), eksterni prenosni uređaji, moguće šifre iz beleški. Akviziciju dokaza (prikupljanje) neophodno je da izvrši digitalni forenzičar specijalista za računare. Uključen računar se smatra osetljivim dokazom jer se digitalni dokazi koji na njemu postoje mogu lako uništiti sa udaljenog sistema. Zato su obavezne standardne procedure, kao na primer, isključivanje računara sa mreže, pre nego što se započne potpuna forenzička istraga.
- **Podfaza dokumentovanje** - Podrazumeva fotografisanje, skiciranje i video snimanje mesta krivičnog dela i fizičkih dokaza. Glavni cilj ove faze je da se prikupi i zabeleži što više mogućih informacija i detalja na fizičkom mestu zločina, da bi se sačuvali raspored i važni detalji. Kada je reč o digitalnom incidentu vrši se fotografisanje i dokumentovanje računarskih konekcija kao i samo stanje računara. Od značaja može biti i dokumentovanje broja i veličine hard diskova i RAM memorije, dokumentovanje MAC adresa, mrežnih adaptera sa računara na osnovu kojih je moguće identifikovati sistemske i mrežne aktivnosti iz DHCP logova. Takođe je preporuka da se dokumentuju i serijski brojevi računara ili neki drugi tagovi na računarima. S obzirom da forenzičke laboratorije ne mogu da dobiju originalni fizički hardver na analizu, veoma je važno da se u ovoj fazi dokumentuje što više detalja koji su u vezi sa fizičkim dokazima, što će biti od velike koristi za analizu i kasniju rekonstrukciju.
- **Podfaza akvizicija** - Podrazumeva temeljnu pretragu i prikupljanje dodatnih fizičkih dokaza sa fizičkog mesta krivičnog dela. Pretraga može biti orijentisana prema nedostajućim delovima fizičkih dokaza kao na primer oružje, a može da bude metodična sa striktnim šablonima pretrage jer svaki tip dokaza podrazumeva specifične standardne procedure o načinu akvizicije. Kada je reč o digitalnom incidentu ova podfaza podrazumeva pretragu za dodatnim medijima i digitalnim uređajima na mestu zločina. Može uključivati i kontaktiranje mrežnog ili sistem administratora sa ciljem obezbeđivanja i dobijanja informacija iz log fajlova o pristupu sistemu, updatu sistema, firewall-u, antivirusa, sistema za detektovanje upada na sistem - IDS, i iz drugih specifičnih logova. Svi fizički prikupljeni dokazi sa mesta krivičnog dela, šalju se u forenzičke laboratorije radi analize, a njeni rezultati će se koristiti u narednoj podfazi. Ukoliko se računarski sistem smatra za fizički dokaz, on će se konfiskovati kao dokazni materijal. Procedura akvizicije mora biti dokumentovana u smislu, na koji način se prikupljaju osetljivi podaci sa sistema koji je aktivan i na koji način isključiti računar.
- **Podfaza rekonstrukcija** - Podrazumeva razvijanje teorije o protivpravnoj aktivnosti na osnovu organizovanja rezultata analize prikupljenih iz fizičkih i digitalnih dokaza

i fotografija i video snimaka sa mesta krivičnog dela. Uključuje korišćenje naučnih metoda u radu sa dokazima da bi se proverila razvijena teorija o protivpravnoj aktivnosti. U slučaju digitalne protivpravne aktivnosti, rezultati istrage digitalnog mesta krivičnog dela su u korelaciji sa fizičkim dokazima da bi se osumnjičeni povezao sa digitalnim događajima. Na primer, aktivnosti u ovoj podfazi mogu da povežu aktivnosti kompromitovanog servera sa aktivnostima na radnoj stanici (npr kućnom računaru) osumnjičenog preko logova na jednom i na drugom sistemu ili preko logova sa mrežnih uređaja od strane Internet servis provajdera. Efikasnost ove faze zavisi upravo od angažovanja dobrih eksperata iz digitalne forenzike koji mogu da povežu događaje iz više izvora digitalnih dokaza.

- **Faza prezentacije** - Podrazumeva prezentovanje fizičkog mesta krivičnog dela i digitalnih dokaza zajedno sa teorijom o učinjenoj protivpravnoj aktivnosti sudu ili rukovodstvu korporacije.

4. Faza istrage digitalnog mesta krivičnog dela - Za početak ove faza smatra se momenat kada su digitalni uređaji prikupljeni kao fizički uređaji sa fizičkog mesta krivičnog dela ili kada se počne sa analizom sačuvanog mrežnog saobraćaja radi obezbeđivanja dokaza. Računarski sistem se posmatra kao mesto zločina i pretražuje se radi prikupljanja dokaza. Svrha ove faze je da se identifikuju elektronski događaji koji su se desili na sistemu da bi se prezentovali istražitelju fizičkog mesta krivičnog dela. Trebalo bi napomenuti da postoji interakcija istrage fizičkog mesta krivičnog dela, sa istragom digitalnog mesta krivičnog dela. To znači da se rezultati ove faze prenose u istragu fizičkog mesta krivičnog dela. Svaki digitalni uređaj se posmatra kao posebno fizičko mesto krivičnog dela i rezultati dobijeni iz analize svakog digitalnog uređaja prosleđuju se podfazi istrage fizičkog mesta krivičnog dela. Takođe, vrši se rekonstrukcija da bi se identifikovale veze između digitalnih uređaja. Fizička mesta krivičnih dela kao i digitalna mesta mogu biti organizovana u primarna i sekundarna mesta, što omogućava analizu različitih tipova uređaja na različitim mestima [110]. Na primer, server na koji je izvršen upad bio bi primarno mesto zločina, a log server koji je bio kasnije kompromitovan zbog izmene log fajlova koji su u vezi sa upadom, posmatrao bi se kao sekundarno digitalno mesto zločina. Podfaze istrage digitalnog mesta krivičnog dela, uglavnom obavljaju forenzički specijalisti, obučeni za rad sa forenzičkim alatima i tehnikama za digitalnu analizu. Ove podfaze su sledeće :

- **Podfaza očuvanje** - Očuvanje digitalnog mesta krivičnog dela podrazumeva obezbeđivanje izlaza i ulaza digitalnog mesta krivičnog dela uz očuvanje osetljivih digitalnih dokaza (dokazi koji se lako mogu izmeniti ili nestati). Podrazumeva korake kao što su izolovanje sistema od mreže, prikupljanje osetljivih podataka (dokazi koji se lako mogu izmeniti ili nestati) koji se mogu izgubiti prilikom isključivanja sistema, identifikovanje sumnjivih procesa na sistemu. Takođe je neophodno i evidentiranje svih ulogovanih sumnjivih korisnika na sistemu. Obratiti posebnu pažnju na log datoteke koji predstavljaju svedoke događaja i njih posebno obezbediti ukoliko postoji pretnja njihovog brisanja pre kreiranja forenzičkih kopija. Neki od modela ovu fazu očuvanja podrazumevaju kao čuvanje digitalnih dokaza, dok ovaj model podrazumeva očuvanje kompletnog digitalnog okruženja. U ovoj fazi pravi se kompletna forenzička kopija fizičkog sistema (mirror) na forenzičkom računaru, čime se realizuje očuvanje kompletnog digitalnog mesta krivičnog dela, što predstavlja jednu veliku prednost nad fizičkim svetom - lako kopiranje digitalnog okruženja. Ove forenzičke kopije sadrže celolupno digitalno mesto krivičnog dela za razliku od običnog bekapa koji čuvaju samo dodeljene podatake (eng. allocated) u digitalnom mestu krivičnog dela. U zavisnosti od tipa istrage originalni hard disk može da bude čuvan kao fizički dokaz sve do okončanja postupka, a može posle postupka replikacije biti vraćen u produkciju, ako su u pitanju kritični sitemi. Isto tako, kada se izvši snimanje mrežnog saobraćaja, postiže se efekat čuvanja neizmenjenog stanja mreže.

- **Podfaza pregled** - U ovoj fazi pronalaze se očigledni delovi digitalnih dokaza koji odgovaraju tačno određenoj vrsti protivpravne aktivnosti. Preporuka je da se ova faza realizuje u forenzičkoj laboratoriji, jer se u njoj može postići jedino kontrolisano. Ukoliko to situacija nalaže, ova faza može da se izvršava i na kompromitovanom sistemu "uživo", ali bi u svakom slučaju bilo neophodno napraviti forenzičku kopiju sistema, da bi se digitalni dokazi mogli ponovo prikupiti i u kontrolisanim uslovima. Ponekad se ova faza izvodi i direktno na terenu da bi se utvrdilo da li je potrebno da se sistem donosi na punu forenzičku analizu i u tom slučaju sistem se podiže u sigurnom okruženju pomoću butabilnog DVD/CD/floppy diska/diskete, da bi digitalni dokazi ostali nepromenjeni. Na primer, ukoliko se radi o dečijoj pornografiji istražni organi će prikupiti sve grafičke slike sa sistema i identifikovaće one koje bi predstavljale potencijalne dokaze. Ukoliko se radi o neovlašćenom upadu na server, istražni organi će tražiti očigledne znakove rootkit instalacija, exploite, pregledali bi se logovi aplikacija i vršila bi se pretraga za novim konfiguracionim datotekama. U nekim drugim slučajevima mogu se vršiti analize keša Internet pretraživača i njegove istorije. U zavisnosti od veštine osumnjičenog, za protivpravne aktivnosti istražitelji će izvršiti procenu potrebnih tehnika koje će primeniti u istrazi. Moguće je i dodatno konsultovanje ili angažovanje eksperata iz kriptografskih oblasti, eksperata za oporavak podataka (ukoliko su određeni podaci obrisani ili nestali), eksperata iz digitalne forenzičke analize .
- **Podfaza dokumentovanje** - Podrazumeva pravilno dokumentovanje pronađenih digitalnih dokaza. Forenzička kopija sistema dobijena u toku podfaze Očuvanje ima istu ulogu kao i fotografija ili video snimak fizičkog mesta krivičnog dela. Svaki deo digitalnog dokaza koji je pronađen u toku analize forenzičke kopije (mirror) originalnog sistema, mora biti jasno i precizno dokumentovan. Digitalni dokazi u računarskom sistemu mogu postojati na različitim nivoima apstrakcije pa moraju biti dokumentovani u skladu sa tim [24]. Na primer, fajl može biti dokumentovan, koristeći njegovu punu putanju i puno ime, može biti određena klasterima na fajl sistemu koje fajl koristi ili sektorima na disku koje fajl koristi. Mrežni podaci mogu biti dokumentovani izvornom i ciljnom adresom na različitim mrežnim nivoima. Da bi se na sudu dokazao integritet digitalnih dokaza obavezna je primena kriptografske heš funkcije kao na primer MD5 ili SHA-1[99], nad dokazima da se dobije heš vrednost koja dokazuje integritet [136]. Tri su pravila kada je reč o forenzičkom hešu. Prvo pravilo je, da se ne može predvideti heš vrednost fajla ili drajva, ne postoje dva heša koja se odnose na isti fajl odnosno drajv, ukoliko se bilo šta promeni u fajlu ili drajvu heš vrednost se mora promeniti. Da bi dokazi mogli da se koriste na sudu u ovoj fazi vrši se kreiranje lanca neprekidnog očuvanja integriteta i nadzora nad dokazima (eng. chain of custody).
- **Podfaza akvizicija** - Predstavlja vremenski najzahtevniju fazu, podrazumeva detaljnu digitalnu forenzičku analizu sistema, radi pretrage i prikupljanja digitalnih dokaza. Koristi rezultate iz faze Pretraga da bi tipski fokusirala analizu. Analogno je fotografisanje, uziman je otisaka prstiju, uzoraka krvi ili šara guma sa mesta zločina. Kao u fizičkom svetu, nepoznato je koji će se podaci koristiti kao digitalni dokaz pa je cilj ove faze da se sačuvaju sve digitalne vrednosti [26]. Nealocirani prostor na fajl sistemu jeste predmet analize, jer može sadržati obrisane fajlove. Prikupljeni mrežni saobraćaj programom za snimanje mrežnog saobraćaja, takođe može biti predmet analize. U zavisnosti od okolnosti, pretraga može biti usmerena na pregledanje sadržaja svakog klastera (što se smatra fizičkom pretragom) ili svakog fajla (što se smatra logičkom pretragom) [127]. Tehnike za analizu digitalnog mesta krivičnog dela kao i alata biće prikazani u posebnom poglavlju.

[99] SHA-1 predstavalja unapređenu verziju heš algoritma razvijenu od strane National Institute of Standards and Technology (NIST)

- **Podfaza rekonstrukcije** - Ova faza koristi naučne metode da bi se testirali dokazi i na osnovu toga odbacili bi se neodgovarajući digitalni dokazi. U ovoj fazi se konstatuje na koji je način digitalni dokaz dospeo na mesto izvršenja protivpravne aktivnosti i šta predstavlja njegovo prisustvo. Ukoliko određeni digitalni dokaz nedostaje, faza Pretrage nastaviće da identifikuje dodatne dokaze. Na primer, ukoliko je reč o upadu na server, ova faza može dovesti u vezu iskorišćavanje ranjivosti određenih servisa sa rootkit instalacijom uz korišćenje mrežnog sniffera.
- **Podfaza prezentacija** - Ova faza podrazumeva prezentovanje pronađenih digitalnih dokaza fizičkom istražnom timu (ukoliko postoje posebni istraživački timovi fizičkih i digitalnih mesta krivičnih dela), jer rezultate iz digitalne istrage ovaj tim koristi (integrišući rezultate istrage iz svakog digitalnog mesta krivičnog dela) u fazi Rekonstrukcije. U većini slučajeva fizički i digitalni tim za istragu su isti, pa se informacije lakše razmenjuju između članova tima.

5. Kontrolna faza - Predstavlja fazu pregleda stanja istrage sa ciljem identifikovanja oblasti koje bi mogle da se poboljšaju. Kada je reč o digitalnoj protivpravnoj aktivnosti, podrazumeva se procena uspešnosti izvršene fizičke i digitalne istrage zajedno, kao i svaka ponaosob, kao i da li postoji dovoljno fizičkih i digitalnih dokaza da bi se slučaj rešio. Ukoliko rezultat nije pružio očekivane rezultate, može buti primenjena neka nova procedura ili nova obuka.

Glavni cilj svih ovih navedenih modela jeste da se proizvede dovoljno dokaza koji će biti adekvatni i prihvatljivi za sud. Ne postoji univerzalni okvir digitalne istrage, pa se može uočiti da se izneti modeli uglavnom oslanjanju jedni na druge ili izmenama ili dopunama prethodnih modela, a neki od njih imaju veoma slične pristupe. Razlike se mogu uočiti i prema fokusu samog modela u smislu da li je skoncentrisan na određenu fazu digitalne istrage [99][100]. Prilikom digitalne istrage uvek odabrati upotrebljiv i fleksibilan model (nezavisan u odnosu na trenutnu tehnologiju) koji se može primeniti na sve aktuelne visokotehnološke kriminalne aktivnosti (odnosno dovoljno opšti) i one koje mogu da se dese u bližoj budućnosti. Takođe, model koji bi bio odabran mora biti zasnovan na postojećoj teoriji fizičke istrage, što u praktičnom smislu podrazumeva sprovođenje istih koraka koje sledi stvarna istraga. Model mora biti i dovoljno apstraktan i primenjiv, kako na zvanični tip istraga, tako i na korporacijiski tip i da obuhvata računarske incidente . U takve modele spadaju model Casey i model Carrier i Spafford.

[100] Michael Kohn , JHP Eloff and MS Olivier, Framework for a Digital Forensic Investigation, dostupno http://mo.co.za/open/dfframe.pdf, 03.01.2012

2.3 DIGITALNA FORENZIKA

Kao odgovor na visokotehnološki kriminal javila se potreba za razvojem nove naučne discipline koja će se njime baviti, kao i regulisanje pravnih osnova vezanih za uspešno procesuiranje krivičnih dela iz ove oblasti.

Digitalna forenzička istraga predstavlja proces koji korišćenjem naučnih metoda i tehnologije, razvija i testira teorije kroz hipoteze, analizirajući digitalne uređaje, koji predstavljaju relevantan dokaz u sudskom postupku. Cilj takve istrage je da se utvrdi istina o protivpranoj aktivnosti i svih okolnosti u vezi sa počiniocem i načinom izvršenja krivičnog (prekršajnog dela). Digitalni dokaz u tom slučaju predstavlja digitalni objekat koji sadrži pouzdane informacije koje podržavaju hipotezu ili je opovrgavaju[71].

Kada je reč o elementima računarskog i Internet kriminala, njih predstavljaju protivpravne aktivnosti počinilaca zajedno sa okolnostima pod kojima je to delo počinjeno.
Kako bi se učinjena nezakonita dela dokazala i njihovi počinioci procesuirali i sankcionisali, potrebno je primeniti procedure digitalne forenzike kao naučne discipline sa izuzetno značajnom praktičnom primenom.
Upravo digitalna forenzika kao relativno nova naučna disciplina (uspostavljena 1999. godine od strane IECO - International Organization on Digital Evidence) obezbeđuje jedini pouzdani alat za istragu računarskog kriminala, akviziciju i analizu digitalnih podataka i pripremu i prezentaciju digitalnih dokaza pred sudom [130]. U slučaju da je došlo do zloupotrebe IKT sistema, odnosno računarskog kriminala ili potrebe za upravljanjem računarskim incidentom, administrativnih zahteva ili civilne parnice, odgovore će nam dati digitalna forenzika koja podrazumeva otkrivanje (pretraga, istraga) i sakupljanje (akviziciju), čuvanje (upravljanje), dokazivanje (analizu) i ekspertsko svedočenje/veštačenje (prezentaciju) digitalnih dokaza pred sudom [130].

Tradicionalna forenzika (forenzička obrada različitih vrsta protivpravnih postupanja) nije imala adekvatan odgovor na sve prisutniju vrstu kriminala vezanu za računarske sisteme, odnosno kriminala koji se odvija na globalnoj mreži zvanoj Internet. Upravo je digitalna forenzika ta naučna disciplina koja može ponuditi relevantan dokaz odnosno digitalni dokaz. Fantastičan razvoj IKT-a postavlja velike izazove pred digitalne forenzičare koji moraju imati permanentnu i svakodnevnu edukaciju kako bi bili za korak ispred počinioca koji sprovode protivpravne aktivnosti (one aktivnosti koje su u suprotnosti sa propisima) u digitalnom okruženju.

Brzina tehnološkog razvoja uticala je na razvijanje ove mlade naučne discipline, koja zajedno sa paralelnim razvojem drugih nauka, primenjuje nove metode koje utiču na brzinu, i jednostavnost prikupljanja čvrstih dokaza, istražuje anti-forenzičke aktivnosti, sa ciljem da otkrije istinu u vezi sa učinjenom protivpravnom radnjom.

Upravo takva složenost problema na koju forenzičari nailaze, uslovil je i specijalizovanje stručnjaka za različite oblasti. U taksonomiji digitalne forenzike, a u odnosu na predmet forenzičke istrage, digitalnu forenziku možemo podeliti na: *forenziku računarskih sistema, forenziku mobilnih uređaja, forenziku baza podataka i forenziku računarske mreže uključujući i Internet ili kibernetičku forenziku*[101]. Ovaj rad se bazira na digitalnoj forenzici računarskih sistema pod Windows i Linux okruženjem.

Treba istaći da je za digitalnog forenzičara od presudne važnosti praćenje i razvoj informacionih tehnologija. Ponekad su razlike u operativnom sistemu ili verziji nekog programa od suštinskog značaja. Zato je bitno postojanje profilisanosti digitalno forenzičkih eksperata prema stručnoj oblasti (operativni sistemi, baze podataka, mrežni sistemi kao i profilisanje prema drugim IKT sistemima).

[101]Albert J. Marcella, Robert S. Greenfield, Cyber Forensics, CRC Press LLC 2002 strana 317

Digitalna forenzika ima široku primenu i to od policijsko-sudskih i vojno-obaveštajnih aktivnosti, civilnog i bankarskog sektora i osiguravajućih društava do kompanija različitih profila. Svi ovi entiteti moraju biti izuzetno oprezni sa podacima kojima raspolažu, jer u protivnom može biti prouzrokovana nemerljiva šteta zbog industrijske špijunaže, zloupotrebe IKT sistema, ali i nekih drugih oblika protivpravnih postupaka. Procena je, da šteta od različitih delovanja visokotehnološkog kriminala, ne uzimajući u obzir njegove potencijalne veze sa organizovanim kriminalom, na godišnjem nivou iznosi oko 200 milijardi dolara[102].

Najveći deo računarske forenzike odnosi se na forenziku računarskih sistema, što predstavlja i predmet ovog rada. Digitalna forenzika računarskog sistema obuhvata naučno ispitivanje i analizu podataka sa čvrstih diskova, fajl sistema, i prostora za skladištenje podataka unutar računarskog sistema, tako da se podaci mogu koristiti kao neoborivi i čvrsti dokazi pred sudom [137][138].

Prema dr Vulfu (H.B. Wolfe) računarska forenzika predstavlja metodičan niz tehnika i procedura za prikupljanje dokaza iz računarske opreme i drugih uređaja za skladištenje podataka i digitalnih medija, koji mogu biti predstavljeni sudu u adekvatnoj i smislenoj formi.

Stiv Hejli (Steve Haily) iz Cybersecurity instituta, računarsku forenziku posmatra kroz postupke dobijanja, očuvanja, identifikacije, tumačenja i dokumentovanja računarskih dokaza prema propisanim pravilima, pravne procese, postupak očuvanja integriteta dokaza, činjenična izveštavanja o pronađenim informacijama kao i pružanje stručnog mišljenja pred sudom u vezi sa pronađenim dokazima.

Na osnovu navedenih definicija može se zaključiti da računarska forenzika podrazumeva upotrebu unapred definisanih procedura i tehnika za detaljno ispitivanje računarskog sistema, a sa ciljem dobijanja relevantnih digitalnih dokaza.

Često u literaturi može da se pronađe poistovećivanje digitalne forenzike računarskog sistema sa procesom oporavka podataka. Ovo je samo delimično tačno. Digitalna forenzika oporavlja podatke koje je korisnik (maliciozni) namerno sakrio ili izbrisao, za razliku od slučajno izgubljenih ili izbrisanih, što kao krajnji cilj ima da se obezbedi validnost oporavljenih podataka za dokaze pred sudom. Forenzičari računarskih sistema, sledeći strogo definisana pravila, prikupljaju medijume (čvrste diskove i sve druge sekundarne medije za skladištenje podataka) za koje sumnjaju da se na njima nalaze digitalni dokazi, osiguravaju ih od bilo kakvih promena, i iz velike količine digitalnih podataka moraju pronaći relevantne i održive dokaze. Vrše analizu, kako bi rekonstruisali aktivnosti koje su vršene na njima i pripremili razumljiv izveštaj koji će moći poslužiti za vođenje sudskog procesa ili interne istrage u kompaniji. Takođe, procedura upravljanja i oporavka podataka posle destruktivnog vanrednog događaja podrazumeva korišćenje digitalno forenzičkih tehnika i alata za oporavak izgubljenjih podataka sa hard diskova. Računarska forenzika igra veliku ulogu u praćenju potencijalnih počinilaca protivpravnih aktivnosti. To se postiže u najopštijem smislu identifikacijom protivpravne aktivnosti, prikupljanjem dokaza, izgradnjom "lanca nadležnosti nad digitalnim dokazima", analizom dokaza, prezentovanjem pronađenih dokaza, svedočenjem i sve to u okviru vođenja sudskog postupka protiv okrivljenog. Digitalni dokazi mogu biti oslobađajući, optužujući ili da ukazuju na osnovanu sumnju.

2.3.1 Uloga računara u kriminalnim aktivnostima

U periodu od 1994. do 1998. Godine, Ministarstvo pravde Sjedinjenih Američkih država (eng. *US Department of Justice* - USDOJ) kreiralo je skup kategorija i na osnovu njih niz

[102]Dragan Prlja, Sajberkriminal, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, 28.12.2008, dostupno na http//www.prlja.info/sk2008.pdf

vodiča koji se odnose na pretragu i zaplenu računara. Ono što je bitno napomenuti je, da su se kroz pomenuta dokumenta definisale kategorije u kojima se pravi razlika između informacije i hardvera kada su u pitanju dokazi. Naime, hardver se posmatra kao elektronski dokaz, a informacija kao digitalni dokaz. Ova distinkcija je veoma važna sa aspekta dokaznog stanovišta kao i razvoja različitih procedura. U ovom kontekstu informacije se posmatraju u formi programa i podataka koji su smešteni na računaru, dok se pod hardverom podrazumevaju sve fizičke komponente računarskog sistema. S obzirim da kategorije nisu međusobno isključive, neka kriminalna aktivnost može da pripada u više kategorija. Kategorije koje navodi CCIPS (The Computer Crime and Intellectual Property Section kategorije su sledeće [103]:

1. Hardver kao dokaz (*Hardware as Evidence*).
2. Hardver kao instrument kriminalne aktivnosti (*Hardware as an Instrumentality*).
3. Hardver kao zabranjeni materijal ili plod kriminalne aktivnosti (*Hardware as Contraband or Fruits of Crime).*
4. Informacija kao dokaz (*Information as Evidence*).
5. Informacija kao instrument kriminalne aktivnosti (*Information as an Instrumentality*).
6. Informacija kao plod kriminalne aktivnosti (*Information as Contraband or Fruits of Crime*).

Ministarstvo pravde Sjedinjenih Američkih Država je 2002. godine ažuriralo dokument, tako da je u skladu sa današnjom tehnologijom i zakonom prerastao u Uputstvo za "Pretragu i zaplenu računara i pribavljanje elektronskih dokaza u krivičnom istragama" (eng. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" [104])[45]. Veliku zaslugu u kreiranju dokumenta ima, profesor Pravnog fakulteta univerziteta Džordž Vašington, Orin S. Kerr koji je zajedno sa svojim kolegama, advokatima, timom iz CCIPS (Computer Crime and Intellectual Property Section), tužilaštvom SAD-a kao i specijalistima iz FBI-a ali i iz drugih saveznih organa, bio angažnovan na izradi ovog Uputstva. Razlika između vodiča i uputstva je ta, što se informaciji i hardveru pridaje ista važnost, dok se kod uputstva pridaje veći značaj informacionom delu. Ukoliko hardver sam po sebi ne predstavlja dokaz, instrument ili plod kriminalne aktivnosti onda se on posmatra kao skladište za podatke [34]. Uputstvo ukazuje na to, da čak i ako je sama informacija bila meta kriminalne aktivnosti, može biti neophodno da se zapleni hardver iz različitih razloga. S obzirom da svaka od navedenih kategorija podrazumeva jedinstvene zakonske procedure koje se moraju poštovati, ovo Uputstvo treba da bude konsultovano od strane istražitelja, tužioca i advokata odbrane. U daljem tekstu biće navedene karakteristike kriminalnih aktivnosti za svaku od navedenih kategorija.

Henry Lee, profesor forenzičke nauke na univerzitetu New Have i direktor "Forensic Research and Training Center" ističe, da paralelno sa istražnim fazama digitalni dokazi prolaze kroz svoje faze [110]. Prva faza je faza prepoznavanja (eng. recognition), odnosno izjednačavanje mesta pronalaženja dokaza sa mestom izvršenog zločina. Navedeno prepoznavanje vrši se tokom izvođenja istražnih radnji prikupljanja dokaza (faza istraživanja i pretraživanja). Druga faza je identifikacija (eng. identification) u kojoj se pregledaju i upoređuju klasne karakteristike dokaza sa poznatim uzorcima da bi se utvrdila klasa konkretnog dokaza. Poslednja faza je individualizacija (eng. individualization), gde se pregledaju individualne karakteristike predmetnog dokaza, da bi se odredilo da li je predmetni dokaz jedinstven u odnosu na druge dokaze u okviru klase ili da utvrdi da li predmetni dokaz potiče iz predmetnog izvora izvršenja krivičnog dela, kao i ostali dokazi. Kada su računari u pitanju, teško je izvršiti individualizaciju digitalnog dokaza u istoj meri

[103] http://www.irational.org/APD/CCIPS/toc1.htm#IV, 15.12.2011
[104] http://www.justice.gov/criminal/cybercrime/searching.html, 15.12.2011

kao što se to može uraditi sa fizičkim dokazom, zato što su digitalni objekti generisani instrukcijama kod kojih se može javiti i element slučajnosti.

Hardver kao instrument kriminalne aktivnosti[105]

U slučaju da je hardver odigrao značajnu ulogu u kriminalnoj aktivnosti, onda se on smatra instrumentom kriminalne aktivnosti. Ova diferencijacija je veoma bitna zbog slučajeva kada je hardver korišćen kao oružje u kriminalnoj aktivnosti (na primer poput pištolja ili noža), što može dovesti i do dodatnih optužbi ili uvećanja kazne. Dobar primer hardvera kao instrumenta kriminalne aktivnosti, može da bude hardver koje napravljen isključivo za svrhu kriminalne aktivnosti kao na primer, snifer (eng. sniffer) uređaj koji je posebno dizajniran da prisluškuje mrežu. Ovaj tip uređaja se koristi za prikupljanje velikog broja osetljivh informacija, koje se posle mogu zloupotrebiti kao što su šifre, privatni podaci, brojevi bankovnih računa ili kartica, hardverske adrese računara, IP adrese računara i druge informacije koje mogu napadaču pomoći da kompromituje bezbednost računarskog sistema.

Svrha zaplene instrumenta kriminalne aktivnosti je da se spreče buduće kriminalne aktivnosti. Ukoliko se ne može dati argument da je hardver imao "značajnu" ulogu instrumenta u kriminalnoj aktivnosti, onda se ne bi trebalo vršiti njegova zaplena, a tu odluku donose sudovi. Slučajevi iz prakse :

a. U New York-u severni okružni sud, u vezi sa slučajem dečije pornografije, odlučio je da je računar bio instrument za krivično delo. Razlog je taj što je računar imao mogućnost slanja i primanja slika. (United States of America v. Michael LAMB, 1996. [106])
b. U Virdžiniji istočni okružni sud odlučio je da je računar bio instrument krivične aktivnosti zato što je posedovao fajl koji je detaljno opisivao uzgajanje biljke marihuane. (United States v. Real Property 783 F.Supp. 253, 1991. [107])

Hardver kao zabranjeni materijal ili plod kriminalne aktivnosti[108]

Ilegalni materijal (zabranjeni materijal, eng. Contraband), odnosno imovina, je ona imovina koju obični građanin ne sme posedovati u svom vlasništvu. Na primer, pod određenim uslovima, nelegalno je da građanin u svom posedu ima uređaj koji služi za presretanje elektronskih komunikacija[109]. Razlog je što ovi uređaji mogu da omoguće pojedincima da dođu do poverljivih informacija presretanjem mrežnog saobraćaja, kršeći privatnost drugih građana, čime se otvara mogućnost činjenja širokog spektra mnogih drugih kriminalnih aktivnosti. Drugi primer bi bio oprema za kloniranje mobilnih telefona kao i sami klonirani telefoni kao plod kriminalne aktivnosti. Prema tome, plod kriminalne aktivnosti i njeno posedovanje predstavljaju vlasništvo koje je dobijeno kriminalnom aktivnošću kao na primer, ukraden hardver (npr. lap-top) ili kupljen hardver ukradenom kreditnom karticom.

Hardver kao dokaz kriminalne aktivnosti[110]

Ova posebna kategorija kriminalnih aktivnosti hardver, kao dokaz, ne pripada ni grupi hardvera kao instrumenta kriminalne aktivnosti, ni grupi hardvera kao zabranjenog materijala ili ploda kriminalne aktivnosti. Na primer, ako se skener ili štampač koristi za falsifikovanje dokumenata ili novca ili poštanskih marki, i ukoliko poseduju jedinstvene karakteristike

[105] Opisano prema Eoghan Casey-u [34].
[106] http://securitylaw.info/pdf/945_F_Supp_441.pdf, 16.12.2011
[107] http://www.leagle.com/xmlResult.aspx?xmldoc=19911036783FSupp253_11003.xml&docbase=CSLWAR2-1986-2006
[108] Opisano prema Eoghan Casey-u [34].
[109] Primer se odnosi na Sjedinjene Američke države 18 USCS 2512, 16.12.2011
[110] Opisano prema Eoghan Casey-u [34].

skeniranog ili odštampanog dokumenta (na primer novca, slike, poštanske marke) koje povezuju hardver sa tim dokumentima, taj uređaj (hardver) može da se zapleni kao dokaz.

Informacija kao instrument kriminalne aktivnosti[111]

Informacija može da bude instrument kojim je izvršena kriminalna aktivnost ili ukoliko je ona dizajnirana sa ciljem da se koristi kao sredstvo za izvršenje kriminalne aktivnosti. Dakle, svi programi koji se koriste za izvršenje kriminalnih aktivnosti predstavljaju instrumente kriminalne aktivnosti. Različiti tipovi programa mogu biti iskorišćeni za različite kriminalne aktivnosti kao njihovi instrumenti, tako da neki programi na primer, mogu da omoguće neovlašćeni pristup računarskom sistemu, neki mogu da snimaju korisničke šifre prilikom logovanja na računarski sistem, neki od njih mogu da se koriste za razbijanje zaštita (šifara), primera ima mnogo. Ovi programi poznatiji su po imenu eksploiti (eng. exploits) i upotrebljavaju se sa ciljem da se zloupotrebi ranjivost[112] (eng. vulnerability) nekog operativnog sistema (servisa, programa ili programskog koda), a time i omogući sprovođenje neke kriminalne aktivnosti. Samo u slučaju da se prikaže da je informacija imala značajnu ulogu u kriminalnoj aktivnosti, može da se zapleni kao instrument kriminalne aktivnosti, u suprotnom se ne konfiskuje.

Informacija kao zabranjeni materijal ili plod kriminalne aktivnosti[113]

Kao što je ranije pomenuto za hardver, zabranjen materijal može da bude i informacija koju obični građanin ne sme da poseduje. Najčešća forma informacije koja nije dozvoljena za posedovanje je program za šifrovanje. U određenim zemljama nije dozvoljeno posedovati program koji omogućava jake algoritme za šifrovanje (odnosno ograničena je dužina ključa koji se koristi za šifrovanje ili tip algoritma). Razlog je taj, što bi to kriminalcima omogućilo zaštićenu komunikaciju i veliku privatnost. To za posledicu može imati sledeći scenario : pronađeni inkriminišući dokazi koji su neophodni za uspešnu tužbu su šifrovani, a ukoliko ne mogu da se dešifruju ti podaci, kao posledica dolazi do odbacivanja slučaja usled nedostataka dokaza. Drugi oblik gde se informacija javlja kao plod kriminalnih aktivnosti su slike dečje pornografije, nelegalne kopije računarskih programa, ukradene poslovne tajne (industrijske, trgovačke), šifre ili bilo koje druge informacije dobijene iz kriminalnih aktivnosti.

Informacija kao dokaz[114]

Ovo je najbogatija kategorija od svih pomenutih. Mnoge naše dnevne aktivnosti ostavljaju digitalne tragove. Svi pružaoci usluga (na primer Internet servis provajderi, telefonske kompanije, banke, kreditne institucije), prikupljaju informacije o svojim klijentima. Ovi podaci mogu otkriti veoma važne informacije kao što su vreme aktivnosti pojedinca i njegovo kretanje (kao na primer, vreme kupovine u marketu, iznajmljivanje automobila, kupovina goriva, elektronska naplata putarine, online bankarstvo i kupovina, telefonski pozivi, slanje elektronske pošte, itd..). Sve te informacije mogu se naći u log fajlovima pomenutih pružaoca usluga. Zapisi o komunikaciji telefonom mogu da se nabave od mobilnog operatera, (početak i kraj razgovora, vreme, broj telefona koji je pozvan ili broj primljenog poziva, njihovi jedinstveni identifikatori i jedinstveni identfitkatori uređaja kao na primer, IMEI broj i drugi podaci). Zapisi o posećenoj web stranici mogu se naći na serveru kao i podaci o adresama računara koji su pristupali pomenutoj web stranici na serveru, od Internet servis provajdera mogu se dobiti podaci o vremenu i lokaciji sa koje je osumnjičeni

[111] Opisano prema Eoghan Casey-u [34]
[112] Ranjivost se definiše kao postojanje slabosti usled projektovane ili implementirane greške koja može dovesti do neočekivanog i/ili neželjenog događaja odnosno do ugrožavanja bezbednosti sistema, izvor http://en.wikipedia.org/wiki/Vulnerability_%28computing%29, 21.04.2012
[113] Opisano prema Eoghan Casey-u [34]
[114] Opisano prema Eoghan Casey-u [34]

pristupao web stranici. Ono što je važno reći je, da su ove informacije u slučaju kriminalnih aktivnosti izuzetno dragocene, jer mogu dokazati njihovu vezu sa potencijalnim učiniocem kriminalnih aktivnosti ili dokazati nečiju nevinost[115].

U Americi aktom Computer Assistance Law Enforcement (CALEA)[116] od 2000. godine, telekomunikacione kompanije moraju držati detaljne liste poziva svojih klijenata na neodređeno vreme. U Evropskoj uniji od 2006. godine na osnovu direktive (Directive 2006/24/EC[117]) države, članice, su u obavezi da čuvaju specifične telekomunikacione podatke definisane Direktivom, od 6 meseci do 2 godine[118]. U Srbije je 2010. godine usvojen Zakon o elektronskim komunikacijama, prema kojem pružalac komunikacionih usluga mora da čuva podatke o elektronskim komunikacijama 12 meseci[119]. Kao i svaka medalja tako i ova vrsta nadzora ima svoje dve strane, dobre i loše. Dakle, dobra strana je što te informacije mogu da pruže dokaze u vezi sa kriminalnim aktivnostima, a loša je što iste mogu da se zloupotrebe kao i što se time ugrožava privatnost građana [23]. S tim u vezi, potrebno je naglasiti da se u velikom broju zemalja još uvek vode velike polemike, vezane za ovu vrstu čuvanja informacija, po pitanju vremena i vrste podataka zbog ugrožavanja privatnosti (u ovom slučaju privatni život i privatna komunikacija) koja je zagarantovana zakonom odnosno članom 12 Univerzalnom deklaracijom o ljudskim pravima kao i ustavnim pravom. U svakom slučaju se mora postići dobar balans između dovoljne sigurnosti, sa jedne strane i privatnosti, sa druge, i na tome se mora još dosta raditi.

2.3.2 Digitalna forenzička istraga

Digitalna forenzička istraga podrazumeva prikupljanje činjenica i njihovu proveru, nakon čega se formira hipoteza i vrše njena testiranja kroz traženje dokaza koji mogu da je potvrde ili opovrgnu, što može da utiče i na menjanje zaključaka, ukoliko se pronađu novi dokazi (što bi izazvalo i novi ciklus obrade dokaza). Centralno mesto u digitalnoj istrazi predstavlja neki digitalni uređaj koji je predmet ili sredstvo nezakonitog postupanja. Digitalni uređaj može biti (zlo)upotrebljen sa ciljem osumnjičenog da putem Interneta (iz)vrši određene pripreme krivičnog dela ili vršenjem neke digitalne aktivnosti u virtuelnom okruženju koja je u suprotnosti sa pozitivnim propisima (važeći propisi određene nacionalne države ili međunarodni propisi ratifikovani od strane države koja procesuira krivično delo u sudskom postupku) ili opštim aktima pravnog lica [120](na primer neovlašćen pristup računaru, posedovanje i distribucija nedozvoljenog materijala, različiti tipovi zloupotrebe mailova - ucene pretnje...). Identifikacijom (iz)vršenja nedozvoljene aktivnosti od strane nadležnih organa, isti, iniciraju istragu u pretkrivičnom postupku. Digitalna forenzička istraga se generalno može podeliti u dve različite kategorije : zvanična istraga i korporativna istraga.

Kada je reč o zvaničnoj istrazi, ona obuhvata istragu o sredstvima odnosno alatima sa kojima je učinjena protivpravna aktivnost, utvrđuje se motiv protivpravne aktivnosti i definiše se tip protivpravne aktivnosti i procesuira ga. Zvanične istrage vode zvanični istražni organi koji čine tim sa tačno označenim rukovidiocem istrage i zahtevaju sudske naloge. Pitanje zvanične istrage reguliše se Zakonikom o krivičnom postupku "Sl. glasnik RS", br. 72/2011, 101/2011, 121/2012, 32/2013 i 45/2013. U članu broj 2, se definišu osnovni pojmovi kao što je osumnjičeni, okrivljeni, optuženi, itd... "Osumnjičeni" je lice prema kome je zbog postojanja osnova sumnje da je učinilo krivično delo nadležni državni organ u predistražnom postupku preduzeo radnju propisanu ovim zakonikom i lice protiv koga se

[115] Odnosno dokaz može biti optužujući ili oslobađajući.
[116] http://www.justice.gov/criminal/cybercrime/usamay2001_4.htm
[117] http://en.wikipedia.org/wiki/Directive_2006/24/EC, 17.12.2011
[118] Mada u praksi ima odstupanja. Ne pridržavaju se sve članice striktno te direktive, neki od primera su Nemačka Švedska.
[119] http://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html, 17.12.2011
[120]Pod uslovom da su isti usklađeni sa pozitivnim propisima.

vodi istraga. "Okrivljeni" je lice protiv koga je podignuta optužnica koja još nije potvrđena, ili protiv koga je podnet optužni predlog, privatna tužba ili predlog za izricanje mere bezbednosti obaveznog psihijatrijskog lečenja, a glavni pretres ili ročište za izricanje krivične sankcije još nije određeno, odnosno izraz koji služi kao opšti naziv za osumnjičenog, okrivljenog, optuženog i osuđenog. "Optuženi" je lice protiv koga je optužnica potvrđena i lice za koje je povodom optužnog predloga, privatne tužbe ili predloga za izricanje mere bezbednosti obaveznog psihijatrijskog lečenja, određen glavni pretres ili ročište za izricanje krivične sankcije u skraćenom krivičnom postupku. Krivično gonjenje je definisano članom 5. Krivično gonjenje započinje:

1) prvom radnjom javnog tužioca, ili ovlašćenih službenih lica policije na osnovu zahteva javnog tužioca, preduzetom u skladu sa ovim zakonikom radi provere osnova sumnje da je učinjeno krivično delo ili da je određeno lice učinilo krivično delo;

Članom 7. je definisan način pokretanja krivičnog postupka. Krivični postupak je pokrenut:

(1) donošenjem naredbe o sprovođenju istrage (član 296.);
(2) potvrđivanjem optužnice kojoj nije prethodila istraga (član 341. stav 1.);
(3) donošenjem rešenja o određivanju pritvora pre podnošenja optužnog predloga u skraćenom postupku (član 498. stav 2.);
(4) određivanjem glavnog pretresa ili ročišta za izricanje krivične sankcije u skraćenom postupku (član 504. stav 1, član 514. stav 1. i član 515. stav 1.);
(5) određivanjem glavnog pretresa u postupku za izricanje mere bezbednosti obaveznog psihijatrijskog lečenja (član 523.). Zakon stavlja u nadležnost javnom tužiocu da goni počinioca krivičnih dela, pa je to regulisano članom 43. Osnovno pravo i osnovna dužnost javnog tužioca je gonjenje učinilaca krivičnih dela.

Za krivična dela za koja se goni po službenoj dužnosti, javni tužilac je nadležan da:

(1) rukovodi predistražnim postupkom;
(2) odlučuje o nepreduzimanju ili odlaganju krivičnog gonjenja;
(3) sprovodi istragu;
(4) zaključi sporazum o priznanju krivičnog dela i sporazum o svedočenju;
(5) podiže i zastupa optužbu pred nadležnim sudom;
(6) odustane od optužbe;
(7) izjavljuje žalbe protiv nepravnosnažnih sudskih odluka i da podnosi vanredne pravne lekove protiv pravosnažnih sudskih odluka;
8) preduzima druge radnje kada je to određeno ovim zakonikom.

Kod korporativne forenzičke istrage odgovor na incident izvodi jedna osoba i uglavnom spadaju u istrage niskog nivoa ili ne spadaju u protivpravne aktivnosti već u incidentne radnje. Ona se može smatrati i kao predistražni postupak zvanične istrage visokotehnološkog kriminala. Istraga u organizaciji se sprovodi u kontrolisanom okruženju. U praksi se realizuje kroz pokretanje istrage, utvrđivanje karaktera računarskog incidenta i analiziranje prikupljenih podataka. Treba napomenuti, da se prikupljanje i prosleđivanje digitalnih dokaza zvaničnim organima istrage, odnosno organima u organizaciji, vrši jedino prema odobrenju vlasnika kompromitovanog sistema i odluci organizacije. I zvanična i korporativna istraga slede ista forenzička pravila.

Bitno je istaći, da, nije svaka incidentna aktivnost i protivpravna aktivnost. Postoje različiti pojavni oblici incidentnih radnji i neke od njih predstavljaju i protivpravne aktivnosti što za sobom povlači i zvaničnu istragu. Na osnovu pojavnih oblika incidentnih radnji i protivpravnih aktivnosti, prikazanih u najvećem delu relevantne literature, moguće je izvršiti njihovu klasifikaciju prema stepenu značajnosti (ozbiljnosti) na sledeći način : nizak nivo ,

srednji nivo i visoki nivo značajnosti baš kao što je izloženo u EC-Council i Cengage learning, literaturi za serfifikaciju za računarskog forenzičara (eng. Computer hacking forensics investigator certification CHFI) [58]. Detaljnija klasifikacija sa više kategorija definisana je u Federal Incident Reporting Guidelines od strane US-Cert-a[121]. Kod nas se klasifikacija težine krivičnih dela definiše opisom bića krivičnog dela u Krivičnom zakoniku Srbije.

FBI za kvalitativnu procenu rizika i zaštitu federalnog informacionog sistema, predlaže i koristi gradaciju: *nizak-N, srednji-S, visok-V* u tzv. bezbednosnoj kategorizaciji. Na primer, ako neka informacija ima sledeću procenu rizika: poverljivost – **N**, integritet - **S** i raspoloživost – **V**, onda ovu informaciju svrstavamo u kategoriju visoko rizičnih, što znači da će i preduzete mere zaštite biti najveće.Ovaj metod je prihvatljiv, jer istovremeno anulira veliki broj neodređenosti koje kvalitativna procena rizika uključuje.

Incidenti niskog nivoa značajnosti nose najmanje opasnosti, ali se moraju rešavati u toku radnog dana nakon njegove detekcije. Zahtevaju odgovor u roku od 90 minuta, a rešavanje može biti i do 6 sati. Na primer, u ovu kategoriju može spadati gubitak lične šifre, neuspešna skeniranja i pokušaji skeniranja mreže i presonalnih računara i servera, prisustvo računarskog virusa ili crva i pozajmljivanje računarskih naloga u okviru organizacije.

Incidenti srednjeg nivoa značajnosti su znatno ozbiljniji i uglavnom su inkriminisani propisanim odredbama zakona određene države na osnovu visine pričinjene štete. Zahtevaju odgovor u roku od 30 minuta a rešavanje do 4 sata.
Kod nas, težina krivičnog dela definisana je u Krivičnom zakoniku "Sl. glasnik RS", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009 i 121/2012. Neki od primera bi bili neovlašćeno skladištenje i obrada podataka, ilegalan pristup kancelarijama, uništavanje imovine pričinjena računarskim incidentom, krađa ličnih podataka, širenje računarskog virusa ili crva većeg inteziteta, neovlašćeno dobijanje privilegovanog pristupa računaru ili serveru. Kod nas, krivično delo oštećenje računarskih podataka i programa definisano je Članom 298. :

> (1) Ko neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program, kazniće se novčanom kaznom ili zatvorom do jedne godine.
> (2) Ako je delom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi četiristopedeset hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do tri godine.
> (3) Ako je delom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do pet godina.
> (4) Uređaji i sredstva kojima je učinjeno krivično delo iz st. 1. i 2. ovog člana, ako su u svojini učinioca, oduzeće se.

Incidenti visokog nivoa značajnosti takođe su inkriminisani propisanim odredbama zakona određene države, na osnovu visine pričinjene štete. Kod nas, za svako krivično delo, definisana je težina dela na osnovu štete koja je pričinjena, a takvih krivičnih dela ima dvadesetak vezanih za visokotehnološki kriminal i neka od njih data su u prilogu ovog rada (prilog 4.).

Kada je reč o protivpravnim aktivnostima visokog nivoa značajnosti, njih treba rešavati odmah nakon njihovog nastanka. Zahtevaju odgovor u roku od 15 minuta, a rešavanje do 2 sata. U ovu kategoriju spadaju DOS napadi, upad u računarski sistem ili mrežu, računarski virus ili crvi velikog intenziteta, trojanski konji ili zadnja vrata (eng. backdoor), neovlašćenja izmena hardverskih komponenti na računaru, neovlašćeno

[121] http://www.us-cert.gov/government-users/reporting-requirements.html, 21.04.2012

instaliranje firmware-a na računarskom sistemu ili neovlašćeno instaliranje programa na serveru. Član 212. definiše uništenje i oštećenje tuđe stvari :

(1) Ko uništi, ošteti ili učini neupotrebljivom tuđu stvar, kazniće se novčanom kaznom ili zatvorom do šest meseci.

(2) Ako je delom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi četiristopedeset hiljada dinara, učinilac će se kazniti novčanom kaznom ili zatvorom do dve godine.

(3) Ako je delom iz stava 1. ovog člana prouzrokovana šteta u iznosu koji prelazi milion i petsto hiljada dinara ili je delo učinjeno prema kulturnom dobru, zaštićenoj okolini nepokretnog kulturnog dobra, odnosno prema dobru koje uživa prethodnu zaštitu, učinilac će se kazniti zatvorom od šest meseci do pet godina.

(4) Za delo iz st. 1. do 3. ovog člana, ako je oštećena stvar u privatnoj imovini, gonjenje se preduzima po privatnoj tužbi.

Ilegalno prenošenje novca ili njegovo preuzimanje, ilegalni download zaštićenih materijala, kao na primer muzički fajlovi, video fajlovi, programi ili drugi fajlovi koji su zakonom zabranjeni, upotreba računara za čuvanje slanje i primanje dečije pornografije, kockanje ili kršenje bilo kog zakona određene države tumačiće se kao protivpravna aktivnost Članom 185 b. (Iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu).

Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala primenjuje se radi otkrivanja, krivičnog gonjenja i suđenja za:

(1) krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom;

(2) krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000 ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara;

(3) krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, koja se zbog načina izvršenja ili upotrebljenih sredstava mogu smatrati krivičnim delima visokotehnološkog kriminala, u skladu sa članom 2. stav 1. ovog zakona.

Period odgovora prema navedenim kategorijama, na incidentnu radnju, odnosno protivpravnu aktivnost i njihovo rešavanje varira u zavisnosti od velikog broja faktora kao na primer specifičnosti delatnosti organizacije, osetljivosti samih podataka, mogućnosti ponavljanja napada i mnogih drugih faktora. Predložena vremena u zavisnosti od tipa incidenta prikazana su u tabeli US-CERT-a[122].

Praksa je pokazala da se sve češće javlja potreba primene forenzičke istrage u korporativnom okruženju u vezi sa računarskim incidentima. Ove interne istrage u organizaciji imaju za cilj utvrđivanje tipa incidentne radnje, kao i trajno eliminisanje uzroka incidenta.

Treba napomenuti, da su principi i standardne operativne procedure digitalne forenzičke istrage gotovo isti kako u zvaničnoj, tako i u korporativnoj istrazi. Forenzički istražitelji istragu moraju voditi na takav način „kao da će slučaj koji se istražuje završiti na sudu“, tj. da će u nekoj od istražnih faza, za koju se utvrdi da forenzički istražitelji u organizaciji nemaju nadležnost, istraga morati predati zvaničnim organima. Sam intenzitet istrage može varirati, ali pristup izvorima dokaza kao i procedure očuvanja dokaza u lancu istrage, moraju biti isti u zvaničnoj i korporacijskoj istrazi [76].

Potrebno je istaći i značaj informacije o cilju napada ali i utvrditi eventualno postojanje uzročno-posledične veze (direktne ili indirektne) sa ostalim kumulativno

[122] http://www.us-cert.gov/government-users/reporting-requirements.html , 21.04.2012

počinjenim krivičnim delima kao što su na primer trgovina narkoticima, ljudima, oružjem, protivpravno sticanje imovinske koristi prevare, iznude, zloupotrebe službenog položaja i dr.

Digitalna forenzička istraga podrazumeva upotrebu različitih forenzičkih alata i tehnika, odnosno njihovu primenu u toku trajanja istrage. Primenjuje se u različitim slučajevima npr: kada treba da se postavi hipoteza o protivpravnoj radnji, zatim prilikom eliminisanja očiglednosti (npr. delo je nesumnjivo izvršeno sa određenog računara, ali to ne znači da je delo svakako izvršio vlasnik tog računara, već je moglo biti reči o upadu trećeg lica na taj računar i iskoristio ga za neku protivpravnu aktivnost), dalje, pri rekonstrukciji protivpravne radnje ili otkrivanja tragova osumnjičenog računara. Pored opisanih najvažnijih metodologija odnosno modela digitalne forenzičke istrage, u ovom radu, biće prikazan i veliki broj alata i tehnika koji mogu da se koriste u digitalnoj forenzičkoj istrazi nad računarima pod Windows ili Linux operativnim sistemom. Modeli koje možemo pronaći u literaturi se uglavnom razlikuju na osnovu ugla posmatranja krivičnog dela, a samim tim i njihova primenjivost može da varira. Postoje modeli istrage fizičkog mesta krivičnog dela, modeli digitalnog mesta krivičnog dela (koji se zasnivaju na postojećoj teoriji fizičke istrage) i integrisani modeli gde je računar sam po sebi digitalno mesto krivičnog dela, pa se teorija istrage fizičkog mesta krivičnog dela primenjuje na digitalnu forenzičku istragu. Istraga fizičkog mesta krivičnog dela koristi zakone prirode da bi našla fizičke dokaze, a istraga digitalnog mesta krivičnog dela ih koristi da bi pronašla digitalne dokaze [27].

Kada je u pitanju istraga fizičkog mesta krivičnog dela dominantna teorija je Lokardov zakon razmene [191]: Kada dva objekta dođu u interakciju (kontakt) doći će do razmene materije između njih. Primer dlake sa zločinca, vrlo često se zadrži na fizičkom mestu krivičnog dela. Kad je u pitanju digitalna mesto krivičnog dela, privremeni fajlovi, sadržaj RAM memorije koji je snimljen na disku i izbrisani fajlovi ili njegovi delovi, mogu postojati zbog uticaja programa odnosno Operativnog sistema koji je osumnjičeni koristio ili izvršavao. Prema tome, podatak koji uđe u digitalno mesto ostavlja tragove digitalnog dokaza iza sebe na različitim mestima : memorija, hard disk, prenosiva memorija. Što se tiče ključnih reči u literaturi ima mnogo različitih mišljenja kada je reč o najvažnijim forenzičkim pojmovima kada su u pitanju digitalno forenzički procesi. U literaturi postoji veliki broj definicija kada su u pitanju pojmovi iz digitalne forenzike i zbog toga će biti iznete one najvažnije za proces istrage :

- **-fizički dokazi** - predstavljaju fizičke objekte na osnovu kojih se može utvrditi izvršenje krivičnog dela, i koji mogu da dokažu vezu između počinioca krivičnog dela i žrtve, ili mogu da dokažu vezu između izvršioca zločina sa samim zločinom. Primer fizičkih dokaza : Računar, DVD-ROM, hard disk, mobilni telefon ;
- **-digitalni dokaz** - predstavlja digitalni podatak koji može potvrditi računarski kriminal i koji može da dokaže vezu između počinioca krivičnog dela sa samim krivičnim delom. Primer digitalnih dokaza : podatak na hard disku (na primer log fajl), u memoriji u mobilnom telefonu ;
- **-fizičko mesto krivičnog dela -** predstavlja fizičko okruženje u kome se nalaze fizički dokazi zločina. Okruženje gde se dogodila prva protivpravna aktivnost naziva se primarno fizičko mesto krivičnog dela, a sva ostala fizička mesta nazivaju se sekundarna fizička mesta krivičnih dela [110] ;
- **-digitalno mesto krivičnog dela -** predstavlja digitalno (virtuelno) okruženje kojeg čine sistemski program, programi i hardver u kome se nalazi digitalni dokazi protivpravne aktivnosti. Okruženje gde se dogodila prva protivpravna aktivnost naziva se primarno digitalno mesto krivičnog dela, a sva sledeća digitalna mesta nazivaju se sekundarna mesta digitalna mesta krivičnih dela ;

U današnje vreme, većina kompanija za svoj marketing i promociju koristi Internet, čime njihova izloženost postaje sve veća, a samim tim raste mogućnost od potencijalnih

napada i špijunaže (kao jednom od pojavnih oblika visokotehnološkog kriminala). Ukoliko dođe do određene incidentne situacije u okviru kompanije (koji nije bio pretnja po bezbednost države), takve istrage pre svega vode timovi koje kompanija angažuje. U tom slučaju pokreće se kompanijska istraga koja nema represivan karakter prema pojedincu-izvršiocu (u smislu njegovog lišavanje slobode), već može pribaviti dokaze za eventualno dalje postupanje nadležnih državnih organa. Istraga unutar kompanije može dovesti do pokretanja disciplinskog postupka u slučaju da se dokaže postojanje protivpravnog postupanja od strane zaposlenog.

Kada se steknu uslovi za sprovođenje zvanične istrage po dobijanju odobrenja, istraga počinje da se sprovodi fazno, ulaskom u trag izvršiocu ili osumnjičenom, otkrivanjem njegovog identiteta, i po potrebi lišavanjem slobode, kako bi se onemogućilo uništavanje dokaza ili ponavljanje istog dela, odnosno uticaj na potencijalne svedoke.

Sjedinjene Američke Države i druge države uspostavile su specijalizovane grupe radi istrage računarskog kriminala na nacionalnom nivou. Međutim zbog velike količine zahteva koji su pristizali ovim grupama, prevazišli su se postojeći resursi. Sledeći korak je bio kreiranje i razvoj regionalnih centara za procesiranje digitalnih dokaza. Međutim i ovi regionalni centri su takođe postali preopterećeni, što je za posledicu imalo kreiranje i razvoj jedinica za rukovanje digitalnim dokazima pri lokalnim agencijama reda i zakona. Ilustrativno bi to bilo prikazano na sledeći način : na incidentne situacije odgovaraju lica sa osnovnim veštinama prikupljanja i pregleda digitalnih dokaza i upravo ta lica na lokalnom nivou rešavaju većinu slučajeva. Ukoliko se radi o procesiranju komplikovanih slučajeva podrška stiže od strane regionalnih laboratorija. Kod najzahtevnijih slučajeva uključuju se nacionalni centri. Ovi centri sprovode istraživanja, a takođe razvijaju alate koji mogu da se koriste na regionalnim i na lokalnim nivoima.

Potreba za specijalizacijom u digitalno forenzičkoj oblasti je postala nužnost zbog munjevitog razvoja tehnologije i sajber kriminala. Prikupljanje digitalnih dokaza vrše tehničari digitalnog mesta zločina, ljudi koji pregledaju dokaze, i istraživači koji analiziraju sve raspoložive dokaze kako bi se izgradio slučaj. Ove specijalizacije ne odnose se samo na policiju već se uspostavljaju i na korporativnom nivou.

U slučaju da je jedna osoba angažovana i odgovorna za prikupljanje, procesiranje i analiziranje digitalnih dokaza, bitno je da se ovi postupci izvode posebno. Svaka od oblasti specijalizacije podrazumeva određene veštine kao i primenu različitih procedura. Treba istaći da je specijalizacija prema oblastima veoma bitna jer se time lakše definišu kako treninzi, tako i standardi iz tih oblasti.

2002. godine radna grupa za digitalne dokaze (SWGDE[123]) je objavila vodiče za trening "Najbolje prakse računarske forenzike"[124] [63]. Američko udruženje direktora laboratorije za zločine - ASCLD (eng. American Society of Crime Laboratory Directors) je predložilo zahteve za ljude koji pregledaju digitalne dokaze u forenzičkim laboratorijama (ASCLD 2003). To je bilo praćeno u 2005. godini objavljivanjem ISO 17025 standarda (Opšti zahtevi za kompetentnost laboratorija za ispitivanje i eteloniranje laboratorija (General requirements for the competence of testing and calibration laboratories) gde se pominje pregled digitalnih dokaza u kontekstu akreditovane discipline pod internacionalnim standardima (ISO 17025; ENFSI 2003).

Razvoj standarda iz ove oblasti je napravio potrebu za standardima prakse za individue. To znači, da bi se obezbedilo da ljudi koji pregladaju digitalne dokaze imaju sve potrebne veštine da obavljaju svoj posao kompetentno, kao i da prate ispravne procedure, razvijani su treninzi i programi sertifikacije prema pomenutim standardima. Glavna svrha je višenivoiska sertifikacija [71]:

[123]Scientific Working Group for Digital Evidence

[124]Best practices for Computer Forensics

1. Ispit opšteg znanja (koji svi moraju da prođu, uključujući i osoblje koje prvo odgovara na incident, a koje rukuje digitalnim dokazima) ;
2. Viši sertifikati za individue koje rukuju u mnogo kompleksnijim slučajevima u laboratorijskim uslovima.

U slučajevima bezbednosnih incidenata, pravilno prikupljanje relevantnih podataka može značajno povećati verovatnoću dolaska do informacija o tome ko je izvršilac napada, odakle je napad izvršen, na koji način je napad izvršen i sl.

2.3.3 Digitalni dokazi

Dokaz je ono što razdvaja hipotezu od neosnovane tvrdnje [184]. On može potvrditi ili oboriti hipotezu, pa je od izuzetne važnosti pitanje njegovog integriteta koji se može prihvatiti ili odbaciti pred sudom. Upravo zato je i veoma važan datum za digitalnu forenziku kao mladu naučnu disciplinu 1991. godina. Naime, u Portlandu (država Oregon), te godine je održano zasedanje Međunarodne asocijacije računarskih naučnika IACIS [125] gde je konstatovano i odlučeno da su „digitalni dokazi“ ravnopravni sa dokazima prikupljenim na tradicionalan način, odnosno fizičkim predmetima [118].

Prema SWGDE/IOCE [126] [127] standardu dokazi su klasifikovani u tri osnovne kategorije[48][128]:

- **digitalni dokaz** – informacija od značaja za krivični postupak koja se nalazi ili prenosi u digitalnom obliku;
- **fizički predmeti ili dokaz** – fizički medijum koji skladišti ili prenosi digitalnu informaciju;
- **digitalni podaci** – informacije od značaja za krivični postupak koje su povezane sa fizičkim predmetom;

Priznavanjem digitalnih dokaza kao ravnopravnih i prihvatljivih za sud, nastala je računarska forenzika kao deo forenzičke nauke, u čijem je fokusu obrada legalno pribavljenih dokaza pronađenih u računaru i na digitalnim medijima za čuvanje podataka.

Pod pojmom digitalnih dokaza prema definiciji IOCE u oblasti forenzičkih nauka, digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost i koja je ili uskladištena ili prenesena u takvom obliku. Prema tome digitalni dokaz obuhvata računarski uskladištene i generisane dokazne informacije, digitalne audio i video signale, digitalnu fotografiju, zapis sa digitalnog mobilnog telefona, informacije na digitalnim faks mašinama i informacije sa drugih digitalnih uređaja. Znači, digitalni dokaz je bilo koja informacija generisana, obrađivana, uskladištena ili prenesena u digitalnom obliku na koju se sud može osloniti kao merodavnom, kao i druge moguće kopije originalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije.

Digitalni dokaz je svaka informacija uskladištena, generisana ili prenesena u binarnoj (digitalnoj) formi, uključujući i njihovu odštampanu formu, koja obuhvata digitalne podatke: računara, digitalnog foto/audio/video/mobilnog telefona/faksa i drugih digitalnih uređaja, a koja ima dokazujuću vrednost na koju se sud može osloniti [74][73].

U nastavku biće navedene definicije nekoliko pojmova koji se često koriste kao sinonimi, što pri svakodnevnom korišćenju računara ne predstavlja problem, ali prilikom forenzičke analize njihovo razlikovanje je veoma značajno.

[125]IACIS – International Association of Computer Specialist
[126]Scientific Working Group on Digital Evidence (SWGDE) http://www.swgde.org/
[127]International Organization on Digital Evidence (IOCE) http://www.ioce.org/core.php?ID=1
[128]Michael cross, Scene of the Cybercrime, Second Edition, syngress, 2008, strana 628.

Originalni digitalni dokaz (eng. evidence media**)** je fizički predmet i/ili podaci sadržani u tom predmetu u vreme akvizicije (otkrivanja, prepoznavanja, izvlačenja) ili zaplene predmeta koje treba istražiti. Na primer, to mogu biti podaci snimljeni na računaru koji je fizički privremeno oduzet dok istraga traje sa ciljem dostavljanja tog dokaza sudu, po iniciranju sudskog postupka.

Duplikat digitalnog dokaza (eng. target media**)** je precizna digitalna reprodukcija svih objekata podataka sadržanih u originalnom fizičkom predmetu (HD, CD ROM-u, FD, memoriji, itd.).

Kopija digitalnog dokaza je precizna reprodukcija informacija koje su sadržane na originalnom fizičkom predmetu, nezavisno od originalnog fizičkog predmeta.[129]

Mesta na kojima digitalni forenzičari u praksi pronalaze potencijalne dokaze su sledeća :

- log fajlovi;
- konfiguracioni fajlovi;
- bekap fajlovi;
- artefakti fajl sistema;
- printer spool fajlovi;
- Internet kolačići;
- swap/page fajlovi;
- sistemski fajlovi;
- fajlovi sa istorijom;
- privremeni fajlovi;
- Internet bookmarks ;
- Internet omiljene lokacije;
- hibernacijski fajlovi;

Tipovima fajlova u kojima forenzičari pronalaze potencijalne dokaze su sledeći :

- fajlovi zaštićeni šifrom[130]
- skriveni fajlovi
- kompresovani fajlovi
- tabelarni fajlovi
- fajlovi baza podataka
- kalendarski fajlovi
- multimedijalni fajlovi (audio, video, grafički fajlovi)
- adresarski fajlovi
- fajlovi elektronske pošte

2.3.4 Prikupljanje podataka

Prikupljanje podataka moguće je realizovati forenzičkim odgovorom uživo tj. aktivnom (eng. *Live forensic*) ili post-mortem forenzikom, koja podrazumeva privremeno oduzimanje računarskog sistema, imidžovanje (uzimanje forenzičke slike bit po bit) elektronskih, optičkih i fleš diskova i akviziciju i analizu digitalnih podataka na radnom imidžu.

[129]Izvor: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/ , 01.11.2011

[130] Za uklanjenje šifri ili enkripcije sa fajlova koriste se za to specijalizirani alati. U praksi moguće je korišćenje Winhex editora za uklanjanje šifri sa fajla. Neki od specijaliziranih alata koji mogu oporaviti šifru ili je zaobići su Passware Kit Forensic (dostupno na http://www.lostpassword.com/kit-forensic.htm), i alati dostupni na sajtu http://www.password-crackers.com/en/category_117/ . Ukoliko je potrebno zaobići šifru za logovanje koristi se program ntpasswd ili ERD commander. LC4 može pogoditi šifre starijih NT sistema. Forenzički jedan od najmoćnih alata su PRTK i DNA kompanijie AccessData. Postupak oporavka zaštićenih fajlova jeste veoma kompleksan i spada u deo posebne forenzičke oblasti koja nije predmet ovog rada.

Digitalna forenzika "uživo" - podrazumeva prikupljanje podataka i analizu koja se sprovodi nad originalnim dokazima. S obzirom da je to momenat gde se spaja forenzika sa bezbednosnim elementima i zaštitom koja je jedan od tih elemenata, forenzički odgovor "uživo" biće predmet posebnog razmatranja u radu.

U post-mortem forenzičkom prikupljanju postoji nekoliko načina izrade kopija i duplikata digitalnog dokaza, uz pomoć specijalnih alata za te namene:

- **kopija** (eng. c*opy*) - uključuje samo informacije o datotekama iz fajl sistema, ne i o *slack* ili neiskorišćenom prostoru i nisu očuvane vremenske oznake. Prema tome, klasično kopiranje koje ne zadovoljava zahteve digitalno forenzičke istrage ;
- **rezervna ili mirror kopija** (eng. b*ackup*) - datoteke kopirane za buduću restauraciju sistemskih ili programskih podataka, služe kao sigurnosna kopija (na primer ISO image). Ovaj način očuvanja dokaza zasniva se na metodi kopiranja svih podataka na disk, što predstavlja mirror kopiju (eng. mirror image). Ova kopija može, ali i ne mora predstavljati identičnu kopiju originala, zbog toga što se ona najčešće koristi samo kao sigurnosna kopija (eng. *backup*), a u složenijim situacijama *mirror image* ne tretira se kao forenzička kopija. Ne zadovoljava sve zahteve digitalno forenzičke istrage.
- **forenzička kopija bitsream image** (bit-po-bit, sektor-po-sektor kopija, disk-to-file, disk-to-image*)* - ova kopija predstavlja egzaktnu repliku svih sektora. Predstavlja forenzički duplikat originalnog hard diska i rad na njemu se smatra kao rad na originalnom računaru. Zapravo, predstavlja napredniju metodu reprodukcije podataka kopirajući svaki bit, jedinice i nule, od početka do kraja (bez brisanja ili bilo kakve izmene nad podacima) medija u jedan logički fajl tj. imidž [146]. Takođe se kopiraju i slobodni (eng. free space) i nealocirani prostori na disku, zbog toga što se na njima često nalaze izbrisani podaci. Prave se obavezno dve forenzičke kopije – jedna radna i jedna referentna za dokazivanje integriteta ispitivanog hard diska pred sudom). Bitstream disk-to-image je i najčešće korišćena metoda u praksi. Najčešći alati kojima se prave forenzičke kopije su : EnCase[131], AccessData FTK[132], SMART[133], Sleuth Kit[134], iLook[135].
- **forenzička kopija bistream disk-to-disk** - Bitstream disk-to-disk, kao što samo ime sugeriše, replicira sadržaj medija (diska) direktno na drugi medijum (disk). Izvodi se kada nije moguće uraditi bitstream image kopiju. Prilikom izvođenja ovog postupka voditi računa o geometriji i CHS (Cylindar-Head-Sector) konfiguraciji diska na koga se kloniraju originalni podaci. Ovaj način zahteva postojanje medija sličnog originalu, forenzički čistog, sa većim kapacitetom nego originalni medijum [96]. Najščešći alati kojima se izvodi bitstream disk-to-disk su : AccessData FTK, EnCase, SafeBack[136], i Norton Ghost[137].

U slučajevima protivpravnih aktivnosti npr. bezbednosnih incidenata, pravilno prikupljanje relevantnih podataka može značajno povećati verovatnoću dolaska do informacija o tome ko je izvršilac, odakle je ili gde je izvršena protivpravna aktivnost i na koji način je ona izvršena.

Pre izvršenja forenzičke duplikacije digitalnih dokaza, veoma je važno da se digitalni forenzičar upozna sa podacima iz BIOS-a računarskog sistema koji je predmet istrage da bi

[131] http://www.guidancesoftware.com/encase-forensic.htm
[132] http://www.accessdata.com/
[133] http://www.asrdata.com/forensic-software/smart-for-Linux/, 02.03.2011
[134] http://www.sleuthkit.org/, 02.03.2011
[135] http://ilook-investigator.software.informer.com/, 02.03.2011
[136] http://www.forensics-intl.com/safeback.html, pristupljeno 02.03.2011
[137] http://us.norton.com/ghost/, 02.03.2011

odredio osnovnu geometriju hard diska[138] na kompromitovanom računaru i utvrdio but sekvencu (eng. boot sequince)[139] na njemu.

Ono što je bitno napomenuti jeste upotreba hardverskih ili programskih blokatora upisa (eng. write-blocker) tokom izvođenja bekapa ili bitstream repliciranja zbog očuvanja integriteta originalnog medijuma.

Kada je u pitanju forenzička duplikacija u literaturi su dominantni pristupi koji se uglavnom realizuju sa forenzičkim alatima AccessData FTK [140], Encase[141], Diskpro Clone-N-Recover[142], SafeBack[143], ASR Data SMART for Linux[144], DD za Linux[145] i DD za Windows[146]. U principu DD komanda je ugrađena u gotovo sve savremene forenzičke alate.

Nakon preuzimanja originalnog hard diska iz ispitivanog računara i njegovog povezivanja na forenzičku radnu stanicu sledeći korak jeste pravljenje slike (eng. image) originalnog hard diska koristeći pomenute forenzičke alate. Izuzetno je važno da se dokumentuju svi detalji vezani za hard disk kao što su serijski broj, pozicije džampera (eng. jumpers) na hard disku, vidljiva oštećenja i neke druge specifične karakteristike.

Drugi pristup jeste pravljenje slike hard diska (ili eksternog hard diska ili uređaja za skladištenje podataka) koja će biti preneta na forenzičku radnu stanicu putem zatvorene mreže ostvarene isključivo između ispitivanog uređaja i forenzičke radne stanice. Ove specijalne forenzičke mreže koriste su u slučaju masovnih istraga na više distribuiranih lokacija u kojima učestvuje više digitalnih forenzičkih istražitelja, za uzimanje imidža osumnjičenih računara na terenu i njihovo slanje u forenzičku laboratoriju. Ova veza može da se realizuje na osnovu point-to-point interfejsa između ispitivanog sistema i forenzičke radne stanice putem mrežnog sviča ili ukrštenim mrežnim kablom (cross-connect cable).

Koji god da se pristup primeni, obavezno koristiti programske[147] (slika 3.) ili hardverske blokatore upisa (eng. write blockers) na hard disk (slike 2.), a svaki preduzeti proces dokumentovati i uraditi čeksum MD5 i SHA-256 nad originalnim digitalnim dokazom i nad dobijenom slikom, jer je to jedini pouzdani način pred sudom da se dokaže integritet i autentičnost dobijenog digitalnog dokaza. Postoji veliki rizik da će doći do izmene podataka na USB uređaju (npr. eksternom hard disku) ukoliko se ne koriste programski ili hardverski blokatiori upisa kao standardna praksa između forenzičke radne sitanice i ispitivanog (povezanog) uređaja [176]. Ograničenja programskih blokatora upisa izložili su Menz i Bress u svom radu "*The fallacy of software write protection in computer forensics*" [126] kao i Carvey i Altheide u radu „Tracking USB storage: Analysis of Windows artifacts generated by USB storage devices" [29]. Bilo da se radi o programskim ili hardverskim blokatorima koristiti one koji su prihvatljivi od strane NIST organizacije[148].

Na Windows operativnom sistemu jedan od načina zaštita upisa na prenosive uređaje moguće je ostvariti uz pomoć regedit alata na sledeći način:

-„*Computer\HKEY_LOCAL_MACHINESYSTEM\CurrentControlSet\Control*"

-Dodati novi ključ i imenovati ga kao „*StorageDevicePolicies*" :

New→Key

---

[138] Dokumentovati postavke hard diska što podrazumeva evidentirati parametre vezane za maksimalni kapacitet, broj cilindara, glava i sektora ispitivanog hard diska.

[139] But sekvenca podrazumeva redosled pokretanja odnosno butovanja određenih uređaja na sistemu kao na primer floppy-cd-rom-network-pcmci-hard drive

[140] http://accessdata.com/products/computer-forensics/ftk, komercijalni alat, 02.03.2011

[141] http://www.guidancesoftware.com/forensic.htm, komercijalni alat, 02.03.2011

[142] http://www.e-mart.com/www/index.html, komercijalni alat, 02.03.2011

[143] http://www.forensics-intl.com/safeback.html, komercijalni alat, 02.03.2011

[144] http://www.asrdata.com/forensic-software/saw/, 02.03.2011

[145] http://Linux.about.com/od/commands/l/blcmdl1_dd.htm, open source alat, 02.03.2011

[146] http://www.chrysocome.net/dd, open source alat, 02.03.2011

[147] Primer za softverske blokatore je SAFE Block, http://www.forensicsoft.com/ Za svaki operativni sistme postoje posebno namenjena verzija.

[148] http://www.nist.gov/index.html, 03.03.2010

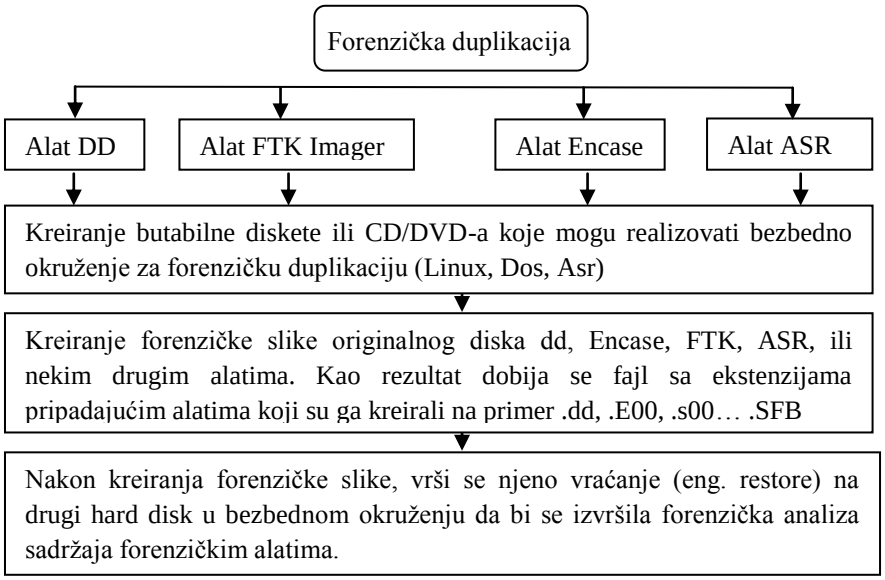
-Pod ključem „*StorageDevicePolicies*“ dodati nov DWORD podatak „*WriteProtect*“ : *New→DWORD*
-Podesiti vrednost za „*WriteProtect*“ na 1 čime će se omogućiti zabrana upisa na prenosive uređaje.

Pomenuta opcija zaštita upisa uz pomoć regedit alata, može biti od velike koristi administratorima sistema u korporativnim okruženjima u cilju suzbijanja curenja osetljivih informacija i širenja virusa na prenosive uređaje.

Slika 2. *Hardverski blokator upisa Agape SuperDrive Lock*[149]

Slika 3. *Blokator upisa softverski ForensicSoft SAFE Block*[150]

Na slici 4. je prikazana ilustracija postupka forenzičke duplikacije :



Slika 4. *Postupak forenzičke duplikacije*

Takođe treba naglasiti da forenzička duplikacija računarskih sistema može biti neadekvatna u određenim okolnostima u smislu previše potrebnog vremena i adekvatnosti u operativnom smislu kada je reč o prikupljanju podataka Na primer, dupliranje velikih terabajtnih diskova ili RAID diskova, ili prostora za skladištenje u *Cloud Copmuting* sistemima gde se čuvaju velike količine digitalnih podataka (tzv. *Big Data*, IBM). U ovakvim

[149] Izvor : http://www.agapeinc.in/visitforensicsite.php, 03.03.2010
[150] Izvor : http://www.forensicsoft.com/safeblock.php 03.03.2010

slučajevima uzimaju se selektivno imidži onih particija koje sadrže podatke navedene u osnovanoj sumnji za pokretanje istrage.

Zato je veoma važno da se digitalna forenzika kao naučna disciplina koristi sa ciljem što šire edukacije digitalnih forenzičara, u suprotnom mogu se, pojaviti veliki problemi oko prikupljanja relevantnih dokaza. Ovi dokazi su u većini slučajeva u apstraktnom obliku. Ti digitalni – apstraktni dokazi su uglavnom u binarnoj formi predstavljeni 0 i 1. Skup tih binarnih brojeva sačinjava niz kojim mogu da se opišu folderi, fajlovi koji mogu biti dokumenta, slike aplikacije. Ovi digitalni dokazi su izuzetno nestabilni (lako promenljivi, „isparljivi podaci“ eng. volatile), jer mogu da se lako uklone, izmene ili nestanu, što u dokaznom postupku može predstavljati veliki problem. Prema definiciji US-CERT[151] (The United States Computer Emergency Readiness Team) volatile podaci predstavljaju one podatke koji se čuvaju u memoriji, ili postoje u tranzitu a koji će biti izgubljeni kada računar ostane bez napajanja ili se isključi. Međutim, ti podaci mogu i da se sačuvaju ukoliko digitalni forenzičar pravovremeno odreaguje.

Izuzetno je važno da digitalni dokazi, koji se iznose pred sud, moraju biti u originalnom zapisu, tj. zabranjeno je eksperimentisanje, izmena ili testiranje nad njima dok traje istraga. Upravo zato služe kopije digitalnih dokaza nad kojima se mogu sprovoditi istražni postupci od strane digitalnog forenzičara i koji se ne iznose pred organe suda. Najčešće greške koje mogu da se jave prilikom prikupljanja podataka su sledeće :

- izmena vremenskih pečata (eng. timestamps)
- zaustavljanje zlonamernih procesa na računarskom sistemu
- instaliranje zakrpa na sistemu (eng. patching) pre izvršene istrage nad sistemom.
- neevidentiranje izvršenih komandi na sistemu
- korišćenje nepouzdanih komandi i binarnih fajlova
- upisivanje preko potrencijalnih dokaza u vidu instaliranja programa na originalnim dokaznim medijima (na primer hard disk) ili pokretanje ili izvršenje programa koji čuvaju svoje izlaze (eng. output) na originalnom dokazu.

Veoma važan proces u forenzičkoj istrazi jeste "kontinuitet dokaznog materijala" COC (eng. chain of custody - COC), a u literaturi se još može se naći i termini poput „lanac očuvanja integriteta dokaza“, „lanac očuvanja nadležnosti“ ili "lanac nadzora", koji predstavlja izuzetno važan proces kojim se prati kretanje dokaza kroz prikupljanje, čuvanje i analizu njegovog životnog ciklusa do momenta kada su prezentovani u sudskom postupku [179]. COC se odnosi na to ko je posedovao objekat i šta je sa objektom rađeno [188]. Ovim procesom se evidentira svaka osoba koja u nekom određenom momentu obrađuje dokaze, uključuje datum i vreme kada su prikupljeni, preneseni, razlog prenošenja, broj slučaja i broj dokaznog predmeta. To znači da svaki put, ukoliko se dokaz premešta od jedne osobe do druge ili sa jednog mesta na drugo to mora biti evidentirano. Prekid COC može dovesti u sumnju da je dokaz ili izmenjen ili zamenjen ili falsifikovan odnosno zloupotrebljen. Ono što se može uočiti kao problem jeste nemogućnost konstantnog prisustva jedne osobe koja prati dokazni materijal od njegovog prikupljanja sa lica mesta do njegovog prezentovanja na sudu. Praksa je pokazala da se to može prevazići kreiranjem potvrda iz forenzičkih laboratorija po prijemu dokaznog materijala na ispitivanje. Takođe, forenzičke laboratorije izdaju odgovarajuću potvrdu u momentu isporuke rezultata čime se obezbeđuje integritet dokaza. U slučaju kada se u proces uključuje i forenzička laboratorija, neophodno je i svedočenje forenzičara ili laboranta o tome na koji je način dokazni materijal skladišten i zaštićen u laboratoriji za vreme ispitivanja. Međutim, bolje rešenje može biti, ako se svaki pristup ispitivanom imidžu verifikuje uzimanjem heš vrednosti, koja mora biti istovetna kao originalna heš vrednost imidža. Nepodudaranje heš vrednosti sa originalnom u bilo kojem koraku istrage, znači prekid COC, što može dovesti u sumnju da je dokaz ili izmenjen ili zamenjen ili falsifikovan odnosno zloupotrebljen.

[151] http://www.us-cert.gov/

Pored digitalnih postoje i fizički dokazi koji mogu biti prikupljeni na incidentnom mestu i koji mogu imati dokazujuću vrednost u smislu da se na tom mestu nalazilo osumnjičeno lice. Takvi dokazi pružaju potvrdu o povezanosti određenog uređaja i osumnjičenog koji je sprovodio protivpravnu radnju.

Za opis incidenta pojedinačni dokazi se moraju kombinovati kako bi se izgradio čvrsti i neoboriv dokazni materijal pred sudom. Od izuzetne je važnosti da se svi originalni dokazi, deponuju u sefove ili da se čuvaju u skladištima za posebne namene, u zavisnosti od osetljivosti incidenta kao i da se uvede zabrana fizičkom pristupu mestu incidenta, svima osim digitalnim forenzičarima i ovlašćenim istražiteljima. Ove mere se preduzimaju da se ne bi ugrozio proces istrage (ovo je sa ciljem da bi se izbeglo slučajno ili namerno kompromitovanje ili uništavanje prikupljenih dokaza). U suprotnom može doći do uništenja dokaza a samim tim bi i uspeh kompletnog istražnog postupka bio ozbiljno doveden u pitanje. Osnovno pravilo je da svi dokazi moraju biti adekvatno dokumentovani, a lica koja njima pristupaju moraju imati utvrđenu odgovornost kada nad njima vrše ispitivanja.

Lica koja imaju mogućnost sprovođenja ispitivanja i izvođenja digitalnih dokaza možemo podeliti u tri kategorije, a to su:

1. Istražitelji - koristi veliki broj forenzičkih alata i tehnika, a uglavnom su zaposleni u nadležnim inspekcijskim i kontrolnim organima.
2. Profesionalci informaciono komunikacionih tehnologija – koriste mali broj forenzičkih alata i tehnika i to uglavnom iz njima stručne oblasti. Oni rade kao zaposleni u organizacijama. To su klasični informatičari u IT odeljenjima, kao što su administratori sistema i mreža, inženjeri mrežne infrastrukture, specijalisti zaštite-administratori zaštite računarskih sistema, administratori zaštite računarskih mreža, procenitelji rizika itd… Oni ipak koriste elementarne forenzičke alate – alate komandne linije (DOS komande ili Linux komande). U Win XP OS ima najmanje 100 DOS komandi koje se mogu aktivirati i koristiti kao odličan forenzički alat. To je i prva kategorija forenzičkih alata. Inače forenzički alat je sve što forenzičaru (*umetniku*) može polsužiti za otkrivanje digitalnog dokaza, kao što je u ratu sve oružje (kamen, štap itd.).
3. Timovi – koriste veliki broj alata i tehnika, imaju sposobnost da odgovore na širok spektar računarskih incidenata. Od specijalista zaštite i informatičara, pa i drugih lica iz organizacije (pravnik, za HR, za fizičko obezbeđenje) formiraju se timovi za upravljanje rizikom i upravljanje računarskim incidentom. Ovi timovi se angažuju po potrebi i nisu stalni. Svaki član tima obavlja redovne zadatke, a uključuje svoje kompetencije kad se zahteva – godišnja detaljna analiza rizika (obavezna prema ISO/IEC 27001 ISMS standardu) i u slučaju glavnog incidenta, kada je naneta šteta organizaciji). U oba tima mogu biti angažovani i profesionaci i pojedinci kao spoljni saradnici ili konsultanti).

Da bi sud priznao digitalni dokaz postoje određeni uslovi i procedure koje je neophodno ispuniti : analiza, čuvanje kao i ponovljivost kompletne procedure istrage, ukoliko to sud zahteva od digitalnog forenzičara.

Kada je reč o čuvanju dokaza, zahteva se poštovanje procedura da bi dokaz posedovao sve potrebne atribute. Ovi atributi u stvari opisuju elemente standardne operativne procedure digitalne forenzičke istrage.

Prvi element je naziv procedure, zatim sledi namena, tj. opis namene digitalnog dokaza, kada će se koristiti i ko će ga koristiti (ovo je vrlo značajno zbog preuzimanja odgovornosti da se neće uticati na dokaz kako istraga ne nalaže). Svaki digitalni dokaz mora pratiti opisana procedura u koracima i merama opreza pod kojima se digitalni dokaz koristio u istrazi. Osim atributa koji opisuju pomenute elemente, oni mogu opisivati i korake kod kojih se zahteva tačnost u istrazi tzv. kalibrisanje i opis korišćenih matematičkih operacija tzv. kalkulisanje.

Treba istaći vrlo važnu činjenicu, a to je da su oprema, materijal, kontrole i standardi pod kojima se ispituju digitalni dokazi, veoma bitni. Takođe, neophodno je opisati ograničenja sigurnost i reference same opreme i alata sa kojom se vrši ispitivanje.

Jedan od najčešćih principa koji su za sud prihvatljivi, a odnose se na digitalne dokaze je „Daubert princip“ koji pod svojim osnovnim kriterijumom podrazumeva primenu naučnog metoda od strane eksperta kako bi se izvršila proverljivost prezentovanih naučnih dokaza na sudu. Ovo je veoma važno zbog toga što podjednako važi za sve naučne, tehničke i inženjerske dokaze koji će biti predstavljeni sudu.

Izuzetno je bitno da digitalni dokazi sa osumnjičene mašine budu dobijeni ili prikupljeni forenzičkim alatima koji su prihvatljivi pred sudom. Isto tako, digitalne dokaze sud može verifikovati i ako je digitalni dokaz u obliku određenog fajla.

U svim sudskim postupcima u kojima se koriste digitalni dokazi isti moraju biti dobijeni ili izvučeni sa osumnjičene mašine zahvaljujući forenzičkim alatima, prema tačno definisanim procedurama.

Na primer u Sjedinjenim Američkim Državama 2004. godine odlučeno je da su merodavni forenzički alati AccessData FTK Imager i EnCase. Ovo su forenzički alati testirani na bagove u NIST[152]-ovoj laboratoriji za nepoznate softvere i prvi priznati u svetu od pravosudnih sistema na Zapadu. Koriste se u brojnim zemljama i drugi alati kao što su *Ilook-IX*[153] (FBI[154], SAD), *X-Way Forensic*[155] (NPIA[156], Engleska) , *Paraben*[157] (BKA[158], Nemačka), kao brojni alati na Linux platformama otvorenog koda. Brayan Carrier je promovisao priznavanje alata otvorenog koda u svojim radovima. Naše službe koje se bave digitalnom forenzikom koriste EnCase (prvi je naučno verifikovan sa preciznim brojem grešaka koje unosi u isipitivani digitalni materijal, a koje ne menjaju intergitet ispitivanog materijala), FTK Imager-om, ali i sa HELIX kompilaciojom alata, verzijom u kojoj se nalazi licenciran EnCase 4). Treba napomenuti da se priča o alatima mora prihvatiti fleksibilno. Ako forenzičar koristi bilo koji alat, i zna objasniti da li jeste ili ako jeste koje i kakve promene je izazvao na ispitivanim podacima, taj rezultat mora biti priznat na sudu, pod uslovom da vam druga strana na bilo koji način (ne uvek forenzički) ospori i obori dokaze i hipotezu. Kod nas sudija ne ulazi u prirodu alata – to može advokat suprotne strane, ako zna.

Zato u međunarodnoj sudskoj praksi koja je vezana za visokotehnološki kriminal, tipovi alata koji se primenjuju pri izvođenju dokaza mogu da variraju. Da bi forenzički alati bili prihvatljivi pred sudom, uslov je da imaju poznati stepen greške i moraju biti prihvaćeni od strane relevantnih naučnih krugova ili objavljeni u relevantnim naučnim časopisima.

2.3.5 Analiza prikupljenih podataka

Forenzička analiza podataka u opštem smislu može da se posmatra kao fizička i logička analiza. Fizička analiza izvodi se isključivo nad forenzičkom slikom. Podrazumeva pretraživanje stringova (eng. string), pretraživanje i raspakivanje (eng. extract) fajlova prema tipu fajlova i prema formatima, izdvajanje slek prostora i praznog prostora[159] i nealociranog prostora[160]. Dokazni tragovi - fragmenti informacija upravo se mogu naći u slobodnom ili

[152] http://www.nist.gov/index.html, 30.04.2012
[153] http://www.perlustro.com/, 30.04.2012
[154] Federal Bureau of Investigation, http://www.fbi.gov/, 30.04.2012
[155] http://www.x-ways.net/forensics/, 30.04.2012
[156] National Policing Improvement Agency,http://www.npia.police.uk/, 30.04.2012
[157] http://www.paraben.com/, 30.04.2012
[158]BKA odnosno , Federal Criminal Police Office, http://www.bka.de/, 30.04.2012
[159] Prazan prostor predstavalja deo fajl sistema ali koji nije dodeljen podacima.
[160] Nealociran prostor predstavlja prostor na hard disku koji nije dodeljen fajl sistemu.

slek prostoru. U daljem tekstu ovi prostori (slek, prazan i nealociran prostor) će biti detaljno razmatrani.

Logička analiza obuhvata analizu svakog fajla na svim particijama. Na primer mountovanje svake ispitivane particije u read-only modu pod Linuxom, exportovanje particije putem SAMBE do forenzičke radne stanice kao i ispitivanje svake datoteke odgovarajućim programom za pregled datoteka (eng. file viewer).
Tipične liste koje se kreiraju u prilikom analize podataka odnose se na posećene web sajtove, e-mail adrese kao i određene ključne reči.

Forenzička analiza podataka sa računarskih sistema podrazumeva pripremu podataka i samu analizu podataka. Priprema podataka podrazumeva izradu radnih kopija svih digitalnih dokaza koji mogu da se nalaze na različitim medijima, a nakon toga izvršiti statistiku podataka. Zatim se kreira lista postojećih fajlova na sistemu. Potom se radi oporavak obrisanih fajlova i nedodeljenog prostora. U okviru pripreme podataka potrebno je i proveriti potpis svakog fajla na sistemu i izvršiti identifikaciju onih fajlova kod kojih je promenjena ekstenzija (eng.. signature analysis) i identifikovati sve poznate sistemske datoteke.

Sama analiza podataka može da obuhvati veliki broj forenzičkih ispitivanja. Tu spada i izvlačenje (eng. extract) elektronskih poruka i atačmenta (eng. attachments), pregledanje istorije web pretraživača, pretraga prema kriterijumu relevantnih stringova (eng. strings), pregledanje instaliranih aplikacija, analiza instaliranih programa, identifikovanje i dešifrovanje zaštićenih fajlova, detaljan pregled fajl po fajl i analiza datuma i vremena sistema i relevatnih foldera i fajlova (eng. date/time stamp).

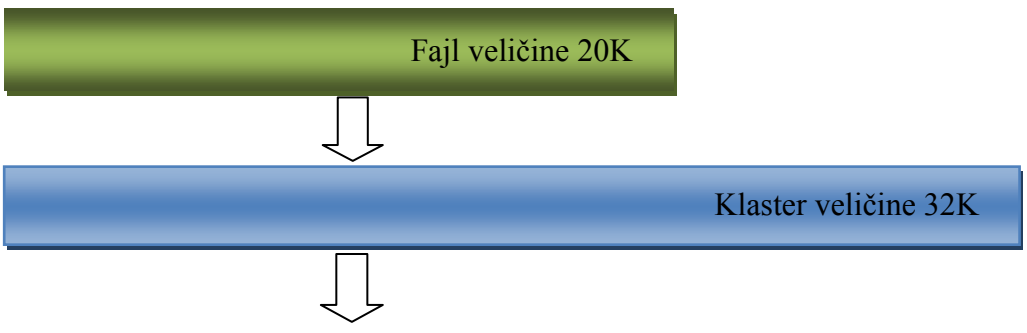
Izazov u ovoj fazi predstavlja mogućnost realizovanja brze forenzičke analize koja može da se ostvari kroz korišćenje najnovije tehnologije i primene specijalno obučenog kadra za protivpravne aktivnosti. Takođe, izazov mogu biti i veliki troškovi (koje bi trebalo predvideti u fazi pripreme za protivpravnu aktivnost) koji se odnose na generisanje podataka za digitalnu forenzičku istragu ili za internu istragu u organizaciji.

Pre nego što budu objašnjeni načini izrade kopija i duplikata digitalnog dokaza trebalo bi ukazati na određena mesta i njihove specifičnosti, koja mogu da sadrže dragocene informacije koje je potrebno analizirati nakon urađene duplikacije u post-mortem analizi. Prema tome, ukoliko je dobijeno dovoljno informacija koje potvrđuju da se protivpravna aktivnost dogodila, sledi odluka o izvođenju forenzičke duplikacije. Ta mestu su sledeća :

- slek prostor na disku (eng. slack space) ;
- slobodan ili nedodeljen prostor na disku (eng. free or unallocated space)
- loši sektori na hard disku (eng. bad sectors)

Na navedenim mestima se mogu naći veoma značajni podaci kada je u pitanju forenzička istraga pa će u daljem izlaganju biti objašnjeno šta predstavljaju ova mesta na hard disku.

Da bi se razumelo šta je to slek prostor na disku i kako se to odnosi na računarsku forenziku, najpre treba razumeti kako se disk organizuje na najnižem nivou. Diskovi su podeljeni u niz staza (eng. track). Ove staze su fabrički podeljene dalje na niz sektora. U jednom sektoru se upisuje 512B (bajta) podataka. Skup sektora, zavisno od veličine čvrstog diska, formira klaster. Neiskorišćeni deo prostora na hard disku u okviru klastera podrazumeva oblast, od kraja datoteke (koja popunjava deo klastera), do kraja klastera kao na slici 5. :



Slika 5. *Prikaz fajla, klastera i slek prostora*

Ono što treba da se primeti je da jedan fajl na Operativnom sistemu u Windows-u ima dve veličine, logičku i fizičku veličinu (kada se uradi properties nekog fajla možemo primetiti dve veličine size i size on the disk koje se u nekim slučajevima ne poklapaju). Razlog leži upravo u pomenutom načinu na koji fajl sistem skladišti podatke na hard disku. Bez ulaska u previše detalja o načinu rada fajl sistema odgovor na nepoklapanje fizičke i logičke veličine (odnosno njihovoj razlici) leži u razumevanju Fajl sleka koji se sastoji iz dva dela : drajv slek i RAM slek. Poznavanje ovih karakteristika fajl sistema, kada je u pitanju digitalna forenzika, igra važnu ulogu kada je u pitanju forenzička analiza operativnog sistema.

Na osnovnom nivou sektor (eng. sector) čini najmanju oblast hard diska na koju se mogu upisivati podaci. Ovi sektori su grupisani u klastere (eng. clusters). Na Windows sistemima sektori su fiksne veličine 512 bajtova (eng. bytes) dok veličina klastera zavisi od veličine samog hard diska. Manji diskovi imaće manju veličinu klastera i obrnuto.

Kad se fajlovi skladište, fajl sistem koristi fiksne veličine blokova koji se nazivaju klasteri .Klasteri predstvaljaju grupe sektora koji se koriste za raspodelu prostora na disku u cilju skladištenja podataka u Microsoft Operativnim sistemima. Znači da se svakom novom fajlu dodeljuje određen broj klastera po sledećem principu :

*Veličina fajla <= broj klastera * veličina jednog klastera*[161]

Kada se kreira fajl, fajl sistem dodeljuje prvi raspoloživ klaster u zavisnosti od logičke veličine podataka. Očigledno je da svaki sačuvani fajl na disku ne može biti tačna veličina jednog ili više klastera, tako da će ostati prostora u poslednjem klasteru. Taj prostor se naziva Fajl slek i kreira se u vreme kada se fajl snima na disk. Na primer ukoliko je klaster veličine 32K, a fajl koji se upisuje je veličine 10K, dodeljen prostor za fajl će biti 32K a preostalih 22K se naziva slek prostorom.

Već je pomenuto da fajl slek ima dva dela RAM slek i drajv slek. RAM slek se odnosi na preostali prostor u poslednjem sektoru samog fajla[162] (odnosno od kraja logičkog fajla do kraja sektora). Trebalo bi napomenuti da iako su klasteri jedinice dodele (eng. Allocation unit), fajl sistem upisuje u delovima od 512 bajtova. Veoma retko će veličina datoteke biti tačan umnožak od 512. To znači, da kada fajl sistem završi upisivanje poslednjeg sektora nekog fajla pojaviće se prostor na kraju tog sektora. Do Windows 95 version B[163] taj prostor se popunjavao slučajnim podacima iz RAM memorije što je predstavljalo veliku bezbednosnu rupu jer podaci iz RAMa mogu da sadrže šifre i druge osetljive podatke. Od tada Windows operativni sistemi ne upisuju podatke iz memorije u fajl sistem, već umesto toga upisuje u preostali prostor poslednjeg sektora fajla heksadecimalnu vrednost x00.

Drajv slek iako je termin koji se ne upotrebljava često[164] on se u literaturi najčešće povezuje sa terminom fajl slek i odnosi se na preostale neupisane sektore u poslednjem klasteru fajla (obuhvata prostor preostalih sektora do kraja klastera) [161]. Fajl sistem ne popunjava ovaj prostor kao što se to nekad radilo sa RAM slekom i on ne čini ništa sa ovim prostorom. Ovi sektori mogu da sadrže različite tipove podataka i mogu sadržati ostatke prethodno obrisanih fajlova ili čak podatke koji su postojali pre poslednjeg formatiranja.

[161] Chetan Gupta , File slack vs ram slack vs drive slack, http://niiconsulting.com/checkmate/2006/06/21/file-slack-vs-ram-slack-vs-drive-slack/, 12.03.2012.

[162] Centar for computer forensic, What is file slack, http://www.computer-forensics.net/what-is-file-slack?/, 12.03.2012

[163] Solutions Centar, The Importance of File slack to Digital Forensics and eDiscovery, http://www.trigonit.com/tech-blog/bid/32299/The-Importance-of-File-Slack-to-Digital-Forensics-and-eDiscovery, 12.03.2012

[164] Razlog je taj što u RAM slek prostor (kao deo fajl sleka) Windows operativni sistem ne smešta podatke iz RAM memorije pa se onda se za preostali deo slek prostora umesto termina drajv sleka koristi termin fajl slek.

Sa odgovarajućim setom alata iskusan digitalni forenzičar može oporaviti podatke koji se nalaze u fajl sleku i nealociranom prostoru. Fajl slek može biti predmet analize sa ciljem da identifikovanja prethodnih radnji osumjičenog računara i može sadražati delove (eng. fragments) elektronskih poruka, dokumenata za obradu teksta i mnogo drugih osetljivih podataka koji mogu pomoći pri otkrivanju učinioca protivpravne aktivnosti. Takođe, ovi slek fajlovi mogu da postoje i na flopi disketama, zip diskovima i ostalim uređajima za skladištenje podatka na računaru. Sa forenzičke tačke gledišta fajl slek je veoma važan kao izvor potencijalnih računarskih dokaza, u istrazi računarskog incidenta ili kriminala.
Na primer, jedan od Linux-ovih alata koji se koristi za prikupljanje i oporavak podataka iz nealociranog prostora sa fajl sistema jeste alat iz TCT[165] kolekcije koji se zove "unrm". Drugi alat koji se takođe odnosi na podatke iz nealociranog prostora zove se Lazarus (takođe iz TCT kolekcije). Ovaj alat analizira sirove podatke prikupljenih unrm alatkom i klasifikuje podatke prema tipu. U nastavku biće izloženi primeri zauzeća fajla na NTFS disku.

Primer 1

Na NTFS disku sa sektorima veličine 512 bajtova, i 8 sektora po klasteru čini veličinu klastera 4096 bajtova (512*8). Ukoliko je fajl veličine 5200 bajtova, to znači da će slek prostor biti 3072 bajta i 20 bajta RAM sleka.
Fajl veličine 5100 bajtova zauzima 9 sektora. S obzirom da NTFS fajl sistem radi sa klasterima ne sa sektorima fajlu će biti dodeljena 2 klastera. Prvi klaster (8 sektora) biće kompletno popunjen fajlom, ali drugi klaster će da sadrži samo 1004 bajta fajla (4096+1004=5100).
To znači da prvi sektor (512 bajtova) od drugog klastera biće kompletno popunjen fajlom, ali će drugi sektor drugog klastera sadržati samo 492 bajta. Prostor na kraju drugog sektora drugog klastera je poznat kao RAM slek (kao dump iz RAM-a nekadasnjih operativnih sistema) i u ovom slučaju iznosi 20 bajtova (492+20=512).
Nakon ovog sektora postoji još 6 sektora do kraja drugog klastera (jer fajlu je dodeljeno dva klastera odnosno 16 sektora ukupno). Ovih 6 sektora predstavljaju fajl slek, što iznosi 3072 bajta slek fajla.

Primer 2

Kreiran jedan „txt“ fajl uz pomoć programa Notepad sa upisanom rečju „doktorat“. Desni klikom na snimljeni fajl proverava se properties tog fajla. Može se primetiti da postoje dva njegova svojstva (eng. Attributes) „Size“ i „Size on disk“.
Size: 8 bytes (8 bytes)
Size on disk : 4.00 kb (4096 bytes)

Postavlja se pitanje odakle se stvara ova razlika, jer ukoliko je fajl velik samo 8 bajtova zašto su preostali bajtovi dodeljeni datoteci i da li oni služe nekoj svrsi. Prosečnom korisniku nije od koristi, ali digitalnom forenzičaru je itekako od koristi. Odgovor leži u razumevanju slek prostora. S obzirom da se u literaturi povezuju sa slekom (kako se kolokvijalno naziva) različiti termini poput Fajl slek, RAM slek i Drajv slek to može biti dosta zbunjujuće. Iako ovi termini izgledaju slično, razumevanje i poznavanje razlika između njih jako je bitno, kada je u pitanju forenzička analiza računarskog sistema i u daljem tekstu će biti pojednostavljeni ovi termini. Na slici 6. prikazan je sadržaj klastera nakon snimanja fajla.

Slobodan prostor

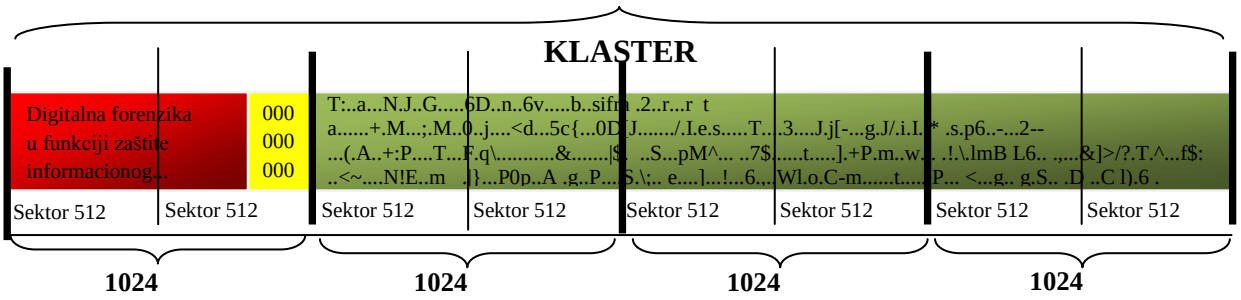
[165] The Coroner's Toolkit (TCT) predstavlja kolekciju forenzičkih alata čiji su autori Wietse Venema i Dan Farmer , dostupno http://www.porcupine.org/forensics/tct.html , 05.04.2013

Podrazumeva prostor na hard disku koji trenutno nije dodeljen datoteci, a može biti i prostor koji nikada nije dodeljen datoteci i obično se nalazi na kraju diska.
Primer jednog klastera koji može sadržati bitne informacije u jednom delu slek prostora.
Veličina klastera - 4096 bajta
Veličina sektora - 512 bajta
Trenutni sadržaj klastera predstavlja fajl doktorat.txt - 800 bajta

- Predstavlja upisan sadržaj fajla doktorat.txt
- Zaključno sa verzijom Windows 95 i Win NT 3.5 ovde bi se našli podaci iz RAM memorije i to je ono što se u literaturi može naći kao termin RAM slek
- Predstavlja drajv slek odnosno fajl slek, ukoliko ne računamo RAM slek i tu se nalaze sirovi podaci (eng. Raw data) koji se nalaze od ranije u ovim sektorima.

Loši sektori

Loši sektori (eng. Bad sectors) predstavljaju oštećeni deo diska na kome se ne mogu izvršiti operacije čitanja i upisa. Procesom formatiranja diska omogućava se operativnom sistemu da identifikuje neupotrebljiv sektor i obeleži ga kao loš. Postoje specijalni programi koji se koriste za oporavak podataka u lošim sektorima, što digitalnom forenzičaru može biti od velike važnosti.



Slika 6. *Prikaz sadržaja Klastera nakon snimanja fajla*

Sa stanovišta digitalne istrage bitno je znati da klasteri mogu biti označeni kao loši, sa ciljem skrivanja podataka. U NTFS loši klasteri su označeni u metadata fajlu koji se zove $BadClus koji je u MFT-u 8 zapis[166][85]. $BadClus jeste rasčlanjeni fajl čija je veličina podešena prema veličini celog fajl sistema. Kada se detektuje loš klaser on će biti dodeljen ovom fajlu. Veličina podataka koji mogu biti skriveni sa ovom tehenikom je neograničena, prostim dodeljivanjem klastera [178].

2.3.6 Prihvatljivost digitalnog dokaza

Da bi digitalni dokaz bio prihvaćen od strane suda treba da poseduje pet osobina:

Prihvatljiv – u skladu sa određenim pravnim pravilima, pre nego što bude dostavljen sudu. Ukoliko se koristi kopija, potrebno je koristiti najbolju kopiju, ukoliko se koristi original tada kopija nije od značaja. S obzirom da se danas može napraviti kopija digitalnog dokaza (u nastavku rada biće objašnjeni načini pravljenja pravno prihvatljivih kopija digitalnog dokaza) istovetnog originalu, upotreba kopije je

[166] Postupak opisanu u radu Cheong Kai Wee „Analysis of hidden data in the NTFS file system“ dostupnog na sajtu http://www.forensicfocus.com/hidden-data-analysis-ntfs [203], pristupano 24.05.2013

pravno prihvatljiva i ako postoji original. I upravo u praksi se koristi i primenjuje prezentovanje kopije da bi se eliminisale sve sumnje vezane za izmenu tj. zloupotrebu sa originalnim dokazom.

Autentičan - Dokazni materijal mora nedvosmisleno upućivati na krivično delo i učinioca. Ukoliko se ne može dokazati autentičnost digitalnog dokaza na sudu, bez obzira što je dokaz prikupljen i analiziran na propisan način, sudija može proglasiti dokaz nevažećim nerelevantnim (neprihvatljivim) za donošenje sudske odluke.

Kompletan – u smislu da dokaz treba da prikaže ceo slučaj sa svim aspektima bitnim za donošenje sudske odluke. Dokaz mora biti objektivan i prikazati sve bitne okolnosti za sudsko odlučivanje – kako one koje se stavljaju na teret okrivljenog, tako i okolnosti koje mogu biti oslobađajuće, ukoliko postoje.

Pouzdan –ne sme postojati nikakva sumnja u vezi sa načinom na koji su dokazi prikupljeni i kako je sa njima rukovano. U suprotnom, to bi bacilo sumnju na autentičnost i istinitost dokaza.

Verodostojan i razumljiv – dokaz mora biti verodostojan i lako razumljiv za sud i stranke u postupku. Nema svrhe pred sud iznositi na primer „memory dump" (slika stanja memorije u računaru), s obzirom da sud nema obavezu da poseduje takva stručna znanja pa samim tim neće razumeti šta to znači[167][171].

Neophodno je permanentno praćenje noviteta na polju računarskih sistema što ujedno predstavlja i preduslov valjane akvizicije dokaza sa njih. Takođe, potrebno je primetiti da je sa jedne strane prisutan porast broja načina zaštite podataka, dok sa druge strane to otežava i usporava rad forenzičara i zahteva nova napredna znanja. Digitalni dokaz, kao element istrage, je mnogo ranjiviji od fizičkog, pa je veštom napadaču lakše da ih ukloni, a nepažljivo i nestručno vođenje istrage, takođe može dovesti do gubitka ključnih podataka. Zato je praksa pokazala da digitalni forenzičar timski radi sa specijalistom zaštite, da bi se obezbedila prihvatljiva zaštita računarskih sistema i bezbedan rad računarske mreže u poslovnim sistemima [186].

O bilo kom tipu visokotehnološkog kriminala da je reč, moraju se pronaći odgovori na pitanja koje digitalni forenzičar treba da postavi : ko je izvršio protivpravnu radnju, kada se ona desila i kako, zašto je delo učinjeno, gde je mesto incidenta, šta je bio cilj, a na tužilaštvu je dalje da uz sve to dokaže i uzročno-posledičnu vezu između dela i učinioca kao i nameru da se to delo izvrši (krivica). Odgovore na ova pitanja će pružiti upravo tri tipa dokaza : vremenski dokazi (oni će pomoći u otkrivanju sekvenci ili obrazaca u vremenskim dešavanjima i daju odgovor na pitanje „kada"), relacioni dokazi (podrazumevaju elemente protivpravnih aktivnosti, njihov odnos i pozicije daju odgovor na pitanja „ko, šta i gde") i funkcionalni dokazi (pružaju uvid u to šta je moguće, a šta nije dajući odgovor na pitanje „kako").

Da bi se prikupile sve relevantne informacije i dokazi, bilo da su oni digitalni ili fizički, neophodno je izvršiti analizu ne samo ciljnog računara, već i onih sa kojih je pokrenuta neka nezakonita aktivnost. Takođe, analiziraju se i oni računari koji su indirektno učestvovali u protivpravnom delu. Kada se sve te informacije i dokazi sakupe, oni se dostavljaju nadležnim organima u slučaju da je došlo do ugrožavanja državne i javne bezbednosti, ili korporativnim organima, ukoliko se incidentna radnja desila u njenim okvirima.

Digitalni dokazi su apstraktni i kao takvi mogu se lako izmanipulisati u smislu izmene ili njihovog uklanjanja. U ovom radu u fokusu su upravo informacije od značaja za digitalnu forenzičku istragu koje se nalaze na hard diskovima u okviru računara, bilo da su pod Linux ili Windows operativnim sistemom.

[167]Douglas Schweitzer, Incident Response - Computer Forensics Toolkit, Wiley Publishing, Inc, Indianapolis, 2003, strana 140

Kada računar postaje deo istrage ? Računar postaje deo istrage kada se na njemu ili sa njim izvrši neka protivpravna radnja. U prethodnom poglavlju bio je spomenut Lokardov zakon čiji je tvorac Edmond Lokard, koji govori o tome da prilikom svakog kontakta dva objekta, postoji neka razmena materije, tj. svaki kontakt ostavlja trag [191]. U slučaju digitalnih dokaza tu materiju možemo da posmatramo kao npr. fajlove koji se generišu ili razmenjuju putem računara, koji međusobno komuniciraju i time vrše razmenu „nečega“ a to nešto to su podaci, informacije tj. fajlovi, a u osnovi su bitovi. To znači da je moguće dovesti određene dokaze u vezu sa izvršiocem.

Na osnovu pomenutog prinicipa razmene mogu biti proizvedeni digitalni dokazi koje možemo svrstati u sledeće dve kategorije [34] :

- Dokazi sa atributima koji odgovaraju grupi klasnih karakteristika - karakteristike klase ispoljavaju zajedničke osobine kada se posmatraju slični predmeti odnosno stvari. Mogu biti povezani samo sa grupom izvora a nikada sa samo jednim izvorom [165] .
- Dokazi sa atributima koji pripadaju grupi individualnih karakteristika - pojedinačne karakteristike su jedinstvene i mogu povezati izvršioca ili aktivnost sa većom sigurnošću.

U stvari preko ovih atributa i tumačenjem njihovih karakteristika na osnovu informacija koje u sebi sadrže, digitalni dokazi se mogu razvrstavati prema pomenutim grupama. S tim u vezi, digitalni podaci mogu biti prisutni u mnogim nivoima apstrakcije tako da je od značaja na koji način će se vršiti klasifikacija. Na primer, neki slučajevi zahtevaju pregledanje image-a diska sa hex editorom, a u nekim slučajevima više odgovara procesiranje samog fajl sistema kroz prikazivanje fajlova i foldera.

Na osnovu klasne karakteristike dokaza, istražitelji mogu na primer da otkriju, da je korišćen određeni web server npr. Apache, ili ftp server npr. Vsftpd, ili prizvođača mrežne kartice koju je koristio napadač ili mail server npr Sendmail, ili koja se šema enkapsulacije koristila pri slanju e-mail-a (npr. MIME eng. Multipurpose Internet Mail Extensions preko koje možemo saznati da li je bilo attachmenta. koji tip podataka se nalazi, koji format originalnog fajla u pitanju, kako se vršio encoding itd...). Znači klasne karakteristike digitalnih objekata mogu da ukažu na strukturu podataka i neke opšte vrednosti kao što su vreme ili veličina.

Individualne karakteristike podrazumevaju jedinstvene identifikatore formata datoteka i njenog rasporeda, te mogu biti klasifikovani na osnovu tipa u inodu (ili druge meta data strukture) ili ekstenzije datoteke.

Kako bi se još bolje ukazao na značaj Lokardovog principa razmene, klasnih karakteristika i individualnih karakteristika u digitalnom okruženju može se prikazati na primeru upada na računar. Kada napadač dobije neovlašćeni pristup Linux sistemu sa njegovog računara koristeći ukradeni dial-up nalog i uploaduje različite programske alate na Linux računar preko FTP servera (eng. *File transfer protocol*), programski alati se sada nalaze i na Linux i na Windows računaru. Određene karakteristike ovih alata će biti iste na oba sistema uključujući vremenske pečate i MD5 heš vrednosti. Forenzičar mora poznavati karakteristike Operativnog sistema sa kojim vrši heširanje prikupljenog imidža jer se može desiti da kernel do (i uključujući) verzije 2.4 ne može pristupiti poslednjem sektoru particije na hard disku ukoliko on ima neparan broj sektora [107]. To za posledicu može da ima dobijanje različite heš vrednosti od one dobijene sa kernelom 2.6 baš kao što je Jesse D. Kornblum objavio u svom radu „The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors.”

Windows aplikacije koje se koriste za povezivanje na Linux (Putty, Secure CRT, Telnet, Tunnelier) mogu posedovati zapis o ciljnoj ip adresi računara ili njegovom imenu. Takođe, na računaru napadača moguće je pronaći i listing direktorijuma sa Linux računara, (odnosno računara koji je napadnut) dok ih je program npr. Putty prikazivao na ekranu, u nekom sesijskom fajlu. Ukradeni nalog i šifre su smešteni u operativnom sistemu

napadačevog računara tj. najverovatnije u nekom programu tipa sniffer. Isto tako ftp serveri u svojim logovima skladište podatke o razmeni fajlova, tako da se može utvrditi koje alate je prebacivao napadač na ciljani računar, čime se potvrđuje veza između napadača i napadnutog računara.
Kada digitalni forenzičar preuzme ispitivanje digitalnog dokaza, prave se digitalne kopije za dalju analizu. Praksa je pokazala da je najbolje napraviti 4 digitalne kopije hard drajva pri čemu se na jednu od njih primenjuje heširanje sa MD5 ili SHA algoritmom da bi sačuvao integritet (nepromenjivost) digitalnog dokaza. Zapravo, proces validacije podataka vrši se uzimanjem jedinstvene heš vrednosti forenzičkog imidža, kojim se obezbeđuje integritet referentne kopije za potrebe verifikacije nepromenjenosti originalnih podataka i čuvanja integriteta u lancu istrage, prema zahtevu suda [75]. Takođe jedna kopija se izdvaja i povezuje na forenzički računar da bi se nad njom vršila analiza i ispitivanje. Druge dve kopije služe kao rezervne kopije (backup) za bilo koji nepredviđeni slučaj, a mogu poslužiti i u analizi pod virtuelnim okruženjem, o čemu će više biti reči u poglavlju koje opisuje digitalnu forenziku u virtuelnom okruženju.

Potrebno je naglasiti i određena pravila koja su se kroz praksu pokazala kao vrlo korisna. Digitalni forenzičar mora da svede mogućnost ispitivanja originalnog dokaza na najmanju moguću meru, mora poštovati pravila koja se odnose na dokaze, treba da radi u okviru svojih stručnih znanja i ovlašćenja i da dokumentuje bilo kakvu promenu na dokazu.

2.3.7 Izveštavanje

U slučaju da je istraga sprovedena u potpunosti, obavezno je dostavljanje Izveštaja o istrazi. Kada je reč o istrazi u okviru organizacije, izveštaj se dostavlja vlasniku sistema koji dalje donosi odluku o istrazi. Kada je u pitanju zvanična istraga, izveštaj se dostavlja nadležnim državnim organima za dalji pravosudni postupak.
Kreiranje izveštaja je jedan od jako bitnih elemenata forenzičke analize u računarskoj forenzici i predstavlja veliki izazov za digitalnog forenzičara. Izveštaj mora da sadrži precizan opis protivpravne aktivnosti razumljiv sudu odnosno donosiocu odluka. Izveštaj mora biti blagovremeno kreiran i pravno relevantan odnosno nesporan u smislu pravne kritike. Bitno je istaći, da svi koraci u digitalnoj istrazi kao i zaključci moraju da budu dokumentovani što je pre moguće. Kada se definiše željeni format izveštaja, bitno je, da ga se digitalni forenzičar striktno poštuje. To podrazumeva kreiranje formi, skica i štablona (eng. template) kojim se, adekvatno organizuje i podstiče proces odgovora na protivpravnu aktivnost i evidentiraju svi relevantni podaci. Takav kreirani dokument „Izveštaj o istrazi“ treba da sadrži najmanje tri navedene celine [132] :
Apstrakt istrage :

- Opis događaja :
  - Kratka metodologija istrage ;
  - Kratak opis skupljanja dokaza i metoda čuvanja istih ;
  - Zaključak sa kratkim uopštenim rezonima ;

- Metodološki detalji :
  - Istraga ;
  - Skupljanje i čuvanje dokaza ;

  - Nalaz 1 – Opis ;
  - Diskusija ;
  - Dokazi koji potvrđuju ;
  - ...
  - Nalaz N – Opis ;

Diskusija ;
Dokazi koji potvrđuju ;

- Kratak sadržaj i zaključci :
  Dodatak ;
  Lista ispitanih (intervijuisanih) ;
  Lista dokaza ;
  Programi i alati korišćeni u istrazi ;
  IT eksperti konsultanti ;
  Kontakti na mestima koja su sarađivala (posrednici) ;
  Drugi važni listinzi i informacije.

Veoma je važno da se dokumentovanje vrši blagovremeno i da to obavlja iskusno osoblje da ne bi došlo do određenih propusta i grešaka koje mogu da kompromituju kompletnu digitalnu istragu. Iz navedenog proizilazi da Izveštaj mora sadržati opis korišćene metodologije, opis uspostavljenih i pridržavanih protokola[168], detaljno (step-by-step) opisane forenzičke aktivnosti, detaljno opisani korišćeni metodi i alati, detaljno opisan postupak forenzičke analize i doneti zaključci uključujući i ograničenja.

2.4 DIGITALNA FORENZIKA U VIRTUELNOM OKRUŽENJU

Kada je u pitanju digitalna forenzika u virtuelnom okruženju, vrlo je važno poznavanje samog virtuelnog okruženja i njegovih specifičnosti i mogućnosti koje okruženje može ponuditi u smislu poznavanja prednosti i nedostataka koje mogu da se jave prilikom njegove eksploatacije. Takođe, treba istaći da postoje izvesne razlike u istražnom pristupu digitalnog forenzičara kada su u pitanju fizičke odnosno virtuelne mašine[169]. Ovaj rad neće ulaziti u detaljnu forenzičku metodologiju koja se odnosi na digitalno virtuelno okruženje, već ima za cilj da istakne samo najznačajnije elemente na koje treba obratiti pažnju prilikom digitalno forenzičke analize u virtuelnom okruženju. Takođe, biće objašnjeni i najvažniji segmenti samog virtuelnog okruženja i na koji način oni mogu biti značajni za proces digitalne forenzičke analize.

Ideja virtuelizacije je isprojektovana sa ciljem jednostavnijeg upravljenja velikim brojem virtuelnih mašina čime se pre svega štedi prostor, vreme, novac i potrošnja energije. Kao koncept se pojavila još 1960 godine sa pojavom mainframe računara i ponovo se predstavila personalnim računarima 1990. Popek i Goldberg u svom radu "Formal requirements for virtualizable third generation architectures" [150] su izneli preduslove za arhitekturu koja može da podržava virtuelnu mašinu opisujući je kao „efikasan, izolovan duplikat prave mašine“. Samu virtuelizaciju su opisali kroz ideju VMM (eng. Virtual machine monitor)[170].

Ono što je specifično za virtuelne mašine, je to što one koriste u potpunosti hardver fizičkog servera. VM aplikacija (eng. guest) tzv. gost pokreće sopstveni Operativni sistem na stvarnoj (eng. host) mašini. Jednostavnije rečeno, VM predstavlja virtuelni računar pokrenut u okviru fizičkog računara. Na primer, jedan fizički server može predstavljati virtuelno okruženje sa preko 20 virtuelnih mašina. Komunikacija između fizičkog servera i virtuelnih

[168] U izveštaju je potrebno naglasiti da je prikupljanje i čuvanje dokaza u toku istrage bilo izvedeno u skladu sa zakonom o istražnom postupku i da su obavljeni informativni razgovori i saslušanja propisno izvršeni.

[169] Virtuelna mašina predstavlja kreirano okruženje od strane programskog paketa za virtuelizaciju koja poseduje simulirani skup hardvera (procesor, hard disk, memorija, mrežni uređaji i drugih komponenti) i sopstveni sistemski i aplikativni program.

[170] Virtual machine monitor predstavlja deo programa koji ima 3 karakteristike. Prva je da VMM pruža okruženje za programe koje je identično okruženju na fizičkoj mašini. Drugo, programi koji se pokreću u ovom virtuelnom okruženju imaju veoma mali pad performansi kada je u pitanju brzina u odnosu na fizičku mašinu i treće je da VMM u potpunosti kontroliše sistemske resurse.

mašina se realizuje preko hypervisor-a (program koji obezbeđuje virtuelizaciju) ili *virtual machine manager-a* putem hiper poziva. Hypervisor upravlja sistemskim procesorom, memorijom i drugim resursima koje dodeljuje drugim gost sistemima na zahtev [13]. Hypervisor može da obezbeđuje virtuelizaciju direktno na hardveru (native VM ili Bare-Metal Hypervisor) ili na operativnom sistemu (host VM ili Hosted Hypervisor) [86]. Predstavnici virtuelizacije koja se realizuje direktno na hardveru su : VMware ESX[171], Citrix XenServer[172], i Microsoft Hyper-V[173]. Predstavnici virtuelizacije koja se realizuje na OS su : Parallels Desktop [174] , Microsoft Virtual Server [175] , VMware Server [176] , i VMware Workstation[177].

Virtuelna mašina može raditi izolovano ili može deliti resurse sa drugim virtuelnim mašinama u okviru iste ili druge serverske platforme. Na osnovu ovog specifičnog dizajna i optimizovanih procesorskih operacija u okviru realizovanog virtuelnog okruženja, nema razlike u radu na virtuelnim mašinama u odnosu na fizičke mašine. Postoje različiti tipovi virutelnog ogruženja a najpoznatiji su *Microsoft Hyper-V* [128], *VMWare Vsphere ESXi* [197], *QEMU* [157], *Citrix XenServer* [41]. U daljem tesktu će biti navedena dva ugla digitalne forenzike u virtuelnom okruženju. Prvi posmatra virtuelno okruženje kao digitalno mesto krivičnog dela, a drugi posmatra virtuelno okruženje kao okruženje za digitalno forenzičku analizu.

2.4.1 Virtuelno okruženje kao digitalno mesto krivičnog dela

Kao i svako okruženje i virtuelno okruženje može biti kompromitovano na različite načine, što za posledicu može da ima kompromitovanje kako samih virtuelnih mašina tako i operativnog sistema i fajlova koji se u tom okruženju nalaze [102].

Dobra informisanost i poznavanje načina rada u virtuelnom okruženju su veoma bitni faktori digitalnom forenzičaru, kome je digitalno mesto krivičnog dela upravo virtuelno okruženje koje čine virtuelne mašine. Pristup istrazi se bazira na lociranju i pristupu fizičkom serveru koji pokreće virtuelne mašine. Od velike je važnosti da digitalni forenzičar ima "uživo" (eng. live) pristup digitalnoj mašini koja se posmatra kao digitalno mesto krivičnog dela. Na taj način mogu se prikupiti dragoceni podaci i informacije kao potencijalni digitalni dokazi, u toku rada fizičkog servera. Treba istaći i činjenicu da je mogućnost manipulacije dokaza u ovakvom okruženju, od strane osumnjičenog velika, pa se posao prikupljanja digitalnih dokaza prilično usložnjava.

Principi koji se odnose na digitalnu forenziku računara i koji važe u toku prikupljanja, analize i prezentacije digitalnih dokaza (kao na primeru u prikazanom Carrier modelu), isti važe i za virtuelne mašine u virtuelnom okruženju sa određenim razlikama na koje će biti ukazano u radu. Bitno je istaći da je potrebno koristiti samo testirane i proverene forenzičke alate (na primer *Access data FTK, Encase, X-Way Forensic*) koji podržavaju rad u virtuelnom okruženju kao i da poseduju kompatibilnost sa novijim operativnim sistemima.

Ukoliko se istraga, u vezi sa protivpravnim aktivnostima, usmeri na virtuelno okruženje i ako se obavlja prema nekim od predloženih metodologija iz ovog rada (poglavlje 2.3), uz korišćenje odgovarajućih forenzičkih alata, a sa ciljem pronalaženja relevantnih digitalnih dokaza, istražni postupak će se uspešno okončati. U suprotnom, istraga može da ode u neželjenom pravcu. Digitalna istraga u virtuelnom okruženju može biti javna

[171] Dostupno na http://www.vmware.com/products/esxi-and-esx/overview
[172] Dostupno na http://www.citrix.com/products/xenserver/overview.html
[173] Dostupno na http://www.microsoft.com/en-us/server-cloud/hyper-v-server/default.aspx
[174] Dostupno na http://www.parallels.com/
[175] Dostupno na http://www.microsoft.com/Windowsserversystem/virtualserver/
[176] Dostupno na http://www.vmware.com/products/vcenter-server/
[177] Dostupno na http://www.vmware.com/products/workstation/

(zvanična) i korporacijska, u zavisnosti od toga, o kom tipu incidentne radnje je reč. Istraga počinje fizičkim pristupom fizičkom mestu krivičnog dela, gde se vrši prikupljanje fizičkih dokaza, zatim se pristupa digitalnom mestu krivičnog dela (virtuelnom okruženju koga čine virtuelne mašine) i traje dok digitalni forenzičar ne završi istragu nad digitalnim podacima, spremnim za izveštaj odnosno prezentovanje rekonstruisanog zločina ili incidenta.
Treba istaći činjenicu da je virtuelno okruženje, okruženje koje nudi čitav niz pogodnosti putem svojih veoma korisnih operacija, ali da upravo one mogu biti i zloupotrebljene. Na primer, operacije koje mogu biti zloupotrebljene su migracija virtuelnih mašina, manipulacije sa image-om (slikama stanja) virtuelnih mašina, live migration (manipulacije vezane za migriranje virtuelnih mašina "uživo"). Neke od ovih zloupotreba mogu da za posledicu imaju kontrolu, odnosno zloupotrebu virtuelnih mašina od strane zlonamarnog lica.

Zlonamerne aktivnosti se mogu pronaći, jer se sve aktivnosti beleže na serveru odnosno hostu, i vrlo je važno da digitalni forenzičar samoj istrazi kao i prikupljanju dokaza pristupa striktno prema definisanim procedurama sa početku istrage, jer u suprotnom može doći do gubitaka ili nestanka važnih digitalnih informacija. Virtuelna forenzika mora da ima veći broj prikupljenih dokaza u odnosu na klasičnu digitalnu forenziku, jer digitalni forenzičar mora da prikupi informacije i o paketima podataka, kao i o komunikaciji između zlonamernog korisnika i korisnika nad kojim je izvršena protivpravna aktivnost. U virtuelnoj forenzici sve se dešava u virtuelnim prostorima, koji su smešteni na fizičke (serverske) mašine, a pritom su povezane sa Internetom tako da virtuelno mogu biti gde (jedan takav primer je Cloud computing[178]). Da bi se digitalna mesta krivičnog dela istražila, digitalni forenzičar mora da uđe u digitalno virtuelno okruženje, koje je složeno, i može predstavljati veliki problem forenzičaru, ukoliko nisu izvršene pripremne radnje praćenja uz snimanja aktivnosti osumnjičenog, kao i upoznavanje sa samim operativnim sistemamima koje se nalaze u virtuelnom okruženju. Za razliku od klasične digitalne forenzike, gde se fizičkom računaru pristupalo fizičkim putem, kada je reč o forenzici u virtuelnom okruženju, forenzičar neće moći da ima jednostavan pristup fizičkoj mašini na kojoj je realizovano virtuelno okruženje. To upravo predstavlja i specifičnost digitalne forenzike u virtuelnom okruženju. Jedan od ciljeva koji se postavlja pred digitalnim forenzičarem je i lociranje centralnog mesto sa virtuelnim računarima (a ne, samo lokacija virtuelne mašine) koji u sebi nose veliki broj korisnih informacija koje mogu biti iskorišćene kao potencijalni digitalni dokaz koji može da posvedoči o protivpravnoj aktivnosti. Takođe, vrlo je važno da digitalni forenzičar poznaje sve koncepte virtuelizacije.

Servisi u virtuelnom okruženju

U nastavku će biti naveden slikovit opis važnih servisa koji realizuju virtuelno okruženje, a njihovo upoznavanje može biti od koristi digitalnim forenzičarima [179] [192]:

- **Servis za upravljanje virtuelnih mašina** (Virtual machine management service, VMMS) - upravlja odnosno određuje koje operacije mogu da se izvršavaju u nekom od mogućih stanja vrituelnih mašina. VMMS upravlja sledećim stanjima virtuelnih mašina : pokretanje, aktivno stanje, neaktivno stanje, stanje pravljenja slike stanja (eng. snapshot), stanje primene slike stanja (eng. snapshot), brisanje slike stanja, spajanje diskova. Na osnovu ovih stanja VMMS upravlja operacijama na virtuelnim mašinama (eng. child). Ne upravlja operacijama *Pauza, Snimanje, Isključenje*, već je

[178] Cloud computing kao tip virtuelnog okruženja funkcioniše na sledeći način : korisnik dobija pristup računaru koji je smešten na udaljenom serveru. Ovaj sistem omogućava korisniku bezbedan i udoban rad. Velika prednost ovakvog sistema je, što korisnik ne mora da razmišlja gde mu se nalazi računar a podaci su mu uvek na raspolaganju. Takođe, ne mora da brine ni o održavanju tog računara, a u zavisnosti od toga šta je zakupio, može imati na raspolaganju i ogromnu količinu prostora. Postupak uspostavljanja konekcije sa virtuelnom mašinom je prilično jednostavan. Postoje određeni programski klijenti koji su zaduženi za realizaciju ove konekcije prema serveru koji je priključen na javnu mrežu. Posle uspešnog postupka autentifikacije, korisnik pristupa svojoj virtuelnoj mašini.

[179] Primer je vezan za realizaciju Hiper V okruženja gde je na host-u podignuto okruženje Windows server 2008 R2.

za to odgovoran proces *Virtual machine worker proces* (VMWP) koji se kreira pri pokretanju virtuelne mašine.

- **Radni proces virtuelne mašine** (eng. Virtual machine worker proces) - kreira se na virtuelnoj mašini, pojavljuje se kao izvršni fajl vmwp.exe i učetstvuje u velikom broju interakcija između operativnog sistema na hostu i virtuelnih mašina (child-ova). Ove interakcije podrazumevaju kreiranje virtuelnih mašina njihovo konfigurisanje, upravlja stanjima pauza (eng. pause) i nastavak rada virtuelnih mašina (eng. resume), čuva (eng. saving) i obnavlja virtuelne mašine (eng. restore) i snima slike stanja virtuelnih mašina. Takođe upravlja memorijom, ulazno-izlaznim portovima na matičnoj ploči računara (eng. motherboard) i upravlja IRQ-ovima. Na primer postojanje ovog fajla (vmwp.exe) predstavlja dokaz da na hostu postoje viruelne mašine.
- **Virtuelni uređaji** (eng. virtual device) predstavljaju programske module (upravljačke programe) koji omogućuju konfigurisanje uređaja i kontrolu particija virtuelnim mašinama. Upravljaju se putem virtuelne matične ploče (eng. Virtual motherboard - VMB) koja se dodeljuje svakoj virtuelnoj mašini.
- **Drajver VMBus** - pruža optimizovanu komunikaciju između *host-a* i *child-a* i sastavni je deo *Hyper-V servisa* ;
- **Drajver za virtuelizaciju infrastrukture (eng. Virtual Infrastructure Driver)** - predstavlja komponentu kernela odgovornu za režim virtuelizacije na *host-u*, omogućuje upravljanje virtuelnim procesorom i memorijom.
- **Windows Hypervisor Interface biblioteka (eng. The Windows Hypervisor Interface Library)** predstavlja komponentu kernela kao dinamička biblioteka (eng. dynamic link library - DLL). Omogućava drajverima operativnog sistema pristup procesoru. Nalazi se kao sastavni deo operativnog sistema na hostu. DLL fajl omogućava d*river-ima* operativnog sistema da pristupaju procesoru.

Navedeni servisi možda nemaju direktan uticaj na istražni postupak, ali je važno poznavati bitne procese i njihove mogućnosti u hardverskoj komunikaciji, između procesora i hypervizora odnosno između *host-a* i *child-a.*

Prisustvo pomenutih fajlova u vidu virtuelnih uređaja i drajvera digitalnom forenzičaru može ukazivati o postojanju virtuelnih mašina.

Univerzitet Fairbanks Alaska [180] se bavi istraživanjim u oblasti ispitivanja osetljivih (nestabilnih eng. volatile) podataka korišćenjem virtuelne instrospekcije (eng. Virtual Introspection). Virtuelna introspekcija, kao oblast novog istraživanja i razvoja u digitalnoj forenzici, predstavlja proces posmatranja stanja virtuelne mašine ili putem Virtual Machine monitor (VMM) ili sa neke druge virtuelne mašine koja nije predmet forenzičkog ispitivanja. Oni su razvili set alata za Xen okruženje koji se zove VIX tools [82] ca ciljem da se smanji rizik od izmene nad dokazima tokom njihovog ispitivanja. Takođe, ovaj alat omogućava analizu "uživo" nad Xen virutelnoj mašini[181]. Osnovni pristup ovih alata je da se pauzira osumnjičena virtuelna mašina, zatim se vrši prkukpljanje neophnodnih podataka korišćenjem samo read only operacije i potom se pauza prekida. Kao korisna stvar koja može da se realizuje ovim alatom je mapiranje memorije osumnjičene mašine i dodeljivanje mapiranog dela virtuelnoj forenzičkoj mašini.

Mreže u virtuelnom okruženju

Kada je reč o mrežama u virtuelnom okruženju postoje tri vrste virtuelnih mreža [192] :

[180] http://www.uaf.edu/, 03.01.2012

[181] http://assert.uaf.edu/papers/forensicsVMI_SIGOPS08.pdf, 03.01.2012.

- **Interna virtuelna mreža (eng. Internal virtual networks)** – ovaj tip mreže se ne oslanja na fizički mrežni adapter, već se koristi virtuelni mrežni adapter. Interna virtuelna mreža se upotrebljava kao Intranet i koristi se za međusobno umrežavanje virtualnih mašina u Intranetu. Takođe postoji i opcija njihovog umrežavanja sa *host-om*, što potencijalno otvara mogućnost zloupotrebe child-ova ukoliko dođe do kompromitovanja host računara. Zlonamerni napad bi bio usmeren na programsku oblast sa ciljem zloupotrebe virtuelne mašine ili njihovim gašenjem.
- **Eksterna virtuelna mreža (eng. External virtual networks)** – ovaj tip mreže se oslanja na fizički mrežni adapter i na virtuelni mrežni adapter čime se ostvaruje međusobna komunikacija fizičkih i virtuelnih mašina, kako u Intranetu tako i ka Internetu. Potencijalno se otvara mogućnost zloupotrebe host-a, kako od spolja, tako i od strane samih virtuelnih mašina jer je otvorena komunikacija između hosta i childa. Takođe, zlonamerni napad bi bio usmeren na programsku oblast sa ciljem zloupotrebe virtuelne mašine ili njihovim gašenjem.
- **Privatna virtuelna mreža (eng. Private virtual networks)** – ovaj tip mreže ne oslanja se na fizički mrežni adapter (slično kao kod interne virtuelne mreže), i nije dozvoljena komunikacija sa članovima van privatne virtualne mreže. Takođe ni *host* nema direktnu komunikaciju sa tom mrežom, čime se sprečava zlonamerni napad na ovaj tip mreže. Teoretska mogućnost napada postoji, ali ona je ograničina na hardverski deo hosta.

Da bi se saznalo ime host-a, podaci o mrežnim karticama (fizičkim i virtuelnim) i njihovim konfiguracijama (DHCP parametri, MAC adrese), koriste se određeni alati za tu namenu, koji će biti prikazana u radu u 3. poglavlju. Sve ove informacije o mrežnim adapterima virtuelnih mašina koje se nalaze direktno na hostu, su jako važne digitalnom forenzičaru da bi se upoznala arhitektura virtuelnog okruženja.

Dokaz postojanja hardvera koji podržava virtuelizaciju

Savremeni koncepti virtuelizacije (kao na primer relizacija cloud computing-a), može da se realizuje samo ukoliko se koriste posebno podešeni hardverski kompatibilni procesori, koji imaju podršku za rad sa hypervizorom. Procesori koji se najčešće koriste za realizaciju virtuelnog okruženja su Intel VT[182] i AMD-V[183]. Zašto je značajno da digitalni forenzičar ustanovi tačnu loakaciju fizičkog servera na kojoj se nalazi virtuelna mašina koja je predmet istrage? Razlog je taj, što se upravo na taj način (fizičkim pristupom hostu) može dokazati postojanje ovakvih tipova procesora koji podržavaju hardversku virtuelizaciju, čime se dokazuje mogućnost postojanja virtuelnih mašina koje su mogle biti (is)korišćene za izvršenje protivpranih aktinovsti, a koje su smeštene na samom hostu odnosno fizičkoj mašini. Na primer, Properties operativnog sistema može pružiti osnovne, a dovoljne informacije o tipu procesora. Takođe digitalni forenzičar za dodatne informacije o virtuelizaciji može pronaći i u BIOS-u (pod opcijama za podešavanje virtuelizacije), koje mogu indirektno uticati na ispitivanje i prikupljanje dokaza. Takođe, prisustvo aplikacije kojom se upravljaju virtuelne mašine (menadžer virtuelnih mašina) ukazuje na postojanje virtuelnih mašina, ali i na mesto odakle se pokreću virtuelne mašine o čemu mogu posvedočiti i log fajlovi pripadajućeg okruženja.

Ovi konzolni alati koji mogu upravljati virtuelnim mašinama digitalnom forenzičaru mogu biti od koristi u slučaju potrebe monitoring-a i upoznavanja sa virtuelnim mašinama na živo (eng. live). Na taj način mogu se otkriti značajne informacije : imena virtuelnih mašina, stanje u kojem se nalaze virtuelne mašine (da li su aktivne ili nisu), u kom režimu rada se one nalaze, iskorišćenost resursa od strane virtuelnih mašina i podaci o vremenu i vremenskim

[182] Ovde se nalazi lista Intelovih procesora koji imaju podršku za virtuelizacije : http://ark.intel.com/VTList.aspx, 10.02.2012
[183] AMD platforma za virtuelizaciju :http://sites.amd.com/uk/business/it-solutions/virtualization/Pages/amd-v.aspx, 10.02.2012

zonama. Na primer, to mogu biti „last logon“ log fajlovi ili „configuration log“ fajlovi, a njihove putanje zavise od vrste programa koji realizuju virtuelno okruženje. Takođe, ukoliko se koriste profili ili roaming profili, fajlovi koji bi forenzičaru mogli biti interesantni su NTUSER.dat (specifični sistemski registry korisnički fajl) i drugi aplikativni podaci. U nekim slučajevima se može desiti da se direktorijum TEMP ne kopira zajedno sa profilom pa je potrebno primeniti posebnu pažnju prilikom forenzičkog ispitivanja prikupljenog virtuelnog hard diska.

Dokazivanje vremena

Digitalni forenzičar mora posvetiti izuzetnu pažnju na vreme i vremenske zone ispitivane virtuelne mašine, samog hosta (ukoliko je fizički pristup moguć) i okruženja u kome se trenutno to forenzičko istraživanje sprovodi. Potrebno je evidentirati da li se vremena poklapaju i kolika su odstupanja[184].

Obezbeđivanje digitalnog mesta krivičnog dela u virtuelnom okruženju

Da bi se sačuvali svi potencijalni digitalni dokazi, kako u klasičnoj digitalnoj forenzici tako i u forenzici virtuelnog okruženja, veoma je bitno pre započinjanja ispitivanja "uživo" (eng. live), da se onesposobe sve mrežne komunikacije osumnjičenog host-a. To se radi izvlačenjem mrežnog kabla iz fizičke mašine-host-a, odnosno ukoliko host ostvaruje bežičnu (eng. wireless) komunikaciju za izlaz na Internet ili Intranet, isključiti bežični uređaj na koji je povezan.

Pristup RAM-u

Na primer, da bi se realizovalo virtuelno okruženje sa 16 virtuelnih mašina koji radi pod Windows 7 operativnim sistemom, biće nephodno minimum 16 Gb RAM-a. Windows 7 kao minimum RAM memorije zahteva 1GB RAM-a. Za operativni sistem na hostu biće potrebno minimalno od 512 MB do 4 GB Ram memorije u zavisnosti od OS-a koji je odgovoran za realizovanje virtuelizacije. Ukupna količina rama će u tom slučaju iznositi 20gb RAM-a (16 Gb RAM memorije po childu i 4 Gb na hostu). Ove informacije su važne da bi na osnovu njih digitalni forenzičar imao uvid u ukupnu količinu RAM memorije koja se nalazi na fizičkoj mašini i koliko je od toga iskorišćeno od strane virtuelnih mašina.

Izvlačenje informacija iz RAM memorije moguće je iz onog dela RAM memorije na host-u koji je određen za virtuelnu mašinu koja je pod istragom. To se izvodi uz korišćenje forenzike na živo (pod uslovom da računar nije prethodno isključivan jer bi se time izbrisao sadržaj RAM-a) uz primenu forenzičkih alata za pristupanje digitalnim podacima. Neki od tih alata su Encase, *FTK Imager, X-Way Forensic.* Kada se radi slika stanja Virtuelne mašine (kod VMware), postoji opcija kojom se bira da li će slika stanja da uključi i memoriju. Ukoliko je ispitivana virtuelna mašina imala uključenu ovu opciju prilikom kreiranja slike stanja, fajlovi „vmem“ će biti prisutni u slici stanja. Alatka napisana od strane Chris Betza koja može da istražuje ove vmem fajlove zove se Memparser[185] [15].

Virtuelni hard disk

[184] Ovo dokumentovanje vremena sa virtuelne mašine ili samog host-a može biti snimljeno kamerom ili fotoaparatom, dok vreme okruženja može biti snimljeno na nekoj zvaničnoj tv stanici ili preko radio aparata.

[185] Dostupno na http://sourceforge.net/projects/memparser

Svaka virtuelna mašina upisuje svoje podatke na virtuelnom hard disku. Za digitalnog forenzičara su veoma važne, njegova lokacija, ekstenzije, veličina i konfiguracija, jer virtuelni hard disk može sadržati potencijalne digitalne dokaze.

Svaki *child* na *host-u*, mora negde da beleži svoje podatke. Virtuelni hard diskovi mogu biti smešteni na SAN[186] (eng. Storage area network) ili NAS[187] (eng. Network Attached Storage) uređaje ili na lokalne hard diskove. Informacija o veličini je bitna, zbog organizovanja kopiranja image-a virtuelnog hard diska na svoj forenzički medij, sa kog će se vršiti dalja ispitivanja. Ovo je važno jer ukoliko se radi o virtuelnim hard diskovima velikog kapaciteta proces može znatno da produži istragu. Zato je važno da iz konfiguracionih fajlova digitalni forenzičar sazna što više informacija o broju particija i da uradi sliku same particije za koju se sumnja da sadrži digitalne dokaze. Te informacije se mogu naći u konfiguracionim fajlovima same virtuelne mašine. Određene ekstenzije[188] moge da ukažu na stanje same virtuelne mašine da li je kompletna ili se radi o slici stanja (eng. snapshot) ili promeni stanja. Ove promene stanja mogu da svedoče o instaliranju određenih programa i korišćenju istih. U odnosu na klasično istraživanje digitalnog mesta krivičnog dela koje se bavi isključivo fizičkim digitalnim okruženjem, informacije koje se odnose na stanje virtuelne mašine mogu se naći samo u virtuelnom okruženju. Takođe, postoje i fajlovi koji nose informacije o konfiguraciji virtuelne mašine koja je predmet istrage. Bitno je razlikovati statičke (definisana veličina) i dinamičke virtuelne diskove (dinamički povećavaju kapacite u zavisnosti od potreba). Bitno je istaći da neki programi za virtuelizaciju mogu da upravljaju virtuelnim hard diskovima na različite načine. Ovo je bitno za digitalnog forenzičara, jer nakon određenih operacija nad virtuelnim hard diskovima može doći do značajnih izmena u strukturi. Postoje operacije koje mogu da smanje veličinu virtuelne mašine uklanjajući neiskorišćeni deo prostora (na hostu bi se taj prostor upisao nulama), zatim, postoje operacije koje mogu da konvertuju dinamičke virtuelne diskove u fiksne i obrnuto ili da fiksne virtuelne diskove prošire, a takođe mogu da izvrše spajanje virtuelnih hard diskova kao i spajanje fizičkog hard diska u novi virtuelni hard disk.

S obzirom da polje virtuelizacije postaje sve veće Microsoft je tehnike virtuelizacije počeo da intergriše u svojim operativnim sistemima, kao na primeru operativnog sistema Microsoft Windows 7. U Konfiguracionom meniju koji se odnosi na upravljanje diskovima (eng. Disk management) moguće je napraviti ili priključiti (eng. mount) virtuelni hard disk (VHD) u read-only modu. Druga korisna opcija je i podizanje računara (eng. boot) sa virtuelnog hard diska (odnosi se samo na Windows vhd fajlove). Ono što se u Windows Visti zvalo Complete PC backup to se u Windows 7 zove System image backup i čuva se u vhd formatu [15]. To je iz perspektive digitalnog forenzičara izuzetno korisno jer takva slika (koja može sadržati veliku količinu korisnih informacija) može da se priključi na forenzički računar u read-only modu.

Slike stanja virtuelnih mašina

Slike stanja (eng. snapshots) virtuelnih mašina imaju široke mogućnosti primene. Mogu da se koriste za evidentiranje nastalih promena na operativnom sistemu, povraćaj

[186] SAN predstavlja uređaj za skladištenje podataka i funkcioniše na nivou blokova podataka i namenjen je enterprise rešenjima. Za razliku od NAS uređaja, SAN uređaji dozvoljavaju deljenje skladištenog prostora na „poolove“ koji mogu da se dodeljuju većem broju servera povezanih direktno (eng. direct attached storage) čime se ostvaruje velika brzina prenosa podataka. Konekcija se vrši optičkim kablom (eng. fibre channel). Sastoji se od velikog broja brzih SAS diskova (15K rpm) a mogu se koristiti i SSD (eng. solid state disk) ukoliko su performanse i ušteda energije prioriteti. Pojavili su se i vendori koji nude kombinovane sisteme tako da podaci mogu biti dostupni i putem blok pristupa preko Fibre channela ili može da im se priđe na nivou datoteka sa očekivanim povećanjima brzine i do 100GBps u narednoj deceniji.

[187] NAS predstavlja uređaj za skladištenje podataka i funkcioniše na nivou datoteka, konekciju sa računarima ostvaruje preko lokalne mreže najčešće preko TCP/IP over ethernet. Sastoji se od veće količine diskova podešeni u raid i najčešće se koriste SAS SCSI ili SATA diskovi. Najčešća uloga NAS-a je fajl server uloga i pruža podršku za fajl sisteme i protokole za Windows umrežavanje CIFS, HTTP, Linux umrežavanja SAMBA, NFS.

[188] Ekstenzije ovih fajlova razlikuju se u zavisnosti od progama koji realizuje virtuelno okruženje.

virtuelne mašine u prethodno radno stanje, ukoliko je instaliranje nekog programa (aplikativnog ili sistemskog) uticalo na promenu u radu operativnog sistema. Za digitalnog forenzičara slike stanja su jako važne, jer bi se na osnovu (sa)znanja trenutka učinjenja protivpravne aktivnosti, preko pokretanja slika stanja (od poslednje ka prvoj) na forenzičkoj mašini, a uz primenu forenzičkih alata, izvršio jednostavan pregled virtuelne mašine za forenzički relevantan trenutak. Na osnovu toga, moguće je izvući podatke iz RAM memorije ili virtuelnog hard diska o delovanju osumnjičene virtuelne mašine. Takođe, veoma interesantno može biti poređenje slika stanja ispitivane Virtuelne mašine sa ciljem praćena promena, izmena fajlova ili prilikom identifikacije skrivenih fajlova. Alatka sa kojom može da se prate ove promene nad Vmware virtuelnim mašinama napisana je od strane Zairon-a[189] i zove se Compare Vmware snapshots [15].

Forenzičke kopije virtuelnih mašina

U dosadašnjoj praksi, kada je reč o digitalnoj forenzici fizičke mašine pravile su se dve kopije fizičkog hard disk-a uz pomoć odgovarajućih forenzičkih alata. Nad jednom kopijom koja se numeriše, izračunavala se heš vrednost MD5 ili SHA algoritma, sa ciljem da se dokaže nepromenjenost tj. integritet hard diska. Ta kopija predstavlja dokazni materijal i čuva se do potrebe dokazivanja pred sudom kako bi se dokazalo da nije bilo promene u bitovima. Druga kopija služi za izvođenje forenzičke analize na forenzičkom računaru. U novije vreme, kada su se pojavile i virtuelne mašine postala je nephodnost da se pravi i treća kopija hard diska sa osumnjičene mašine, što predstavlja još jednu novu specifičnost. Na ovim kopijama se nalaze virtuelni hard diskovi i njihove slike stanja (eng. snapshots) zajedno sa svim folderima i fajlovima koji opisuju virtuelnu mašinu koja je pod istragom. Treća kopija se koristi za ispitivanje na forenzičkoj virtuelnoj mašini u sličnom okruženju o čemu će biti reči u narednom poglavlju. Pravljenje slike operativnog sistema je izuzetno zahtevan proces, jer ne sme biti narušen integritet hard diska. Za tu priliku se uglavnom koristi butabilan disk koji sadrži sve potrebne forenzičke alate, a takođe se može iskoristiti eksterni forenzički uređaj da se na njega smesti slika hard diska osumnjičene mašine. Analizu fajlova sa slike hard diska vršiti na forenzičkom računaru. Kao i u kod svake forenzičke analize voditi dokumentaciju o prikupljenim dokazima a postoje čak i programski alati za tu namenu.

Migracija virtuelne mašine

Jedna bitna karatketristika virutelnog okruženja (kao njen sastavni deo u velikom broju slučajeva) je operacija premeštanja, odnosno migracija virtuelnih mašina. Već je spomenuto da ova operacija donosi niz pogodnosti za administratora virtuelnog okruženja (premeštanje virtuelne mašine sa jednog mesta na drugo u okviru istog fizičkog servera ili na neki drugi fizički server). To, sa druge strane, može da omogući učiniocu protivpravne aktivnosti prikrivanje dokaza o nezakonitom postupanju.

Treba istaći činjenicu, da kada virtuelna mašina migrira, prenose se samo informacije koje sadrže podatke o konfiguraciji koje se koriste pri umnožavanja virtuelnih mašina. Međutim, ukoliko se radi o izvozu virtuelne mašine, tada će biti prenete sve informacije uključujući i slike stanja (ukoliko su postojale). Ove operacije mogu da utiču na digitalnog forenzičara da donese pogrešne zaključke, u slučaju da nisu sprovedene određene pripremne radnje tj. praćenje virtuelnog okruženja.

Zadatak digitalnog forenzičara virtuelnog okruženja je, da na osnovu informacija koje može da prikupi, kao što su podaci o mrežnim adapterima, mrežnoj konfiguraciji samog virtuelnog okruženja, domenu, podatke vezane za virtuelne hard diskove, podatke iz slika stanja sistema (eng. snapshots), podatke o perifernim virtuelnim uređajim, podatke iz RAM

[189] Dostuno na http://zairon.wordpress.com/2007/09/19/tool-compare-vmware-snapshots/

memorije, kreira redosled događaja protivpravne aktivnosti koji će biti potkrepljen kako digitalnim dokazima tako i fizičkim.

Forenzički postupak definitnivno treba da usmeri razvoj ka virtuelnom okruženju, jer neki od klasičnih alata za digitalnu forenziku se ne mogu upotrebiti u potpunosti u virtuelnom okruženju, kako zbog kompatibilnosti sa novijim operativnom sistemima, tako i zbog nepraktične primene samih alata (dinamička i kapacitetska hardverska razvijenost je tolika da bi se celokupna istraga drastično usporila). To je još jedna specifičnost virtuelnog okruženja, pa je zato preporuka da se forenzički postupak virtuelnog okruženja sprovodi što više "uživo", praveći slike particija ili delova diska koji se smatraju da mogu da sadrže potencijalne dokaze. Potrebno je reći i to, da kada je istraga usmerena ka virtuelnom okruženju u kojoj se jedna virtuelna mašina dovodi u vezu sa protivpravnom aktivnošću i ostale virtuelne mašine, takođe je potrebno ispitati na forenzičkoj radnoj stanici. Dakle, sve ovo ukazuje na određene specifičnosti u pristupu prikupljanja podataka, u odnosu na klasičnu digitalnu forenziku fizičkih mašina.

2.4.2 Virtuelno okruženje kao okruženje za digitalno forenzičku analizu

Napredovanje računarske tehnologije i dostupnost moćnih konfiguracija, olakšava posao digitalnim forenzičarima primenom virtuelizacije. Forenzičar danas na jednom računaru poseduje mogućnost da ima više instaliranih operativnih sistema tj. više virtuelnih sistema, koji se ponašaju kao zasebni računari i u pogledu softvera, i što je još bitnije po hardveru. Koncept virtuelizacije i specifičnosti digitalne forenzike virtuelnog okruženja su objašnjene na početku ovog poglavlja, a ovaj deo poglavlja biće posvećen virtuelnom okruženju koje će predstavljati *okruženje za realizaciju* digitalno forenzičke analize u procesu istrage digitalnog mesta krivičnog dela. Biće analiziran jedan opšti koncept virtuelnog okruženja i njegova prikazana ograničenja u primeni digitalne forenzičke analize. Ideja kod ovog pristupa je da se proces digitalne forenzičke analize sprovodi istovremeno pod konvencionalnim i virtuelnim okruženjem nezavisno jedno od drugog, što kao benefit može da ima skraćenje trajanja digitalne forenzičke analize [102]. Fokus ovog poglavlja je jedna faza procesa digitalne istrage odnosno digitalna forenzička analiza. Proces digitalne forenzičke analize može se obuhvatiti u 3 ključne faze kao što su to prikazali Kruse i Heiser u svom modelu [108]: dobijanje dokaza, utvrđivanje autentičnosti i analiza.

Christopher Brown, osnivač jedne od vodećih kompanija koja se bavi digitalnom forenzikom, (CTO of Technology Pathways LLC[190]) ističe da tokom faze prikupljanja (eng. acquire) digitalni forenzičar treba da snimi i zabeleži što je više moguće osetljivih tj. lako izmenjivih (nestabilnih) podataka sa živog sistema (eng. live), zatim sledi isključivanje računara, da bi se na kraju kreirale forenzičke kopije (eng. bit stream copy[191]) svih uređaja za skladištenje podataka tj. hard diskova [19]. Većina autora ističe da se pravljenje forenzičke kopije odnosno slike (eng. image) osumnjičenog hard diska realizuje sa programima koji su bazirani na „dd alatu“ [192] kao i da se dobijena foreznička kopija čuva u dd formatu ili nekom koji je baziran na dd-u [139][164][20]. Dobijena forenzička kopija tj. slika (eng. image) predstavlja identičnu kopiju originalnog diska. Treba napomenuti da se staro pravilo, da slika mora biti identična originalnom disku se u novije vreme ne primenjuje striktno. Postoji priličan broj adekvatnih formata slike originalnog hard diska koji se najčešće koriste, a koji

[190] http://www.techpathways.com/DesktopDefault.aspx, 31.02.2012

[191] Ove bit-stream kopije mogu da budu realizovane kao bit-for-bit kopije ili bit-for-bit plus kopije. Oba pristupa su široko prihvaćena, a razlika je u tome što se kod bit copy plus implementiraju i određeni metadata podaci koji imaju ulogu tagovanja dokaznih fajlova sa ciljem očuvanja lanca nadležnosti [139][20][172].

[192] http://en.wikipedia.org/wiki/Dd_%28Unix%29, 31.02.2012

nisu identični originalnom čvrstom disku, jer mogu sadržati dodatne meta podatke kao na primer, imena istraživača, beleške istraživača ili heš vrednosti. Primer za jedan takav forenzički adekvatan format je popularni napredni forenzički format (eng. Advanced forensic format - AFF) [69][68] razvijen od strane profesora dr Simsona Garfinkela i kompanije Basis Technology[193]. S obzirom da ovaj format podrazumeva segmentiranje originalne slike sa dodavanjem zaglavlja, digitalni forenzičar svoj nalaz zasniva na ispitivanju slike koja je na neki način izmenjena, odnosno nije identična originalu.

Sa druge strane, alat dd daje sliku identičnu originalu koja može biti kreirana na istom ili na hard disku većeg kapaciteta i može biti pokrenuta na drugom računarskom sistemu. Ovde se može pojaviti jedan problem koji se odnosi na ponovno uspostavljanje originalnog okruženja zbog različitih kombinacija hardverskih komponenti računara. Na primer, ukoliko se slika ispitivanog računara pokreće na računaru koji poseduje drugačije hardverske komponente od ispitivanog računara, operativni sistem će pokušati da prepozna razlike i da doda upravljačke programe za nedostajuće hardverske komponente da bi se operativni sistem uspešno startovao. Međutim, u nekim slučajevima sistem neće moći uspešno da se startuje ili će postojati servisi i programi koji neće moći da se pokrenu. Pomenuti problem se odnosi takođe i na primenu u virtuelnom okruženju, jer virtuelne mašine mogu da simuliraju samo osnovne hardverske komponente, a nisu predviđene da imaju podršku za veliki broj hardverskih uređaja. To znači da forenzička slika dobijena sa dd alatom takođe ne može biti pokrenuta bez dodavanja fajlova sa određenim parametrima potrebni za podizanje te slike u novom okruženju. Postoje različiti alati koji mogu da reše ovaj problem. Od komercijalnih alata predstavnika je Encase-ov Physical Disk Emulator [194] i Technology Pathways-ov Prodiscover[195]. Od besplatnih alata to je Live View[196] i neki besplatni alati od Technology Pathways.

U velikom broju literature još uvek se polemiše oko toga da li podaci dobijeni iz virtuelnog okruženja mogu biti relevantni. Razlozi su upravo izmene koje moraju da se primene na sliku originalnog hard diska (originalno okruženje) da bi se omogućilo podizanje u virtuelnom okruženju. Ako se zna da je slika pretrpela značajne izmene, može biti odmah osporena pred sudom, iako IT stručnjak može tvrditi da promene nemaju uticaja na izmenu dokazne snage prezentovanih dokaza. Neki autori smatraju da virtuelno okruženje u ulozi digitalno forenzičkog alata nema perspektivu, što se tiče njihove primene u forenzičkoj analizi [62]. Međutim ukoliko se virtuelno okruženje u ulozi digitalno forenzičkog alata primenjuje u kombinaciji sa klasičnim digitalnim forenzičkim pristupom, analiza podataka se može značajno skratiti i mogu se dobiti bolji rezultati. Jedan od modela koji predlaže ovakav pristup je model Ben i Huebner [16]. Ovaj tip modela podrazumeva dva nivoa digitalno forenzičkog kadra. Prvi nivo predstavlja digitalno forenzičke istražitelje - profesionalce (DFIP) potpuno obučene sa velikim isktustvom koji striktno poštuju metode pravila i procedure digitalne forenzičke istrage. Drugi nivo predstavljaju digitalni forenzički istražitelji - računarski tehničari (DFIRT) sa manje forenzičkog znanja i iskustva i ne moraju se striktno pridržavati forenzičkih pravila i procedura, jer nemaju direktan uticaj na proces izveštavanja. Njihova uloga je da pretražuju kopije digitalnih dokaza u cilju pronalaženja što više podataka od potencijalnog interesa za istragu i da sve što pronađu prijavljuju i prosleđuju digitalnim istražiteljima - profesionalcima koji uz pomoć odgovarajućih forenzičkih tehnika potvrđuju nalaze ili dalje pretražuju podatake ukoliko za tim ima potrebe. Što se tiče okruženja jedna od pouzdanih virtuelnih platformi koja omogućava kreiranje virtuelnih računara i virtuelnih mreža uz korišćenje hardvera jednog sistema jeste Vmware. U forenzičkom smislu ova mogućnost ima brojne prednosti. Na primer, moguće je podešavanje gostujućeg sistema

[193] http://www.basistech.com/e-discovery/ , 13.02.2012

[194]Dostupno na http://www.pc-ware.com/medialibrary/central_files/de/hersteller/software/guidance_software/files/ /guidance_07_06_19_encase_forensic_prosuite.pdf, 16.02.2012

[195] http://www.techpathways.com/prodiscoverdft.htm, 16.02.2012

[196] http://liveview.sourceforge.net/, 16.02.2012

prema forenzičkim potrebama, kreiranje slike stanje sistema, rad na njemu i vraćanje sistema u početno predefinisano stanje. Sa takvog virtuelnog sistema moguće je vršiti sva forenzička ispitivanja, uključujući instaliranja i praćenja zlonamernih programa kao i simulacije sigurnosnih incidentnih aktivnosti. Dodatni benefit uključivanja virtuelne platforme u forenzičko istraživanje jeste mogućnost „zamrzavanja“ rada na virtuelnoj stanici. Tako suspendovanom virtuelnom sistemu lako je dostupan sadržaj fizičke memorije koji se nalazi u datoteci sa ekstenzijom *.vmem. Treba napomenuti da je format ove datoteke veoma sličan sa dd image fajlovima, koji se dobijaju forenzičkim prikupljanjem, tako da se one mogu uspešno analizirati[197]. Kada je reč o prenosivim uređajima, Vmware poseduje opciju u kome gostujući operativni sistem nema kontakta sa hostom (domaćinom) čime se blokira veza izmeću prenosivog uređaja i operativnog sistema. Savet je da se primenjuje određena Write protect zaštita (kao na primer one opisane u poglavlju 2.3) na operativnom sistemu sa kojeg se podiže Vmware virtuelna radna stanica.

Ilustrativan primer forenzičke primene u virtuelnom okruženju bi bio sledeći : računarski tehničari pokreću kopiju prikupljene slike u virtuelnom okruženju (kao virtuelnu mašinu), tretirajući je kao normalan sistem i "uživo" pretražuju sve detalje relevatne za istragu. Iako metodologija koju koristi računarski tehničar utiče na integritet prikupljene slike originalnog sistema, to ne utiče na istragu. Razlog je taj, što računarski tehničar radi sa jednom od kopija digitalnih slika osumnjičenog hard diska. Što znači da računarski tehničari koji poseduju dobra tehnička, a manje forenzička znanja mogu primenjivati računarske forenzičke tehnike u fazama bez ugrožavanja digitalnih dokaza.

Podrazumeva se, da se nad jednom kopijom primenila funkcija heš-iranja sa ciljem očuvanja integriteta i ona je sklonjena na sigurno mesto, dok je druga kopija u posedu digitalnih istražitelja - profesionalaca i ona je netaknuta i forenzički validna [204].

Na osnovu dobijenih informacija od strane računarskih tehničara, DFIP mogu potvrditi sve rezultate koristeći odgovarajuće forenzičke alate pridržavajući se striktno odgovarajuće forenzičke metodologije tehnike i procedura. Na osnovu iznetog može se zaključiti da ovakvim forenzičkim pristupom (kombinacija klasičnog i virtuelnog pristupa), koji se ostvaruje kroz saradnju timova različitih nivoa stručnosti koristeći različite tipove alata mogu se dobiti brže rezultati kada je reč o fazi digitalno forenzičke analize (čime se štedi vreme), i smanjuje se opterećenje na digitalno forenzičke istražitelje - profesionalce (a to je veoma bitno jer postoji manjak kadra forenzičkih profesionalaca).

[197] http://www.forensicfocus.com/vmware-forensic-tool, 16.02.2012

3. DIGITALNA FORENZIKA WINDOWS I LINUX RAČUNARSKIH SISTEMA

Pre svake istrage podrazumeva se ispitivanje potrebnih preduslova kao što su : postojanje dovoljnog broja obučenih profesionalaca, forenzičke radne stanice i forenzičku laboratorije za oporavak podataka, saradnja sa javnim tužilaštvom i definisana metodologija. U zavisnosti od tipa istrage (zvanična ili korporativna) zavisi i ko će dati prvi odgovor na incidentnu /protivpravnu aktivnost.

Koliku važnost ima forenzički odgovor i koliko je on osetljiv, možda je i najslikovitiji opis o potrazi za digitalnim podacima dao Fridman u sledećim rečenicama svoje knjige :
"*Svi podaci ostavljaju trag. Potraga za podacima ostavlja trag. Brisanje podataka ostavlja trag. Odsustvo podataka pod određenim okolnostima može da ostavi najjasniji trag od svih.*"[66]

Zaista, digitalni podaci su po svojoj prirodi tragovi u računaru. Digitalni podaci generisani ili uneti u računar ostavljaju brojne tragove u Windows operativnim sistemima. Pretraga za podacima podrazumeva priključivanje forenzičkog alata, što znači ostavljanje tragova na digitalne podatke (Lokardov zakon). Izbrisani podaci ostavljaju tragove u nealociranim i slek prostorima diska, a odsustvo podataka ukazuje na antiforenzičku aktivnost i predstavlja jaku osnovu za sumnju u protivpravne aktivnosti. Virusi, na primer, ostavljaju svoj kod u zaraženim programima. Tragovi kompromitovanja mogu biti u prisutni u različitim oblicima na primer, u izvornim fajlovima programskog jezika, u objektnim fajlovima (eng. Object files), u izvršnim kodovima, u šel skriptama, u izmenema nad postojećim programima ili čak u tekstuelnim fajlovima pisanim od strane napadača. Za istragu je vrlo značajno ukoliko bi se ovi delovi informacija mogli iskoristiti za utvrđivanje izvora napada [180].

Istraživanje incidentnih/protivpravnih aktivnosti podrazumeva prikupljanje podataka (digitalnih dokaza) sa računarskih sistema i mrežnih uređaja, utvrđivanje autentičnosti i njihova analiza.

Prikupljanje podataka može da podrazumeva prikupljanje podataka iz živog sistema (eng. live) da bi se sakupile osetljive tj. nestabilne informacije ili se vrši post-mortem prikupljanje podataka bez izmene ili oštećenja i u tom slučaju se vrši preuzimanje fizičkih dokaza (kao na primer hard diskovi, diskete ili drugi mediji). Nakon preuzimanja fizičkih dokaza vrše se forenzička dupliranja – uzimanje imidža ili kloniranje diska računarskih dokaza i utvrđuje se autentičnost između originalnog digitalnog dokaza sa forenzičkom kopijom. Paralelno se vrši istraživanje i nadzor mreže za dobijanje dodatnih informacija. Pored toga, za dobijanje dodatnih informacija vrše se i intervjui sa odgovarajućim ljudima koji imaju određene detalje u vezi sa incidentnom, odnosno protivpravnom aktivnošću .[198]
Kada se podaci prikupljaju iz "živog" operativnog sistema važno je znati koji su to podaci promenljivi tj. podaci privremenog karaktera (eng. volatile), a koji podaci su postojanog karaktera (eng. non-volatile). Na prvom mestu "lako izmenjivi" podaci, odnosno volatile podaci, su sistemski detalji koji istražiteteljima pružaju uvid u način i prirodu kompromitovanja sistema i nekada mogu biti podaci od krucijalnog značaja. Na primer, to su detalji koji pružaju informaciju o tome ko je ulogovan na sistem, informacije o aktivnim mrežnim konekcijama i pokrenutim procesima na sistemu [115]. Na drugom mestu su podaci

[198] Na primer, u organizacijama uglavnom je potrebno sprovodi kadrovske intervjue sa administratorima sistema i mreže, menadžerima i krajnjim korisnicima. Sa administratorima sistema i mreže pitanja mogu da se odnose na neuobičajene aktivnosti na mreži ili računarskim sistemima, administrativne pristupe sistemima, mogućnosti udaljenog pristupa, da li postoje logovi na sistemima, kao i na postojanje trenutnih bezbednosnih mera. Sa menadžerima organizacije pitanja mogu da se odnose na postojanje osetljivih podataka ili programa na sistemu, istoriji trenutno zaposlenih, nezadovoljstvo zaposlenih i da li je neko u skorije vreme bio otpušten. Pitanja za krajnje korisnike uglavnom treba da obuhvate sumnjive aktivnosti i neuobičajeno ponašanje računara koje korisnik koristi.

koji su po prirodi privremenog karaktera, ali su korisni istražitelju jer može dopuniti informacije o sistemskim detaljima. Na primer, podaci iz privremene memorije (eng. clipboard) i podaci iz planiranih zadataka za pokretanje na sistemu (eng. scheduled tasks).

Od podatka koji neće lako biti izmenjeni na sistemu, na prvom mestu su oni koji daju informacije o statusu, setovanjima i konfiguraciji sistema, na osnovu kojih se može utvrditi način kompromitovanja sistema. Na primer, tu su setovanja registra (eng. registry) i auditinga (praćenje tragova aktivnosti na sistemu). Važnost auditing logova može se sagledati iz sledećih značajnih razloga [59] :

- **odgovornost** - log podaci identifikuju naloge koji su povezani sa određenim događajima (na primer, gde je potrebna dodatna obuka a gde disciplinske mere);
- **rekonstrukcija** - forenzičari na osnovu logova mogu utvrditi vremenski sled ispitivanih događaja;
- **detekcija upada na sistem** - na osnovu pregledanja logova mogu se identifikovati neovlašćeni i neuobičajeni događaji (na primer, neuspeli pokušaji prijava na sistem, zaključani nalozi, prijave na sistem van definisanog vremena, mrežne aktivnosti, visoka iskorišćenost radne memorije…);
- **detekcija problema** - forenzičari i administratori mreže i sistema koriste log podatke za identifikovanje bezbednosnig događaja i problema koje treba rešavati.

Na drugom mestu neizmenjivih podataka su oni podaci koji pružaju istorijske informacije i dodatni kontekst za razumevanje načina i prirode kompromitovanja sistema. Na primer, to su podaci iz logova događaja (eng. event log) i iz istorije Internet pretraživača (eng. Web browser history).

Veoma je važno da se inicijalni tookit (skup alata) dobro pripremi. To podrazumeva korišćenje pouzdanog toolkit-a za inicijalni odgovor koji sadrži pouzdano kreirane binarne izvršne datoteke, pokretanje komandi sa pouzdanog mediuma koje mogu da se pokreću iz komandnog okruženja. Pri kreiranju inicijalnog toolkita obratiti pažnju, da li se neke binarne datoteke oslanjanju (eng. dependencies) na biblioteke ili zavise od nekih drugih fajlova. U nastavku bih naveo osnovne alate koji su neophodni pri inicijalnom odgovoru.

Na osnovu iznete klasifikacije izmenjivih i neizmenjivih podataka u daljem teksu biće prikazani specifični tipovi izmenjivih podataka koji su veoma značajni za forenzičku analizu. To su : sistemsko vreme, ulogovani korisnici, otvoreni fajlovi, informacije o mreži, mrežne konekcije, informacije o procesima, status mreže, sadržaj privremene memorije za skladištenje (eng. clipboard), mapiranje procesa na portove, procesi u memoriji, spisak servisa, istorija pokrenutih komandi, mapirani drajvovi, deljeni resursi na mreži (eng. shares).

Za svaki od ovih tipova izmenjivih podataka postoje određeni alati koji mogu poslužiti da bi se ovi podaci dobili iz sistema [32][31]. Prilikom prikupljanja podataka redosled prikupljanja treba prilagoditi prema karakteru postojanosti podataka. To znači da podaci koji su skloniji brzim promenama treba da budu sačuvani na prvom mestu. Očekivani vek trajanja podataka u zavisnosti od postojanosti podataka dat je u tabeli 4. :

Tabela 4 : Očekivani vek trajanja podataka [61]

Tip podataka	Vek trajanja
Registri, periferna memorija, keš	Nanosekunde
RAM memorija	10 nanosekundi
Mrežno stanje	Milisekunde
Startovani procesi	Sekunde
Disk	Minuti
Flopi drajv i drugi mediji za bekap	Godine
Cd-rom, DVD-rom, odštampani papiri	Desetine godina

Treba skrenuti pažnju da, čak, iako postoji plan i inicijalni toolkit za odgovor, odgovor "uživo" može da bude prilično dugotrajan, takođe inicijalni odgovor može da bude pun izazova za onog ko ga izvodi zbog postojanja različitih nepravilnosti koje moraju biti prepoznate na vreme. Ovaj forenzički odgovor ima za cilj pronalaženje što većeg broja dokaza, otkrivanje relevantnih podataka, očuvanje podataka prema njihovoj osetljivosti, (eng. volatile), sprečavanje spoljašnje izmene podataka uz pripremu lanca očuvanja nadležnosti za pronađene dokaze, sa kompletno dokumentovanim aktivnostima.

U skladu sa navedenim ciljem forenzičkog odgovora, ovaj rad će biti orijentisan ka prikupljanju podataka iz "živog" sistema, sa određenih mesta na sistemu koji mogu ukazati na one forenzičke relevantne događaje koji utiču na bezbednost sistema. Prikupljanje podataka, kao što je pomenuto, podrazumeva prikupljanje podataka sa računarskih sistema i prikupljanje podataka sa mreže. S obzirom da je fokus ovog rada usmeren ka računarskim sistemima baziranih na Windows i Linux platformama, biće prikazani alati i tehnike za prikupljanje dokaza sa pomenutih računarskih sistema (eng. host based evidence). Prikupljanje dokaza sa mreže i sa mrežnih uređaja (eng. network based evidence), nisu predmet ovog rada.

3.1 Forenzički odgovor na protivpravnu / incidentnu aktivnost "uživo" na Windows platformi

Tradicionalne metodologije prikupljanja digitalnih dokaza opisanih ranije u prethodnim poglavljima i dalje predstavljaju najispravniji način prikupljanja prema zakonskoj regulativi. Međutim glavna ograničenja efektivnosti ovog modela su veliki porast kapaciteta HDD (reda TB -terabajta) sa enormnom količinom informacija i sve veći broj sistema kritičnih za misiju organizacija koji zahtevaju neprekidni rad [72].

Obezbeđivanje integriteta podataka je od krucijalne važnosti za svaki tip istrage koji se sprovodi od strane pravosudnih organa. Očuvanje digitalnih dokaza prikupljanjem kroz prikupljanje sistema (forenzičkim kopijama) i dalje će biti standard u narednim godinama [175]. Ipak, postoje izuzeci od pravila. U praksi se dešavaju takve okolnosti da u toku istrage ispitivanog računara postoji potreba da se vrši ispitivanje sistema „uživo“. Istraga uživo dozvoljava forenzičarima da prikupe sa sistema lako izmenjive podatke kojih neće biti u post-mortem forenzičkoj analizi [160].

To znači da se na mestu incidentne radnje, odnosno protivpravne aktivnosti mora doneti odluka, da li da se računar ugasi i uklanja sa mreže, pa da se tek onda prikupljaju potencijalni dokazi ili da se radi digitalna forenzika na "živom" sistemu [166]. Ova odluka ne zavisi samo od incidentne radnje, odnosno protivpravne aktivnosti, već i od tipa samih sistema kao na primer veliki kritični sistemi banaka ili elektronskog poslovanja. Uslovi u kojima se javlja potreba za ispitivanjem računara “uživo” postaju sve učestaliji. Ispitivanje računarskog sistema “uživo” treba da bude strukturirano tako da bude ciljano i da se brzo i efikasno sprovede od strane stručnjaka. U suprotnom, raste verovatnoća pojavljivanja novih pravnih izazova, odnosno odbacivanja dokaza. Član 16 i Član 84. Zakonika o krivičnom postupku definišu kada se dokazi mogu odbaciti. Čl. 16. glasi: Sudske odluke se ne mogu zasnivati na dokazima koji su, neposredno ili posredno, sami po sebi ili prema načinu pribavljanja u suprotnosti sa Ustavom, ovim zakonikom, drugim zakonom ili opšteprihvaćenim pravilima međunarodnog prava i potvrđenim međunarodnim ugovorima, osim u postupku koji se vodi zbog pribavljanja takvih dokaza. Sud je dužan da nepristrasno oceni izvedene dokaze i da na osnovu njih sa jednakom pažnjom utvrdi činjenice koje terete ili idu u korist okrivljenom. Izvedene dokaze koji su od značaja za donošenje sudske odluke sud ocenjuje po slobodnom sudijskom uverenju. Presudu, ili rešenje koje odgovara presudi,

sud može zasnovati samo na činjenicama u čiju je izvesnost uveren. Sumnju u pogledu činjenica od kojih zavisi vođenje krivičnog postupka, postojanje obeležja krivičnog dela ili primena neke druge odredbe krivičnog zakona, sud će u presudi, ili rešenju koje odgovara presudi, rešiti u korist okrivljenog. Član 84. glasi: Dokazi koji su pribavljeni protivno članu 16. stav 1. ovog zakonika (nezakoniti dokazi) ne mogu biti korišćeni u krivičnom postupku. Nezakoniti dokazi se izdvajaju iz spisa, stavljaju u poseban zapečaćeni omot i čuvaju kod sudije za prethodni postupak do pravnosnažnog okončanja krivičnog postupka, a nakon toga se uništavaju i o tome se sastavlja zapisnik. Izuzetno od stava 2. ovog člana, nezakoniti dokazi se čuvaju do pravnosnažnog okončanja sudskog postupka koji se vodi zbog pribavljanja takvih dokaza.

Ukoliko je reč o forenzici na "živom" računarskom sistemu potrebno će biti snimanje stanja RAM memorije i page fajla (swap), otvorenih fajlova, otvorenih portova i otvorenih konekcija prema preporuci koja je detaljno objašnjena u dokumentu *RFC 3227: Guidelines for Evidence Collection and Archiving*[199], da bi se minimizirale promene napravljene na samom sistemu.

Cilj odgovora na incident "uživo" je da se potvrdi da li je postojao incident i ako jeste da li se radi o protivpravnoj aktivnosti ili incidentnoj radnji.

Odgovor na protivpravnu aktivnost "uživo" u praksi podrazumeva pokretanje samo proverenih komandi na kompromitovanom računarskom sistemu sa prethodno uspostavljenim bezbednim komandnim okruženjem [201][42]. To znači da se ne smeju pokretati alati koji se nalaze na ispitivanom računaru. Razlog je taj što fajlovi na ispitivanom računaru mogu biti sadržati zlonamerne kodove, prikrivati prisustvo zlonamernog napadača, inicirati pokretanje logičkih bombi na sistemu i drugih zlonamernih aktivnosti [7]. Takođe, prilikom odgovora na incident ""uživo"" mora sa voditi računa o jednom vrlo važnom već pomenutom principu - Lokardov princip razmene. Kada smo u interakciji sa "živim" sistemom, bez obzira da li smo korisnik, administrator ili digitalni forenzičar, promene će nastati na tom sitemu, što predstavlja potencijalni problem. S obzirom da sistema nije statički promene na "živom" sistemu dešavaju se kao rezultat procesa rada, snimanja ili brisanja fajlova, prilikom kreiranja ili prekida mrežnih konekcija, a mogu se desiti čak samo protokom vremena odnosno radom samog sistema[200]. Međutim to ne mora nužno da ih poništi kao dokaz. Na primer, kod Windows Vista operativnog sistema prema difoltnoj konfiguraciji program za defragmentaciju je podešen da se izvršava svake srede u 03:00 časa [28]. Prilikom istrage ovu informaciju treba uzeti u razmatranje, jer korisnici uglavnom ne menjaju ovu difoltnu postavku. Isto tako iako se sistemski log fajlovi stalno menjaju i mailovi neprestano dolaze, aktovnosti koje se tiču prikupljanja dokaza sa sistema neće stvoriti inkriminišuću poruku poslatu od strane osumnjičenog [65].

Prema tome, promene nastaju samim protokom vremena i u slučaju kada digitalni forenzičar izvršava programe na sistemu da bi prikupio informacije i podatke, kako one koji su po prirodi lako izmenjivi (eng. volatile) tako i one koji to nisu.

U daljem tekstu biće naveden primer Lokardovog principa sa Alatom Netcat koji za cilj ima demonstraciju pomenutog principa i prikupljanje podataka sa ispitivanog računara. Alati koji će biti korišćeni su Netcat[201], Pmdump[202] i Strings[203]. Potrebne su dve radne stanice, jedna ispitivana i jedna forenzička. Postupak je sledeći :

1. Na ispitivanoj mašini pokreće se alatka Netcat sa sledećim parametrima:
c:\pmdump.exe -list | nc.exe IP_ADRESA_FORENZIČKE_RADNE_STANICE 9898

[199] RFC 3227: Guidelines for Evidence Collection and Archiving dostupno na http://www.faqs.org/rfcs/rfc3227.html

[200] Na primer kod Windows XP operativnog sistema prema defaultnim sistemskim postavkama kreiraće se posle 24h System restore point. Ukoliko sistem radi neprekidno 3 dana bez ikakve interakcije biće sprovedena delimična defragmentacija podataka.

[201] Dostupno na http://joncraton.org/media/files/nc111nt.zip

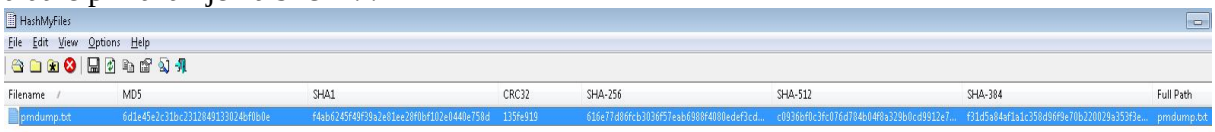
[202] Dostupno na pmdump : http://ntsecurity.nu/downloads/pmdump.exe

[203] Dostupno na http://download.corrupteddatarecovery.com/download-file/strings.exe

Umesto pmdump.exe -list komande može biti bilo koja komanda koja se pokreće sa ciljem prikupljanja podataka sa živog sistema. Izlaz komande šalje se preko TCP kanal na porta 9898 na forenzičku radnu stanicu, gde će se podaci snimati u fajl pmdump.txt umesto na hard disk ispitivanog računara.

2. Na forenzičkom računaru pokreće se alatka Netcat sa sledećim svičevima :
"*c:\nc.exe -v -l -p 9898 > pmdump.txt*"
Ova komanda podrazumeva da program netcat sluša (svič -l) na portu (svič -p) 9898 u verbose modu (svič -v)[204]. Nakon pokrenute komande na ispitivanom računaru svi podaci koji se šalju na TCP port 9898 forenzičke radne stanice biće snimljeni u pmdump.txt.
U task menadžeru ispitivanog sistema možemo primetiti nc.exe sa identifikatorom procesa (eng. PID) koji je potrebno zapisati jer je to upravo nov proces koji se pridodao ispitivanom računaru.

Ova komanda podrazumeva pokretanje programa netcat u klijentskom modu i da se konektuje na port 9898 IP adrese ispitivanog računara. Nakon uspostavljene konekcije sa ispitivanim računarom pojaviće se komandno okruženje (eng. command prompt) sa verzijom operativnog sistema. Komande koje budu pozivane izvršavaće se kroz uspostavljenu konekciju.
Nakon što se komanda izvrši sesija se prekida pritiskom tastera CTRL-C. Nakon toga poželjno je uraditi MD5 checksum pmdump.txt fajla sa alatkom md5sum za dokazivanje autentičnosti sa komandom :
md5sum -b pmdump.txt > pmdump.md5, gde parametar -b govori md5sum komandi da izračuna MD5 heš u binarnom modu.
Zbog veće pouzdanosti mogu se koristiti dodatni heš algoritmi. Na primer, alatka Hashmyfiles[205] generiše MD5, SHA1, CRC32, SHA-256, SHA-384 heš vrednosti. Izlaz ove alatke prikazan je na slici 7. :



Slika 7. *Izlaz alatke Hashmyfiles sa različitim heš vrednostima*

Treba napomenuti da forenzičar može koristiti i netcat varijantu koja se zove Cryptcat[206]. Ona omogućuje zaštićen prenos podataka preko mreže tj. TCP kanalom pružajući zaštitu poverljivosti i autentičnosti. S obzirom da je komunikacija šifrovana napadač nije u mogućnosti da vidi podatke koji se prikupljaju prilikom forenzičkog ispitivanja.

Za iščitavanje prikupljenog fajla koji predstavlja listu procesa u memoriji mogu se koristiti ili besplatne alatke kao što su Systernals Strings.exe [207] ili FoundStone-ov BinText.exe [208] ili određeni komercijalni programi kao što su AccessData FTK [209], ENCASE[210]. U njemu će biti prikazana i IP adresa forenzičkog računara što predstavlja i demonstraciju Lokardovog principa.

To znači da programi koji se koriste za prikupljanje informacija (bez obzira što se podaci ne snimaju direktno na hard disk ispitivanog računara) imaju određeni uticaj na "živi " sistem. Na primer, neki programi će morati da isčitavaju više registarskih ključeva iz baze

[204] Netcat alatka može biti pokrenuta i u nevidljivom modu (svič -d) izvršavajući određeni program koristeći svič -e, na šta forenzičar treba posebno da obrati pažnju ukoliko je takva komanda pokrenuta na ispitivanom računaru. To može biti i pokazatelj namera zlonamernog korisnika.
[205] Dostpuna na http://www.nirsoft.net/utils/hash_my_files.html , pristupljeno 05.02.2013.
[206] Dosputna na http://sourceforge.net/projects/cryptcat/files/ , 05.02.2013.
[207] Dostupno na http://technet.microsoft.com/en-us/sysinternals/bb897439.aspx, pristupljeno 11.02.2013.
[208] Dostupno na http://www.softpedia.com/developer/Foundstone-Inc-16182.html , 05.02.2013.
[209] Dostupana na http://www.accessdata.com/products/digital-forensics/ftk , 05.02.2013.
[210] Dostupna na http://www.guidancesoftware.com/encase-forensic.htm , 05.02.2013.

registra, i te putanje do ključeva biće učitane u memoriju. Na primer, Windows sistemi[211], imaju implementiran prefečing (eng. prefetching) za aplikacije koji služi za ubrzavanje svakodnevnog rada u Windows okruženju. Ono što je važno pomenuti je da se sve akcije (vezane za određene aplikacije, ne samo podizanje sistema, već i korišćenje određenih delova tih programa), koje pokreće korisnik administrator ili digitalni forenzičar na računarskom sistemu, beleže u određeni direktorijum "C:\Windows\Prefetch" (kada je u pitanju Windows XP). Kao benefit se dobija brže podizanje sistema, odziv sistema kao i brži odziv aplikacija. Analogijom se može uporediti sa nekom vrstom keša.

Ukoliko digitalni forenzičar pokreće program koji je već pokrenut na sistemu od strane korisnika, biće modifikovano vreme, poslednji pristup i sadržaj prefetch fajla. Ukoliko digitalni istražitelj pokreće program koji ne postoji na sistemu kreiraće se novi prefetch fajl u C:\Windows\Prefetch direktorijumu. Kod Windowsa XP Limit kreiranja ovih fajlova je 128 nakon čega se direktorijum prazni, ali ostaju 32 najčeće korišćena prefetch fajla. Kod Windows Viste limit kreiranja jeste 134 fajla [28]. Na osnovu navedenog proizilazi da je digitalnom forenzičaru potrebno ne samo znanje da se ove promene dešavaju već je potrebno i dokumentovanje tih promena da bi mogli da objasne uticaj njihovih akcija na ispitivani sistem. Na primer, ukoliko korisnik pokrene aplikaciju "Notepad", sistem će prifečovati fajl smeštajući ga u prifeč direktorijum i imenovati ga sa ekstenzijom .pf na kraju. Uz ime postojaće i dodatni heksadecimalni karakter koji predstavljaju heš vrednost putanje do fajla, što bi u praksi izgledalo kao "notepad.exe-598342B8". Ukoliko takav fajl postoji, za digitalnog forenzičara to je signal da je ta aplikacija pokrenuta na sistemu. Takođe je važno spomenuti i da prifeč fajlovi sadrže i metadata podatke kao na primer, datum kreiranja prifeč fajla, koliko je puta startovan program, kada je poslednji put startovan program, volume i putanju odakle je program startovan. Ti podaci forenzičaru mogu ukazati na datum kada je program prvi put startovan (pod pretpostavkom da prethodni prifeč fajl nije obrisan i da na njegovo mesto nije kreiran novi) i na putanju (uređaja ili drajva) sa kog je program startovan. Programi koji mogu da izvuku metadata podatke iz prefetch fajlova su bintext (već pomenut) koji ima grafički interfejs, prefetch_info[212] koji se pokreće iz komandnog okruženja i zgodan je za forenziku "uživo", alat WFA sa grafičkim interfejsom, TzWorkLLC-ov Windows prefetch parser[213] koji se pokreće iz komandnog okruženja, skripte Harlana Carvey koje se dobijaju uz knjigu Windows forensic analysis [32] i koje rade sa prefetch fajlovima koje generiše Windows XP i Windows Vista, SuperFetch files dumper[214], koji je zgodan za analizu superfetch fajlova (sa ekstenzijama .db) koje generišu Windows Vista, Windows 7, Windows 2008. Svi ovi programi mogu forenzičaru pomoći u kreiranju slike o redosledu događaja na ispitivanom računaru.

Prema preporuci NIST-a [96] redosled prikupljanja lako izmenjivih podataka sa računarskih sistema radi se na sledeći način :

1. Mrežne konekcije;
2. Logovani korisnici i sesije;
3. Sadržaj memorije;
4. Pokrenuti procesi;
5. Otvoreni fajlovi;
6. Mrežna podešavanja;
7. Vreme operativnog sistema.

[211] Windows XP, Vista, Windows 7 po difoltu imaju uključen prefetch-ing dok je kod Windows 2003 i Windows 2008 ostavljena mogućnost da se uključi ali je po difoltu ona onemogućena.

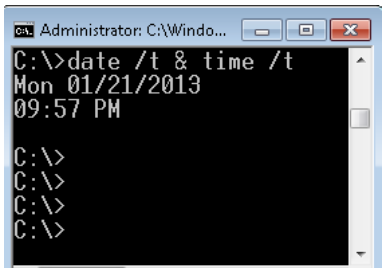
[212] Dostupno na http://redwolfcomputerforensics.com/downloads/prefetch_info.zip, 05.02.2013.

[213] Dostupno na http://www.tzworks.net/prototype_page.php?proto_id=1, 05.02.2013.

[214] Dostupno na http://code.google.com/p/rewolf-superfetch-dumper/downloads/detail?name=rewolf.superfetch.dumper.v1.0.zip&can=2&q=, 05.02.2013.

3.1.1 Podaci od značaja privremenog karaktera na Windows-u - datum i vreme

Operativni sistem skladišti informacije o tekućem vremenu (pomeranju vremena) i vremenskoj zoni. Ove informacije su izuzetno korisne prilikom izgradnje hronologije događaja ili korelacije događaja između različitih sistema. Forenzičar treba da bude svestan da može postojati razlika u vremenu između onog koje prikazuje Operativni sistem i onog vremena iz BIOS-a zbog specifičnih setovanja u Operativnom sistemu, kao što su vremenske zone [96]. Prikupljanje podataka o vremenu i datumu će biti od velike važnosti i jer će doprineti stavljanju u kontekst podatke prikupljene u daljem toku istrage i pomoći u izradi precizne hronologije dešavanja na sistemu. Treba napomenuti i to, da je od značaja i vreme neprekidnog rada računarskog sistema tzv. eng. uptime. Ono se može dobiti putem posebnog alata koji je dostupan na Microsoft-ovom[215] sajtu sa web adresom prikazanom u tabeli. Preporuka je i da se paralelno uslika i realno vreme na primer, slikanje vremena na zidnom satu. Dodatno važna informacija koja može biti korisna u daljem toku istrage jeste vremenska zona podešena na ispitivanom računaru[216] (slika 8.).



Slika 8. *Prikaz datuma i vremena na sistemu*

Takođe trenutno vreme se može dobiti uz pomoć Perl skripte. Sledeća linija koda može se pridodati bilo koji skripti i ona će prikazati trenutni datum i vreme na sistemu [33]:
print localtime(time)."\n";

Za forenzičara osim trenutnog vremena važan podatak može biti i ukupno vreme rada računarskog sistema tzv. Uptime. Taj podatak može biti dragocen, jer svedoči o tome da li je sistem radio u vreme dešavanja forenzički relevantnog događaja ili nije. Alati koji to mogu prikazati su Systeminfo.exe (nalazi se u sastavu Windows XP, 2003, Vista, 7) i psinfo.exe (dostupan preko nekadašnjeg SysInternals.com odnosno sadašnjeg Windows systernals[217]).
Sa preciznom analizom datuma i vremena mogu se proizvesti dokazni podaci koji dokazuju kada su se određene akcije desile. Kada se radi u različitim vremenskim zonama ili usled promene vremena bitno je konstatovati da li je vreme prevedeno na univerzalno kodirano vreme tzv. UTC ili se koristi lokalno vreme. Ključ koji sadrži informacije i vremenskoj zoni i promeni vremena nalazi se u Registarskoj bazi :

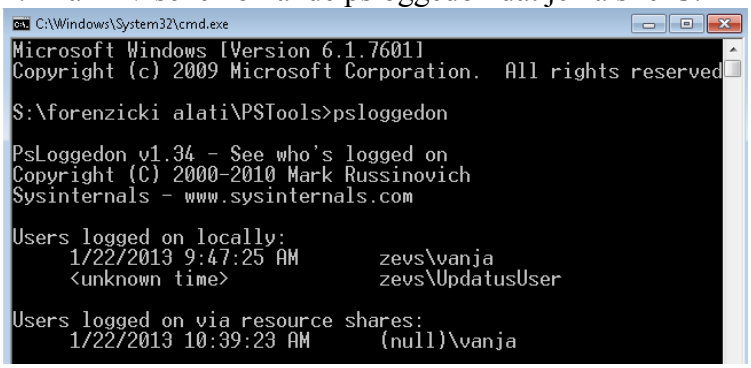
„HKLM\SYSTEM\CurrentControlSet\Control\TimeZoneInformation“

Iako ova informacija nije direktno korisna, od izuzetnog je značaja pri konvertovanju vremenskih pečata ukoliko je računar premešten ili ukoliko je vremenska zona pogrešno podešena.

[215] www.microsoft.com/
[216] Windows sistemi koji koriste NTFS fajl sistem čuvaju podatke o vremenu u UTC formatu, dok sistemi sa FAT fajl sistemom čuvaju podatke o vremenu iz lokalnog sistemskog vremena. Dostupno na http://msdn.microsoft.com/en-us/library/Windows/desktop/ms724290%28v=vs.85%29.aspx, 05.02.2013.
[217] http://technet.microsoft.com/en-US/sysinternals

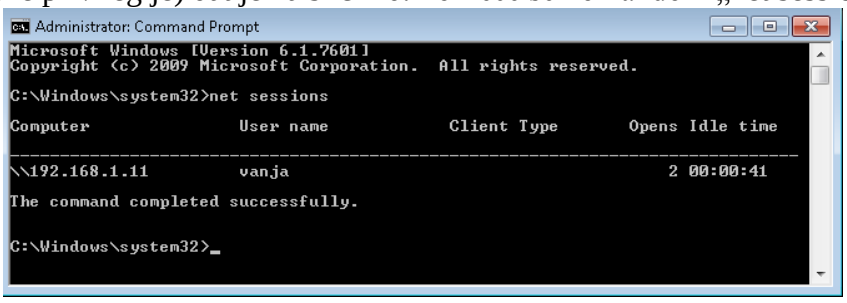
3.1.2 Podaci od značaja privremenog karaktera na Windows-u - Logovani korisnici na sistemu i sesije

Prilikom forenzičkog istraživanja ispitivanog računara, značajno za dalji tok istrage će biti spisak ulogovanih korisnika na sistem kao i postojeće sesije. U nastavku će biti prikazani alati koji digitalnom forenzičaru to omogućuju. Korisnici mogu biti prijavljeni na sistem lokalno, preko konzole ili mogu biti udaljeni korisnici koji koriste "net use" komande i deljene resurse ispitivanog računara. Dobijene informacije o korisnicima i sesijama na sistemu pružaju uvid : u startovanje procesa od strane korisnika/zlonamernog korisnika, vlasništva nad fajlovima kao i poslednji pristup fajlovima. Ukoliko se ovi podaci posmatraju zajedno sa podacima iz bezbednosnih logova događaja (eng. security event log) , u slučaju da je uključen auditing na sistemu, mogu doprineti još boljem razumevanju ispitivanog slučaja na sistemu. Bez konfigurisanog praćenja tragova aktivnosti na sistemu izuzetno je teško uspešno ispitati sigurnosni incident. Besplatna alatka koja digitalnom forenzičaru može pružiti pomenute informacije o korisnicima je psloggedon koja može da se preuzme sa sajta prikazanog u tabeli. Izlaz izvršene komande psloggedon dat je na slici 9.



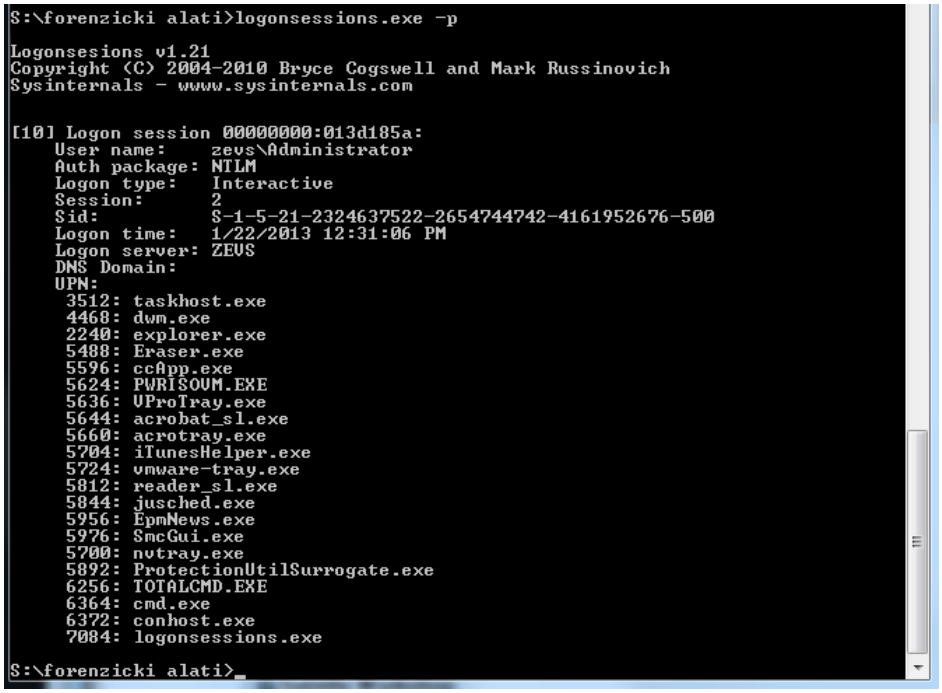
Slika 9. *Prikaz ulogovanih lokalnih i udaljenih korisnika preko deljenih resusra na Windows 7*

Izlaz komande net sessions (koja mora da bude pokrenuta sa nalogom koji ima administratorske privilegije) dat je na slici 10. Pokreće se komandom „net sessions“



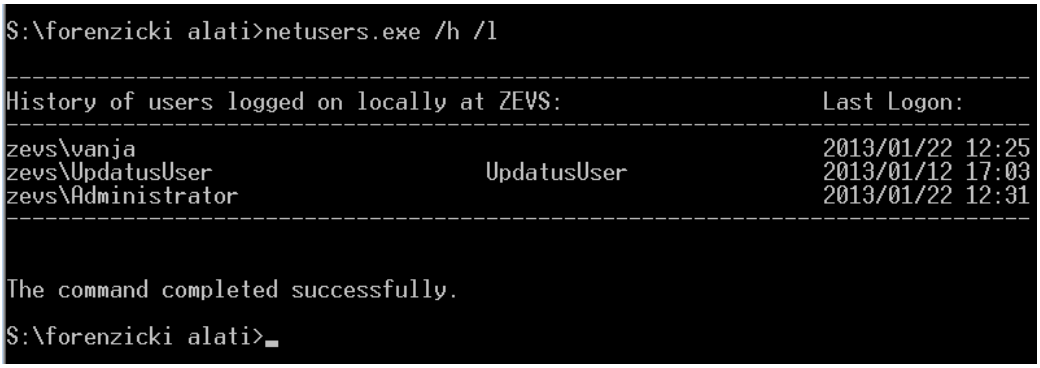
Slika 10. *Prikaz imena udaljenog korisnika koristi deljene resurse sa IP adresom*

Besplatan alat logonsession.exe (može da se preuzme sa sajta prikazanog u tabeli) daje prikaz postojećih sesija na sistemu, koji forenzičaru može da ukaže na tip logovanja, tip autentifikacije na sistem (NTLM, Kerberos, RADIUS), aktivne procese i druge korisne informacije, dat je na slici 11. Pokreće se komandom logonsessions.exe -p



Slika 11. *Prikaz postojećih sesija na sistemu sa alatom logonsessions.exe*

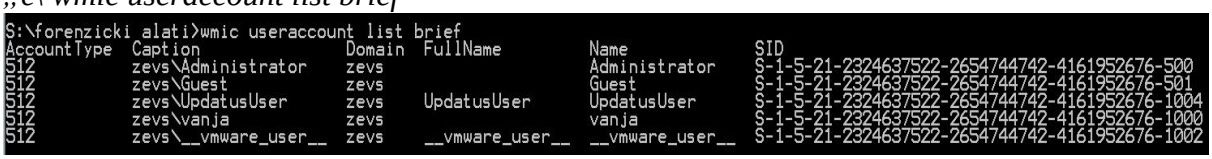
Besplatna alatka netusers (može da se preuzme sa sajta prikazanog u tabeli 9. ovog rada) prikazuje poslednja vremena logovanja korisnika na sistem. Pošto se ti podaci nalaze u registru baze i ova alatka može da se koristi na "živom " sistemu i prepoznaje samo logovanja korisnika preko Windows autentifikacionog mehanizma. Primer upotrebe ove alatke prikazan je na slici 11.



Slika 11. *Prikaz detalja vezanih za poslednje vreme logovanja korisnika sistema*

Alatkom wmi koja je sastavni deo Windows operativnog sistema moguće je dobiti i listu korisničkih naloga na sistemu sa prikazom na slici 12:

„c\ wmic useraccount list brief"



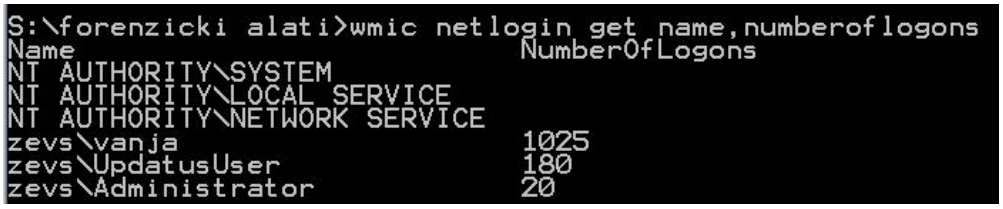
Slika 12. *Prikaz postojećih korisničkih naloga na sistemu*

Listu sa više detalja moguće je dobiti sa komandom :

„C:\wmic useraccount"

Takođe ova alatka može pružiti informaciju o tome koliko se određeni korisnik logovao puta na sistem kao na slici 13. :

„c:\wmic netlogin get name,numberoflogons"



Slika 13. *Prikaz broja logovanja za korisnike na sistemu*

Ukoliko sistem ima veliki broj korisnika moguće je informaciju o broju logovanja dobiti i putem pretrage na osnovu imena sa komandom :

"c:\ wmic netlogin where (name like "%vanja%") get numberoflogons"

Takođe, moguće je u Windows operativnom sistemu dobiti i jako dragocenu informaciju o tome koji se korisnik poslednji logovao na sistem. Ta informacije se nalazi u registru baze :

"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" kada je reč o Windows XP sistemu, odnosno

" HKLM\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI" kada je reč o sistemima Windows Vista, Windows 7 i Windows 8.

Ovi podaci mogu biti korisni forenzičaru, jer mogu da doprinesu kontekstu u daljem toku istrage. Takođe, dobijeni podaci mogu ukazati na činjenicu da se određeni korisnik logovao više puta od uobičajeno prosečnog broja puta, što može biti i vredan bezbednosni parametar.

3.1.3 Podaci od značaja privremenog karaktera na Windows-u - Dump memorijskog procesa i kompletan dump memorije

Prikupljanje podataka iz memorije sistema je važno za forenzičku istragu jer se tu mogu pronaći dragoceni podaci. Podaci koji se mogu izvući su sledeći : ulogovani korisnici, sistemsko vreme, otvoreni fajlovi, informacije o aktivnim procesima, memorija procesa, sadržaj *Clipboard*-a, mapirani procesi i portovi, status mreže, mrežne informacije, mrežne konekcije, mapirani drajvovi, deljeni resursi (fajlovi, direktorijumi), informacije o servisu ili drajveru, istorija komandi.

Da bi forenzičar uspeo da izdvoji deo memorije koje se odnosi na određeni-ispitivani proces Microsoft je omogućio alatku koja se zove Userdump.exe[218]. Treba je koristiti kada forenzičar zna da je napadač pokrenuo maliciozni proces ali tek treba utvrditi o kom procesu je reč. Ova alatka omogućava forenzičaru da prikupi memorijski prostor koju koristi bilo koji izvršni proces. S obzirom da alatka userdump.exe upisuje rezultate direktno na disk, upotreba netcat alata nije izvodljiva. Zbog navedene okolnosti, a da bi forenzički "uticaj" na ispitivani sistem bio što manji, preporuka je da se za ovu namenu mapira jedan mrežni disk i postupak dokumentovati. Razlog leži u činjenici da prikupljena memorija može biti većeg kapaciteta. To se radi sa komandom "net use" :

c:\>net use o: \\192.168.1.5\podaci_prikupljanje

Nakon toga pokreće se Userdump komanda:

c:\>userdump.exe -p koja će izlistati procese, nakon toga pokreće se

[218] Dostupno na http://www.microsoft.com/en-us/download/confirmation.aspx?id=4060, 05.07.2012.

c:\>userdump.exe broj_sumnjivog_procesa o:\dump_procesa.dmp
Treba reći da ID sumnjivog procesa možemo dobiti i iz pomenute alatke "**pslist.exe**"
Sa određenim svič-evima moguće je uraditi i dump više od jednog procesa u okviru jedne komande. Izlaz alatke userdump prikazan je na slici 14. :

```
S:\forenzicki alati\userdump\x64>userdump 4384 testni_dump
User Mode Process Dumper (Version 8.1.2929.5)
Copyright (c) Microsoft Corp. All rights reserved.
Dumping process 4384 (U.S.RoboticsUSBPhone.exe) to
S:\forenzicki alati\userdump\x64\testni_dump...
The process was dumped successfully.
```

Slika 14. *Prikaz uspešno izvršenog dumpovanja procesa komandom userdump.exe*

Da bi se izvršila validacija dumpovanog procesa postoji alatka koja se zove dumpchk.exe dostupna na Debbuging tools for Windows paketa[219]. Treba reći da proces u memoriji umesto u ASCII može biti i u Unicode formatu pa je za pregled dumpa potrebno korstiti alatke koje mogu da rade i sa ASCII i sa Unicode formatima. O jednoj takvoj alatki je već bilo reči i zove se Strings[220]. Kada je reč o Linux-ovom strings, alatu treba napomenuti da on po difoltu ne prikazuje Unicode stringove, već se oni na poseban način omogućavaju.

Jako je važno ispitati sumnjivi proces pre gašenja sistema, jer može biti podešen tako da se nakon izvršenja obriše i da bude samo u memoriji, a opisani način je jedini način da se maliciozni proces otkrije, dokaže njegovo prisustvo i spreči dalja šteta. U suprotnom, odnosno da je računar isključen, ovaj dokaz o malicioznom programu bio bi izgubljen.

Ukoliko forenzičar ima potrebe da prikupi kompletan sadržaj sistemske memorije koji može sadržati delove malicioznog procesa, a ne samo procesa, to se može uraditi sa alatima posebne namene. Forenzičar mora da bude svestan da prilikom postupka prikupljanja memorije na "živom" sistemu sa programskim alatima, može doći do izmene podataka. Razlog je taj što uvođenje novog programa u memoriju može izmeniti podatke iz memorije koji su po karakteru lako izmenjivi (novi podaci zauzeće prostor koji su postojeći zauzimali).
U daljem tekstu biće predstavljeni alati koji su dominantno prisutni u praksi, kada je reč o prikupljanju podataka iz fizičke memorije. Jedan od takvih alata koji služi za kreiranje slike iz memorije je UNIX dd alat koji je kao takav ili uz određene modifikacije sastavni deo mnogih forenzičkih kompleta. DD format je podržan od većine forenzičkih programa. Modifikovana dd verzija čiji je autor George M. Garner iz GMG system inc. [221] koja je u sastavu FAU alata može kreirati dump cele memorije (ali samo kroz korisnički mod). Način upotrebe je opisao Keith Jones[93]:
c:\dd.exe rt if=\\.\physicalmemory of=o:\fullmemorydump.dd bs=4096

Međutim FAU dd radi samo na Windows 2000, Windows XP [31][52], jer je kod ovih sistema dozvoljen pristup fizičkoj memoriji (odnosno objektu \\.\PhysicalMemory) iz korisnčkog moda (eng. user mod). Od Windows XP SP2 je promenjen način adresiranja i pristup objektu \\.\PhysicalMemory nije više moguć kroz korisnički mod, već samo kroz drajvere kernel moda (eng. kernel-mode driver). S obzirom da se podaci tokom prikupljanja menjaju u RAM-u, preporuka je da se heširanje uradi tek nakon što se podaci prikupe na forenzički disk, a ne u toku prikupljanja [31].

Druga alatka čiji je autor Matt Shannon iz Agile Risk Management-a koja je slična DD-u zove se Nigilant32. Ova alatka omogućava forenzičaru da prikaže hard disk, da prikupi podatke iz RAM memorije i da uradi snimak stanja (eng. snapshot) trenutno pokrenutih procesa i otvorenih portova. Koristi grafički interfejs, jako malo prostora zauzima na sitemu (1mb kada je učitan u memoriju) i ima mali uticaj na ispitivani sistem. Može se pokretati sa USB-a ili CD-a. Podržava Windows 2000, XP, and 2003.

[219] Dostupno na http://msdn.microsoft.com/en-us/Windows/hardware/gg463009.aspx, 05.07.2012.
[220] Dostupno na http://technet.microsoft.com/en-us/sysinternals/bb897439.aspx, 05.07.2012.
[221] Dostupno na http://www.gmgsystemsinc.com/fau/ , pristupljeno 13.04.2013

Treća alatka jeste deo ProDiscover Incident Response[222] seta alata kompanije Technology Pathway koji dozvoljava forenzičaru da prikupi sadržaj fizičke memorije sa "živog" sistema. Uz pomoć ovog seta alata moguće je utvrditi, da li je sistem kompromitovan i omogućava prikupljanje potrebnih dokaza da se to i dokaže. Istraživanje može obuhvatati kreiranje slike fizičkog diska ili memorije. Zahteva se instaliranje serverskog apleta (PDServer program) na ispitivanom računaru da bi se realizovao postupak prikupljanja podataka, što ga čini prihvatljivim više korporativnom okruženju nego za pravosuđe.

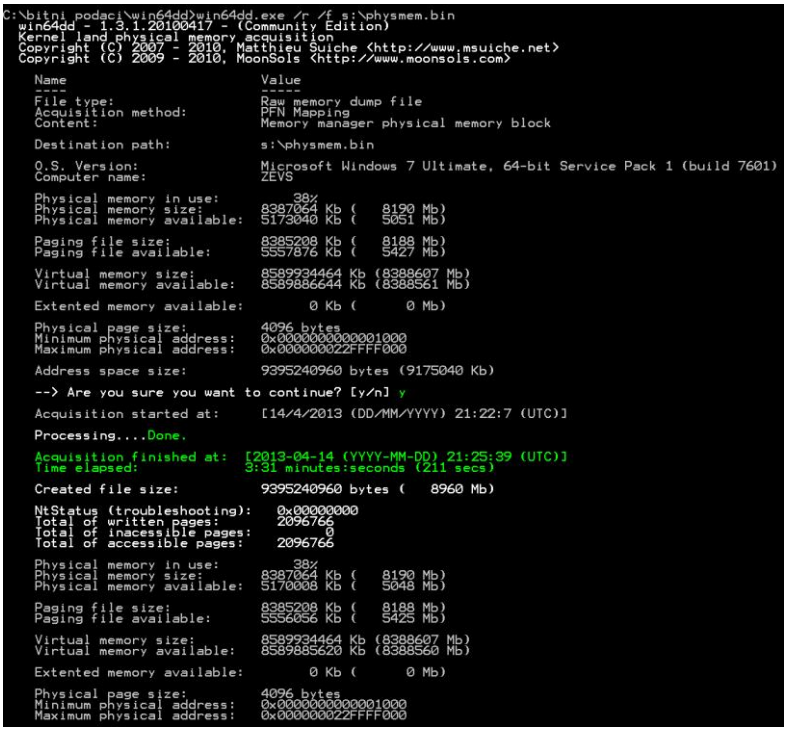
Četvrta alatka KnTDD koja je deo KntTools[223] forenzičkog seta alata čiji je autor George Garner, rešava problem pristupa objektu \\.\PhysicalMemory preko drajvera kernel-moda. Podržava gotovo sve Windows operativne sisteme od Windows 2000 do Windows 8 RTM uključujući i 64-bitne verzije pomenutih sistema. Uz pomoć ove alatke moguće je konvertovati sliku memorije iz "raw" formata u Microsoft crash dump format i analizirati dobijene rezultate uz pomoć Microsoft debugging tools-a. Kreiranje slike memorije može da se prikuplja na eksternom uređaju ili putem mreže. Forenzičar prilikom prikupljanja mora bit svestan Lokardovog principa razmene i shodno tome mora voditi računa da sve što radi na "živom" sistemu detaljno dokumentuje. Ovaj set alata namenjen je pre svega vojsci, pravosuđu, vladinim agencijama i visokoškolskim ustanovama. Za korporacijske potrebe moguće ga je koristiti u zavisnosti od slučaja.

MDD[224] - ova alatka kreirana od strane kompanije ManTech International Corporation služi za prikupljanje slike memorije sa ispitivanog računara iz komandnog okruženje Windows operativnog sistema. Može prikupljati slike memorije sa Windows 2000, XP, Vista and Windows Server 2003 SP1 ali je ograničena sa prikupljanjem do 4GB RAM podataka.

Win32DD i **Wind64dd**[225] - ova alatka čiji je autor Matthieu Suiche služi za prikupljanje sadržaja fizičke memorije. Od dodatnih pogodnosti ima opciju da kreira crash dump (sličan Windows crash dump fajlu) kompatibilan sa Windows debugger alatima. Postoji u 32-bitnoj i 64-verziji [125]. Od operativnih sistema podržava Microsoft Windows XP, 2003, 2008, Vista, 2008 R2, 7.

Jedan primer prikupljanja fizičke memorije sa računarskog sistema Windows 7 x64 prikazan je na slici 15. :

[222] Dostupno na http://www.techpathways.com/prodiscoverir.htm , pristupljeno 14.04.2013
[223] Dostupno na http://www.gmgsystemsinc.com/knttools/ , pristupljeno 14.04.2013
[224] Dostupno http://sourceforge.net/projects/mdd/files/latest/download?source=files , pristupljeno 14.04.2013
[225] Dostupno http://www.moonsols.com/Windows-memory-toolkit/, pristupljeno 14.04.2013



Slika 15. Prikupljanje sadržaja fizičke memorije alatom win64dd.exe

Winen[226] - ova samostalna alatka kompanije Guidance Software koja dolazi u sklopu forenzičkog kompleta Encase (od verzije 6.11) i u sklopu kompleta Helix (od verzije 2.0) služi za prikupljanje sadržaja fizičke memorije. Pokreće se iz komandnog okruženja. Može se pokrenuti sa prenosnog drajva (na primer USB drajv) koji se priključi na računar koji se ispituje. Ima jako mali otisak u memoriji sa minimalnim uticajem na sistem. Prikupljen sadržaj ram memorije smešta se u fajl .E0XX. Postoji u 32-bitnoj i 64-bitnoj varijanti. Podržava sve Windows operativne sistem počev od Windows 2000.

FastDump[227] - alatka kompanije HBGary služi za prikupljanje sadržaja fizičke memorije. Ima jako mali otisak sa minimalnim uticajem na memoriju. Sav kod je statički linkovan tako da nema učitavanja DLL-ova. Veličina mu je samo 80k. Postoje dve verzije ove alatka javna (eng. Fastdump community) koja je besplatna i Pro verzija. Fastdump community podržava samo 32-bitne operativne sisteme sa prikupljanjem podataka iz RAM memorije do 4GB. Ne podržava Windows Vistu, Windows 2003 i Windows 2008. Pro verzija podržava sve Windows OS kako 32-bitne tako i 64-bitne sa mogućnošću prikupljanja podataka iz RAM više od 4GB.

Analiza fajla crash dump predstavlja takođe jedan od načina dobijanja informacija o sadržaju memorije. Za razliku od prikupljanja podataka iz memorije pomenutim specijalnim alatkama, slika memorije dobijena u formi crash dump fajla predstavlja neizmenjenu kopiju [52][32] sistemske memorije u momentu kada se desio krah sistema. Nedostatak ovog načina jeste taj, što se za dobijanje crash dump fajla mora desiti krahiranje sistema, jer nisu svi sistemi podešeni da generišu ovaj fajl. Druga mana je ta što upisivanje ovog fajla može prepisati druge dokaze (obrisani ali ne i nestali podaci). Postoji način na koji on može da se izazove ali on zahteva izmenu, odnosno kreiranje registarskog ključa i restartovanje računara opisanog na Microsoft sajtu[228][229]. Postoje 3 tipa crash dump fajla : kompletan, kernel, mali. Kod Windows XP i Windows Viste po difoltu se kreira "mali" crash dump fajl, dok se kod Windows 2003 servera kreira kompletan crash dump. Treba spomenuti da sistemi sa preko 2

[226] Dostupno http://www.guidancesoftware.com/ , pristupljeno 14.04.2013
[227] Dostupno http://www.hbgary.com/free-tools#fastdump, pristupljeno 14.04.2013
[228] http://support.microsoft.com/kb/927069, 14.04.2013
[229] http://support.microsoft.com/kb/244139, 14.04.2013

GB RAM memorije ne podržavaju kompletan crash dump fajl [32]. Iako je crash dump fajl forenzički ispravan fajl, pomenute mane prilikom njegovog "izazvanog" dobijanja (što nije u forenzičkom maniru) čine ga beskorisnim u istragama pravosudnih oragana. Kada su u pitanju istrage u korporacijama (nezvanične istrage), uz adekvatno konfigurisanje računarskih sistema, pomenuto "izazvano" dobijanje crash dump fajla može biti od velike koristi da se pronađu informacije o kompromitovanju sistema. To za posledicu ima pravovremeno otkrivanje malicioznih aktivnosti ili sprečavanje štete većeg obima u okviru korporacije, što utiče na povećanje bezbednosti.

Analiza hibernacijskog fajla predstavlja takođe jedan od načina dobijanja informacija o sadržaju memorije. Kada sistem odlazi u hibernacijski režim on sadržaj RAM memorije smešta u kompresovan fajl na hard disku pod nazivom hiberfil.sys pod root direktorijumom. Kada se sistem podiže on proverava da li postoji hibernacijski fajl i ukoliko postoji njegov sadržaj učitava u memoriju. S obzirom da su takvi fajlovi uglavnom starijeg datuma, oni se mogu postaviti u kontekst aktivnosti koje su se dešavale u prošlosti. Matthieu Suiche je dekodovao hibernacijski fajl format i prezentovao javnosti (Windows hibernation file for fun "N" profit[230]) svoje otkriće na konferenciji BlackHat USA 2008 godine. Postoje alati (powercfg.exe[231] i psshutdown.exe[232]) kojima se može naterati sistem da ode u hibernaciju i time da se prikupi dump memorije. Isto pravilo važi kao i kod dobijanja crash dump fajla : kada su u pitanju istrage u korporacijama (ne zvanične istrage), uz adekvatno konfigurisanje računarskih sistema pomenuto "izazvano" dobijanje crash dump fajla može biti od velike koristi da se pronađu informacije o kompromitovanju sistema, ali sticanje na takav način nije od koristi za istrage pravosudnih organa.

U zavisnosti od upotrebljenog alata nakon dobijene slike ili dumpa memorije sledi memorijska analiza (što ne spada u kontekst ovog rada). Postoje alati i kompleti alata sa kojima se radi memorijska analiza (na primer find.exe strings.exe, grep ili hex editori) koja pretražuje sadržaj slike ili dump-a memorije u kome se mogu naći dragoceni dokazi. Neki od njih prikazani su u poglavlju 3.1.3 u tabeli 5. Detaljnu analizu dump alata, za prikupljanje podataka iz memorije, prikazali su Takahiro Haruyama i Hiroshi Suzuki na BlackHat Europe konferenciji u radu „One-byte Modification for Breaking Memory Forensic Analysis“ [80]. Međutim, pronađene informacije putem pretraživanja samo na osnovu stringova ponekad je teško uklopiti u kontekst, jer ne postoji način da se pruži uvid u to koji je proces koristio određene informacije. Najnovije tehnike koje se primenjuju u analizi raščlanjuju sliku ili dump memorije i identifikuju blokove procesnog okruženja (eng. Process Environment Block) ili PEB [32][31]. Na osnovu onih informacija koje se nalaze u PEB-u moguće je saznati kome pripada određeni procesni deo memorije[233]. U praksi to znači da ukoliko se na ispitivanom računaru nalazi nezakonit materijal, forenzičar će biti u stanju da otkrije da li je taj materijal preuzet sa znanjem korisnika ili je automatski preuzet od strane malicioznog programa. Sa bezbednosne tačke gledišta prednost ovakvog pristupa povećava šansu pronalaženja malicioznih programa, jer PEB informacije istraživaču mogu pomoći pri diferencijaciji normalnog i malicioznog procesa.

Na primer, moguće je naći određene sekcije log fajlova Web servera koji su ukazivali da je upotrebljen bio exploit sa određene IP adrese, a s obzirom da je log fajl obrisan ovo je dragocen dokaz u istrazi. Takođe, ova informacija bi ukazivala i na ranjivost pomenutog Web servera što bi podrazumevalo primenu bezbednosnih zakrpa na pomenutom sistemu. Treba napomenuti da se koriste uvek ažurirani alati, zbog činjenice da se sa novim verzijama Windowsa ili novim servis packovima može promeniti struktura procesa u memoriji. U tabeli 5. navedeni su alati sa kojima je moguće vršiti analizu prikupljene memorijske slike ili dump-a.

[230] Dosupno http://ebookbrowse.com/bh-us-08-suiche-Windows-hibernation-file-for-fun-n-profit-0-3-pdf-d209085775, 14.04.2013

[231] http://technet.microsoft.com/en-us/library/cc748940%28v=ws.10%29.aspx, 14.04.2013

[232] Dostupno http://technet.microsoft.com/en-us/sysinternals/bb897541.aspx, 14.04.2013

[233] PEB nam takođe pokazuje gde se nalazi slika izvršnog fajla, DLL putanje i komanda koje je startovala proces.

Tabela 5 : Alati za analizu memorijske slike ili dump-a

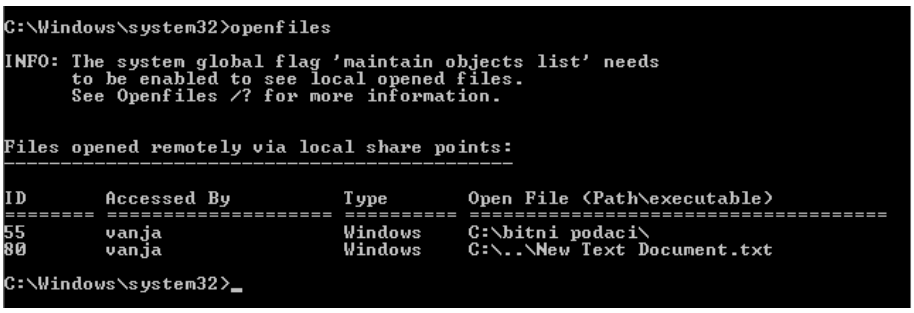
ALAT	OPERATIVNI SISTEM	NAMENA	Zahtev	Dostupnost
Memoryze	Svi x86 i x64	Omogućava raščlanjivanje i analizu memorijskog dump fajla. Podržava Raw image format.	Python	https://www.mandiant.com/resources/download/memoryze
HBGary responder	Svi x86 i x64	Omogućava sveobuhvatnu analizu memorije. U stanju je da obnovi sve osnovne strukture podataka iz prikupljene memorije. Podržava Raw image format. Može se naći u 3 verzije Pro, Field i Community.		http://www.hbgary.com/hbgary-releases-responder-ce
Lsproc.pl	Windows 2000	Izlistava procese	Perl	http://sourceforge.net/projects/Windowsir/files/Windows2000%20Memory/lsproc/ [30]
Lspd.pl	Windows 2000	Izlistava detalje o procesima	Perl	http://sourceforge.net/projects/Windowsir/files/Windows2000%20Memory/lspd%200.8/
Osid.pl	Svi x86 i x64	Identifikuje verziju operativnog sistema iz dumpa ili slike memorije	Perl	Dolazi uz knjigu Harlana Carvey-a [31]
PoolFinder	Windows 2000, Windows XP	Pronalazi dodeljen prostor kernelu OS u dump-u memorije i pagefile-u.	Perl	Sastavni je deo paketa Pool Tools : http://computer.forensikblog.de/files/poolfinder/poolfinder-current.zip
PoolGrep	Windows 2000, Windows XP	Pronalazi stringove u dodeljenom pool-u	Perl	Sastavni je deo paketa Pool Tools : http://computer.forensikblog.de/files/poolfinder/poolfinder-current.zip
PoolDump	Windows 2000, Windows XP	Kreira hex dump od svog alociranog prostora za određenu klasu.	Perl	Sastavni je deo paketa Pool Tools : http://computer.forensikblog.de/files/poolfinder/poolfinder-current.zip
PoolView	Windows 2000, Windows XP	Prevodi određene alocirane poolove u razumljiv format	Perl	Dostupan je za pravosudne organe i specijalnim interesnim grupama na zahtev http://computer.forensikblog.de/en/2007/11/pooltools-version-130.html

PTFinder	Windows 2000, Windows XP	Uključuje sve skripte iz paketa PoolTools kao i osid.pl skriptu i ima grafički interfejs.	Perl sa dodacima [234]	http://computer.forensikblog.de/files/ptfinder/ptfinder-current.zip
Volatility Framework	Windows XP, 2003, Vista, 7, 2008 samo u x32	Predstavlja sveobuhvatan komplet alata sa različim funkcijama analize memorije. Može rasčlanjivati crash dump fajlove. Od formata podržava raw, crash dump i hibernacijski. Takođe, može vršiti konverziju raw formata (dd tip) u crash memory dump format tako da se za analizu mogu koristiti i Microsoft debugger alati. Može vršiti izvlačenje informacija o ugašenim procesima i prekinutim konekcijama.	Python	https://www.volatilesystems.com/default/volatility

3.1.4 Podaci od značaja privremenog karaktera na Windows-u - Otvoreni fajlovi na sistemu

Neke od prethodnih alatki, kao na primer psloggedon.exe mogu ukazati digitalnom forenzičaru ko je kao udaljeni korisnik ulogovan i koje deljene resurse na mreži on koristi. Značajna informacija koju je potrebno dobiti je koji su to fajlovi koje koristi udaljeni korisnik. Alati koji mogu pružiti ove detalje su komanda net file, alatka openfiles.exe i psfile.exe

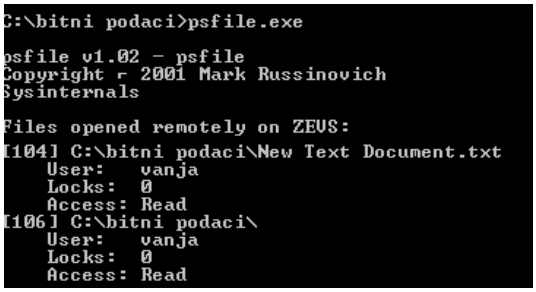
Alatka openfiles (sastavni deo Windows operativnog sistema od verzije XP-pro) prikazuje otvorene fajlove na sistemu i korisnika koji im je pristupio. Primer upotrebe ove alatke dat je na slici 16.



Slika 16. *Prikaz otvorenih fajlova na sistemu od strane korisnika komandom openfiles*

Alatka psfile (može da se preuzme sa sajta prikazanog u tabeli 9. u poglavlju 3.3.1) prikazuje otvorene fajlove na sistemu i ime udaljenog korisnika koji im je pristupio. Primer upotrebe ove alatka dat je na slici 17.

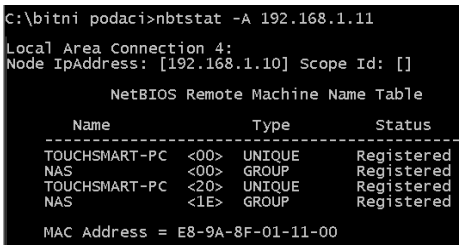
[234] Graphviz i ZGRViewer koji služe za pregledanje grafičkog fajla



Slika 17. *Prikaz otvorenih fajlova od strane korisnika alatkom psfile.exe*

3.1.5 Podaci od značaja privremenog karaktera na Windows-u - Informacije o mreži

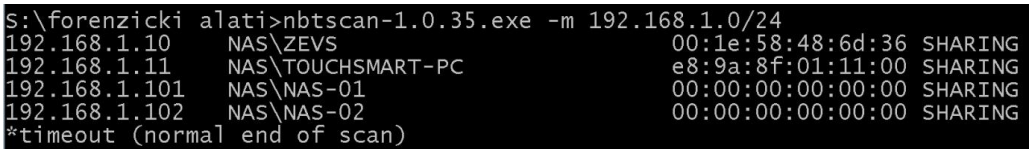
Ukoliko je reč o kompromitovanju računarskog sistema (na primer, upad u sistem), ono što treba ispitati je, da li je sa tog sistema pokušano ili je uspeo upad na neki drugi računarski sistem. Kod Windows operativnih sistema[235], pri pravljenju konekcije prema drugom Windows operativnom sistemu ostaje zapis u kešu Netbios tabeli imena (eng. cached NetBIOS Name Table). Digitalnom forenzičaru ovo može biti od velike koristi pri lociranju kompromitovanih računarskih sistema. Alatka je implementirana u Windows operativni sistem i zove se nbtstat.exe. Ukoliko se želi videti keš Netbios tabele na računarskom sistemu upotrebljava se komanda "c:\nbtstat.exe -c", odnosno ukoliko se želi videti Netbios tabela udaljenog računara sa korisnim informacijama o servisima na ispitivanom računaru, koristi se komanda "c:\nbtstat -A ipadresa_udaljenog_racunara". Primer upotrebe ove komande dat je na slici 18.



Slika 18. *Prikaz NetBios tabele udaljenog računara*

Nedostaci prethodnog alata kao što su rad sa jednom IP adresom, funkcionisanje samo na Windows platformi kao i ne tako čitak format izlaza komande, prevazilazi sjajna besplatna alatka nbtscan.exe. Ona digitalnom forenzičaru može da omogući skeniranje IP adresa iz zadatog mrežnog opsega šaljući NetBios upite, a kao izlaz komande dobija se lista sa ip adresama, Netbios imenima računara, imenima ulogovanih korisnika kao i MAC adresa. Osim na Windows platformi može da se koristi i na Linux platformi. Kao benefit digitalni istražitelj brzo i lako može da uoči sumnjiva NetBios imena na mreži što može da olakša i ubrza forenzičko ispitivanje. Takođe, ukoliko se blagovremeno uoči takva mašina može se sprečiti i potencijalna šteta koju zlanamerni korisnik može naneti, pa se na taj način i povećava zaštita računara na mreži kao i samog informacionog sistema. Prikaz izlaza nbtscan.exe dat je na slici 19.

[235] Netbios servis je prisutan gotovo kod svih Windows operativnih sistem čak je u Windows serveru 2008 u defaultnim postavkama omogućen kao servis.

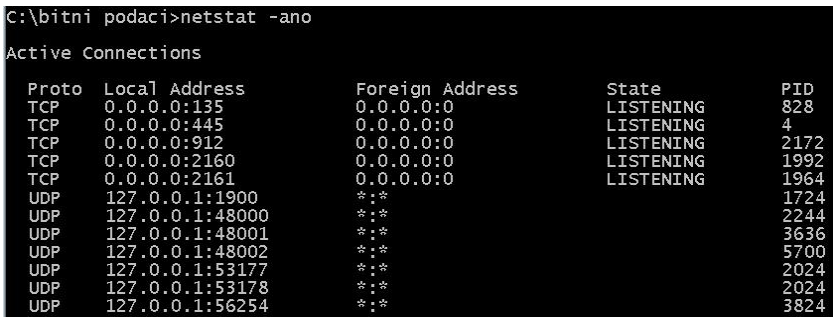


Slika 19. *Izlaz alatke nbtscan u razumljivom formatu sa IP adresama i Netbios imenima*

3.1.6 Podaci od značaja privremenog karaktera na Windows-u - Mrežni status i konekcije

Izuzetno je značajno da digitalni forenzičar, što pre, po prijavi incidentne/protivpravne aktivnosti pravovremeno reaguje da bi sakupio što više informacija iz lako izmenjivih (engl. volatile data) podataka. Neki od njih se upravo odnose na informacije koje računar sadrži o dolaznom i odlaznom mrežnom saobraćaju. To može pomoći forenzičaru da utvrdi da li je maliciozni korisnik (napadač) još uvek prijavljen na sistem. Takođe, moguće je utvrditi i postojanje malicioznog programa (na primer Crva eng. Worms ili Bot-a) koji pokušava da zarazi druge računarske sisteme na mreži. U praksi detektovanje konekcije koju pravi zlonamerni korisnik, odnosno malicioni program[236] nije jednostavan postupak ukoliko na samom sistemu ne postoji neki zaštitni zid (eng. Firewall) koji prati odlazni i dolazni saobraćaj, koji prati i snima u log fajlove kompletan mrežni saobraćaj. Jedan takav besplatan program koji se na sistemu startuje kao servis koji prati TCP i UDP pakete, zove se Port Reporter[237]. Za jednostavniji preled log fajlova koji je Port reporter generisao postoji besplatan program Port Reporter parsing tool[238]. U nastavku rada biće prikazani neki od alata koji digitalnom forenzičaru mogu biti od velike pomoći u prikupljanju informacija o mrežnim konekcijama.

Alatka Netstat koja je deo Windows operativnog sistema jedna je od najpoznatijih alata koja služi za brzo i jednostavno prikupljanje informacija o TCP i UDP konekcijama, njihovim stanjima i statistici mrežnog protoka paketa (IPv4, IPv6, TCP, UDP, ICMPv4, ICMPv6). Najčešće se upotrebljava da se izlistaju sve aktivne konekcije i otvoreni portovi na računaru. S obzirom da se portovi uobičajeno koriste za kreiranje zadnjih vrata na sistemima, forenzičar prepoznajući otvorene portove može otkriti zlonamerne konekcije i blagovremeno zatvoriti te portove. Ova komanda istu namenu ima i na Linux računarskim sistemima. Prikaz izlaza komande netstat sa kojom se dobija prikaz aktivnih konekcija dat je na slici 20.



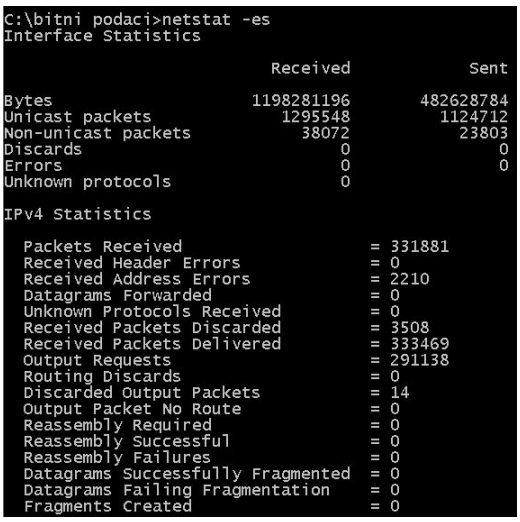
Slika 20. *Prikaz aktivnih konekcija alatkom netstat*

[236] Što u praksi traži odgovor na pitanje da li su podaci kompromitovani ili ne.

[237] Dostupno na http://www.microsoft.com/downloads/details.aspx?familyid=69ba779b-bae9-4243-b9d6-63e62b4bcd2e&displaylang=en , 12.10.2013.

[238] Dostupno na http://support.microsoft.com/kb/884289, 12.10.2013.

Prikaz izlaza komande netstat sa kojom se dobija prikaz statistike mrežnih paketa dat je na slici 21.

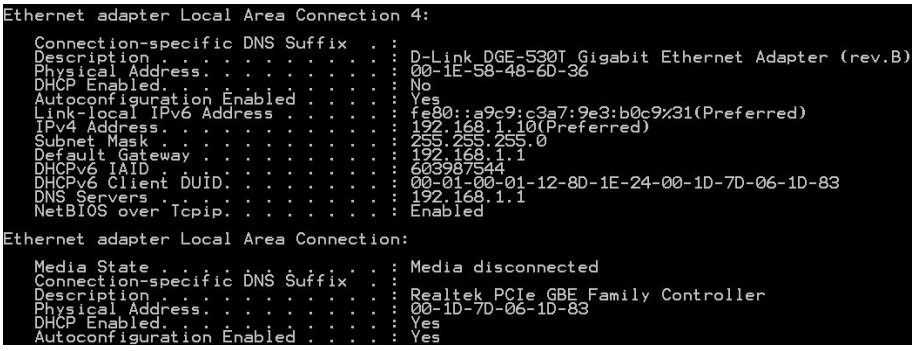


Slika 21. *Prikaz statistike mrežnih paketa*

Prilikom forenzičkog istraživanja, takođe treba obratiti pažnju na neuobičajene otvorene portove. Praksa je pokazala da treba detaljno razmotriti i saobraćaj koji ide preko standardnih portova koji može forenzičara da dovede u zabludu. Jedan od primera bi bio da zlonamerni korisnik preko porta 80 wget.exe aplikacijom download-uje zlonamerne programe i alate za kompromitovanje sistema što će forenzičaru ili sistemu za prepoznavanje upada (eng. IDS) izgledati kao legitiman saobraćaj u mreži [31].

Od izuzetne važnosti za istragu može biti dobijanje informacija o statusu mrežnog adaptera (eng. network interface card - NIC) (LAN ili WLAN[239]) ispitivanog računarskog sistema. Na primer, danas se većina prenosnih računarskih sistema (eng. lap-top) isporučuje sa već ugrađenim bežičnim mrežnim adapterom. To znači da forenzičar na prvi pogled (uvidom u Desktop sistema), ne može da utvrdi da li je ispitivani sistem uspostavio konekciju sa nekom pristupnom tačkom (eng. Access Point - AP) i koju je adresu dobio. Nekada je ta informacija o statusu mrežnog adaptera od velikog značaja za dalji tok istrage. U nastavku će biti izloženi određeni alati sa kojima će biti moguće utvrditri status mrežnog adaptera.

Alatka ipconfig je sastavni deo Windows operativnog sistema, pomoću nje dobijaju se konfiguracione informacije postojećih mrežnih adaptera na sistemu kao i njhiv status. Alatka ima veliki broj korisnih svičeva, ali najsveobuhvatniji je upravo "/all" svič (c:\ipconfig /all) i njen izlaz dat je na slici 22.



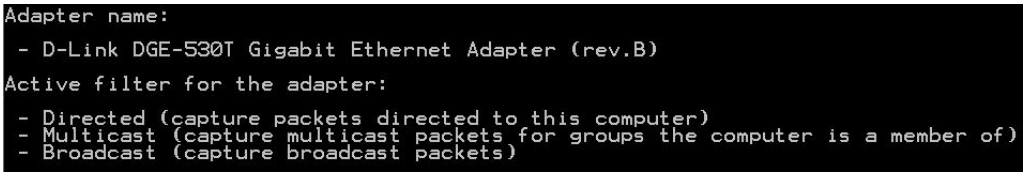
Slika 22. *Prikaz izlaza komande c:\ipconfig /all iz Windows 7 operativnog sistema*

[239] Bežični LAN adapter.

Kao što se može primetiti informacije koje možemo dobiti ovom alatkom su status mrežnog adaptera, njegovo ime, status DHCP-a, IP adresa, fizička adresa, NetBIOS status i drugi parametri. Ovi parametri su izuzetno važni u toku istrage, naročito kada se vrše ispitivanja logova mrežnog saobraćaja.

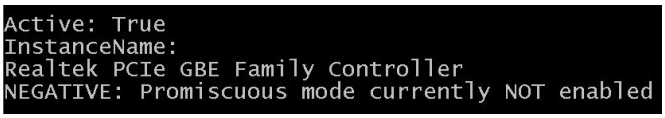
Kada je reč o statusu mrežnog adaptera važno je utvrditi u kom modu je postavljen mrežni adapter da radi. Na kompromitovanom računaru postoji mogućnost da je mrežni adapter postavljen u monitor mod (eng. promiscuous mode) tj. režim kartice sa kojim je moguće "osluškivati" mrežni saobraćaj nasuprot normalnom režimu rada.

S obzirom da administrator sistema i mreže ili digitalni forenzičar ne mogu na jednostavan način utvrditi u kom režimu je podešena kartica da radi, ukoliko ne postoje neki od očiglednih pokazatelja kao na primer postojanje određenih programa koji mogu raditi u režimu prisluškivanja (Ethereal koji se sada zove Whireshark[240] ili Windump[241] kao i mnogi drugi komercijalni programi). Jedini način da se otkrije na živom sistemu je korišćenjem određenih alata ili skripti. Jedan od takvih alata je promiscdetect.exe[242], ndis.exe[243] i promqry.exe[244] čiji su izlazi prikazani na slikama 23., 24. i 25. :



Slika 23. *Prikaz izlaza alatke promiscdetect.exe na Windows 7 OS-u*

Slika 24. *Prikaz izlaza alatke ndis.exe na Windows 7 OS-u*



Slika 25. *Prikaz izlaza alatke promqry.exe na Windows 7 OS-u*

Takođe, detektovanje može da se izvši uz pomoć alatke nmap (pokrenuta sa spoljne Linux mašine) uz pomoć predefinisane skripte koja se zove sniffer-detect.nse odnosno promiscuous.nse u zavisnosti od verzije Nmap-a[245]. Pokreće se sa komandom za zadatu mrežu na primer # nmap --script=promiscuous 192.168.1.0/24

Ukoliko sistem detektuje neku karticu na mreži koja je u režimu "osluškivanja", izlaz komande će biti prikazan na sledeći način :

Interesting ports on Sumnjiv_racunar (192.168.1.123):
Not shown: 996 closed ports

PORT	STATE	SERVICE
22/tcp	open	ssh
23/tcp	open	telnet
53/tcp	open	dns
80/tcp	open	IIS/http

[240] Dostupno na http://www.wireshark.org/, 05.02.2013

[241] Dostupno na http://www.winpcap.org/windump/, 05.02.2013

[242] Dostupno na http://ntsecurity.nu/downloads/promiscdetect.exe , 05.02.2013

[243] Dostupno na disku koji se dobija uz knjigu Windows Forensic Analisys od Harlana Carvey-a [78]. Ovoj alatki je potrebna biblioteka p2x588.dll.

[244] Alatku je napisao Tim Rains ima mogućnost testiranja nad udaljenim računarskim sistemom. Dostupna je na Microsoft sajtu http://www.microsoft.com/en-us/download/details.aspx?id=185, 01.03.2012.

[245] Dostupno na http://nmap.org/nsedoc/scripts/sniffer-detect.html

MAC Address: 00:26:39:41:15:82 (Linksys)
Host script results:
Promiscuous detection: PROMISCUOUS (tests: "111___1_")

Ovo je signal digitalnom forenzičaru da računar ima mrežni adapter koji je u režimu "osluškivanja" i da je u pitanju jedan od Windows operativnih sistema (počev od Windows 2000). Windows 98 se manifestuje sa oznakom "1111__1_" dok se Linux OS manifestuje sa oznakom "11111111". Važno je napomenuti da skripta daje prikaz samo ukoliko pronađe jedan od mrežnih adaptera u modu za "osluškivanje", a ukoliko ne pronađe, ne prikazuje se izveštaj. Treba reći da je blagovremenom detekcijom takvih računara na mreži moguće sprečiti nanošenje dalje štete (ukoliko je ova već nastala), čime se povećava sigurnost ukoliko se način detektovanja automatizuje. Naravno oslanjanje samo na detektovanje nije pouzdana mera bezbednosti i ne treba biti jedina jer u određenim slučajevima samo detektovanje može doći prekasno da bi se moglo sprečiti kompromitovanje određenih podataka.

Takođe, potrebno je tokom forenzičke istrage da se posebna pažnja obrati i na aktivne mrežne adaptere ispitivanog računara. To može dati dodatan kontest u daljem toku istrage i značajan podatak za post-mortem forenzičku analizu.

3.1.7 Podaci od značaja privremenog karaktera na Windows-u - Interna tabela rutiranja

U praksi jedna od malicioznih upotreba kompromitovanog servera podrazumeva nameru napadača da izmenom ove tabele preusmeri saobraćaj na određeni način. Očekivana korist od preusmeravanja saobraćaja jeste zaobilaženje zaštitnih barijera (eng. firewall). Na primer ukoliko postoji zaštita prema računaru koji je sledeća meta napada, napadač može uz pomoć kompromitovanog računara (koji ima direktan pristup meti) zaobići zaštitne barijere. Druga korist koju napadač može da ima od izmena ruting tablela, jeste prisluškivanje paketa na mreži. Da bi administrator ili forenzičar ustanovili da li je ruting tabela menjana, odnosno da li ima tragova pokušaja napada, to se radi sa netstat komandom kao na slici 26. :

#netstat -nr

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.1    192.168.1.10     266
        127.0.0.0        255.0.0.0         On-link        127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link        127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link        127.0.0.1     306
      192.168.1.0    255.255.255.0         On-link     192.168.1.10     266
     192.168.1.10  255.255.255.255         On-link     192.168.1.10     266
    192.168.1.255  255.255.255.255         On-link     192.168.1.10     266
     192.168.61.0    255.255.255.0         On-link     192.168.61.1     276
     192.168.61.1  255.255.255.255         On-link     192.168.61.1     276
   192.168.61.255  255.255.255.255         On-link     192.168.61.1     276
    192.168.187.0    255.255.255.0         On-link    192.168.187.1     276
    192.168.187.1  255.255.255.255         On-link    192.168.187.1     276
  192.168.187.255  255.255.255.255         On-link    192.168.187.1     276
        224.0.0.0        240.0.0.0         On-link        127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link     192.168.1.10     266
        224.0.0.0        240.0.0.0         On-link    192.168.187.1     276
        224.0.0.0        240.0.0.0         On-link     192.168.61.1     276
  255.255.255.255  255.255.255.255         On-link        127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link     192.168.1.10     266
  255.255.255.255  255.255.255.255         On-link    192.168.187.1     276
  255.255.255.255  255.255.255.255         On-link     192.168.61.1     276
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.1.1  Default
===========================================================================
```

Slika 26. *Prikaz interne tabele rutiranja komandom netstat -nr*

3.1.8 Podaci od značaja privremenog karaktera na Windows-u - Startovani procesi i servisi

Za forenzičko istraživanje ispitivanog sistema izuzetno je važno znati koji su procesi startovani na tom sistemu. Treba istaći da Task menadžer (eng. Task Manager) ne pokazuje sve procese kao i procesne detalje koji su od značaja za ispitivanje. Digitalni forenzičar će želeti da zna na primer, apsolutnu putanju izvršnog fajla, iz kog komandnog okruženja je pokrenut proces koji je potrebno ispitati, vreme trajanja procesa, vlasništvo pokrenutog procesa, koji su moduli učitani od strane procesa, sadržaj koji je proces učitao u memoriju. Neke od navedenih procesa Task menadžer može prikazati, a neke ne. U praksi se dešava sledeći scenario, maliciozni program se instalira pod imenom svchost.exe, a to ime je ime regularnog programa na Windows operativnom sistemu koji se nalazi u *„c:\Windows\system32\"* direktorijumu zaštićen sa WFP (eng. Windows File Protection)[246]. Pregledom u Task menadžeru forenzičaru neće biti jednostavno utvrditi koji je od procesa sumnjiv ukoliko nema putanju do izvršnog fajla. Ukoliko forenzičar otkrije putanju i vidi da se svchost.exe pokreće iz nekog drugog foldera umesto iz c:\Windows\system32\, to je signal da taj proces treba biti predmet ispitivanja. Takođe u praksi se dešavalo da se ime procesa zamaskira imenom da izgleda kao da se radi o sistemskom procesu, na primer iskusnom forenzičaru ili administratoru će biti sumnjiv proces netsysw.exe s pokrenutim svičevima -L -d -p 80 -e cmd.exe jer ukazuje da se radi o startovanom netcat programu ili nekom malicioznom programu tipa zadnja vrata (eng. backdoor). Može se reći da od iskustva i veština samih forenzičara i administratora i dobrih alata u pronalaženju malicioznih procesa može zavisiti, kako sama bezbednost Sistema, tako i uspešnost u digitalnoj forenzičkoj istrazi ispitivanog računara.

U daljem tekstu biće opisani alati koji će forenzičaru pomoći u dobijanju više detalja o ispitivanim procesima i servisima.

Alatka koja je sastavni deo Windows operativnih sistema i omogućuje prikaz postojećih servisa na sistemu sa njegovim stanjem, statusom, modom i oznakom procesa je prikazana na slici 27. :

"c:\ >wmic service list brief"

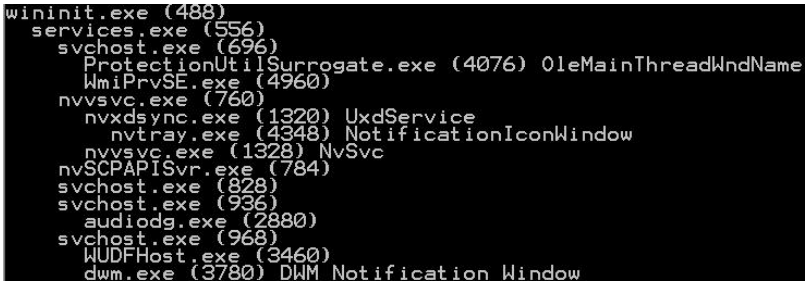
Slika 27. *Prikaz alata wmi koji sa dodatnim argumentima daje detaljnu listu o procesima*

Jako dobra alatka za pregledanje procesa na sistemu jeste Tlist. Ona je sastavni deo Microsoftovog alata za debagovanje[247]. Postoji u 32-bitnoj i 64-bitnoj verziji, ali se ne može naći u novijim verzijama Windowsa (nije sastavni deo od verzije Windowsa XP), jer ga je zamenila alatka TASKLIST. Daje jako dobre detalje kada su u pitanju : ID procesa, ime procesa, identifikator sesije, korišćenje memorije i dll-ova za svaki pokrenut proces, može da

[246] WFP je prisutan od Windows 2000 i štiti sistemske fajlove od izmena i slučajnih brisanja čuvajući svoju "dobru" kopiju u kešu za slučaj da je došlo do namerne ili slučane izmene ili brisanja. Ukoliko se desi generiše se ID 64001 ostavljajući trag na sistemu. Dostupno na http://support.microsoft.com/kb/222193, 03.03.2012

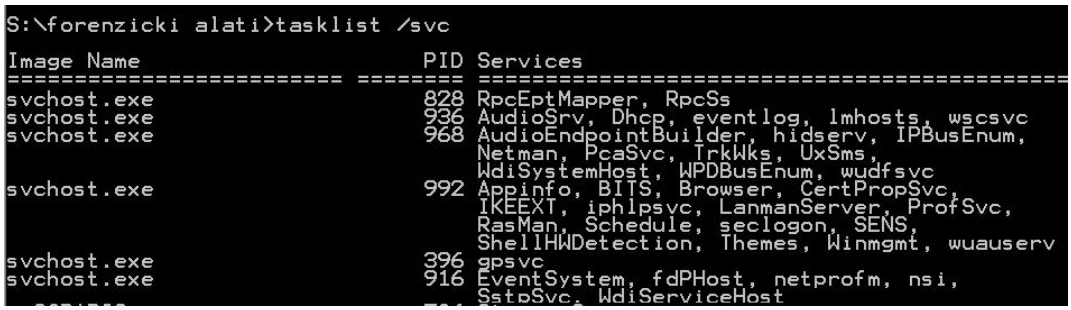
[247] Dostupno na http://download.microsoft.com/download/4/A/2/4A25C7D5-EFBE-4182-B6A9-AE6850409A78/GRMWDK_EN_7600_1.ISO

prikaže punu putanju procesa i hijerarhijski prikaz procesa (slika 28.) tako da se može saznati koji su procesi kreirani od strane nekog drugog procesa, za razliku od TASKLISTA. Na slici 28. prikazan je izlaz tlist alatke sa svičem „t“:



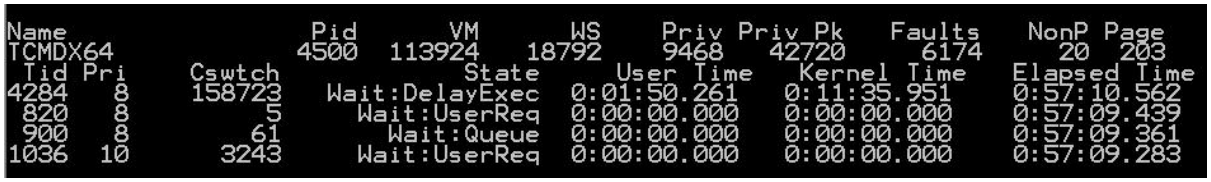
Slika 28. *Prikaz izlaza komande Tlist prema hijerhiji nastajućih procesa sa c:\tlist -t*

Alatka Tasklist je naslednik komande Tlist i sastavni je deo Windows operativnih sistema počev od Windows XP verzije. Ova alatka ima detaljan pregled procesa i forenzičaru može da obezbedi različite izlazne formate (tabelaran prikaz, prikaz sa ";" eng. csv ili kao listing). Izlistava većinu informacija o procesima uključujući i imena programa baš kao i prethodno pomenut alat, ali bez cele putanje. Može da omogući pregledan prikaz procesa i servisa sa identifikatorom procesa ukoliko se uključi svič "c:\tasklist /svc" kao na slici 29.



Slika 29. *Prikaz izlaza alata tasklist sa uključenim svičom /svc*

Alatka Pslist[248], takođe forenzičaru može da pomogne oko dobijanja informacija o procesima i kroz svoje svičeve može da omogući prikaz zauzeća memorije i procesorskog vremena (kao na slici 30.), dužinu trajanja procesa kao i hijerarhijski prikaz procesa kao kod tlist alatke. Nedostaci su mu ti, što ne pruža putanju do izvršnog programa, komandno okruženje pod kojim je startovan proces ili koji je user izvršio određen proces. Na slici 30. prikazan je izlaz pslist alatke sa svičem „x“:



Slika 30. *Prikaz zauzeća memorije i procesorskog vremena komandom c:\pslist -x*

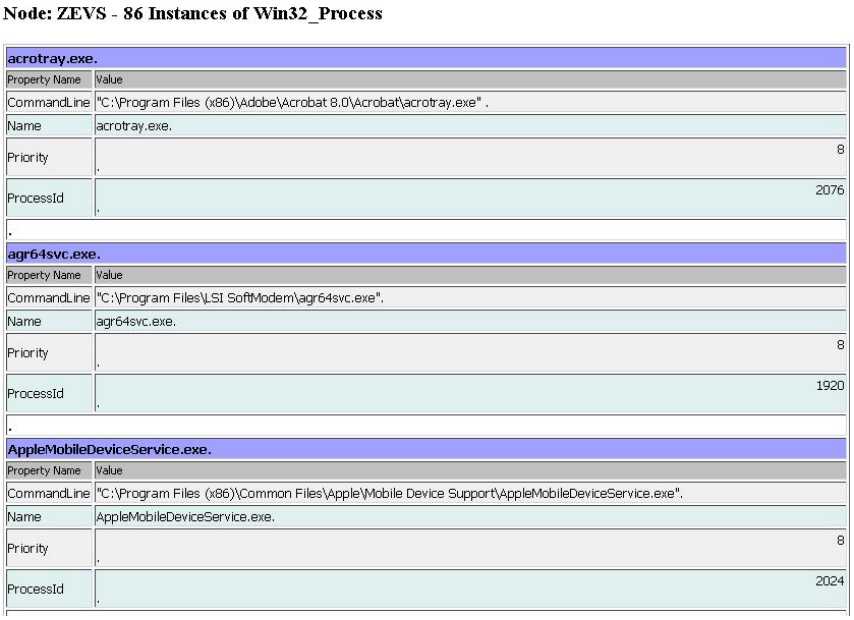
Korisna alatka koja je implementirana u Windows operativni sistem može takođe dati detaljan prikaz o procesima i celom putanjom što može biti forenzičaru od koristi sa dodatnim argumentima koji mogu da izlistane podatke snime u formate kao što su CSV ili html :

"wmic /output:wmic.csv process get name,processid,priority,commandline /format:csv" ili u html formatu što može biti i mnogo preglednije :

[248] Dostupna na http://technet.microsoft.com/en-us/sysinternals/bb896682.aspx, 02.02.2013.

"wmic /output:wmic.html process get name,processid,priority,commandline /format:hform "

Ova komanda izlistava ime procesa, ID procesa, prioritete i putanju do izvršnog fajla i prikazana je na slici 31. :



Node: ZEVS - 86 Instances of Win32_Process

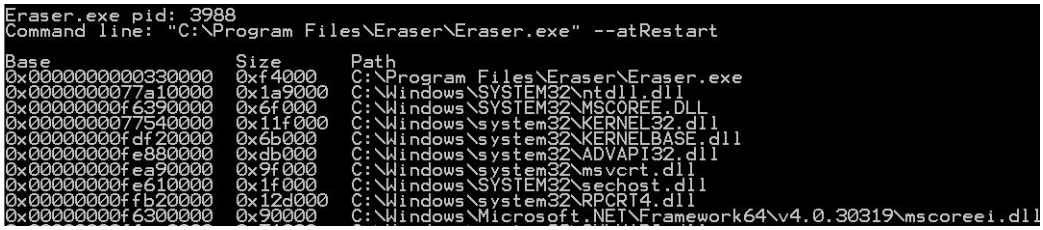
acrotray.exe.	
Property Name	Value
CommandLine	"C:\Program Files (x86)\Adobe\Acrobat 8.0\Acrobat\acrotray.exe" .
Name	acrotray.exe.
Priority	8 .
ProcessId	2076 .

agr64svc.exe.	
Property Name	Value
CommandLine	"C:\Program Files\LSI SoftModem\agr64svc.exe".
Name	agr64svc.exe.
Priority	8 .
ProcessId	1920 .

AppleMobileDeviceService.exe.	
Property Name	Value
CommandLine	"C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe".
Name	AppleMobileDeviceService.exe.
Priority	8 .
ProcessId	2024 .

Slika 31. *Prikaz procesa na ispitivanom sisemu dobijenog sa wmi komandom u html formatu*

Jako korisna alatka koja forenzičaru takođe može biti od pomoći jeste ListDLLs[249] koja je u stanju da prokaže module i DLL-ove koje određeni proces koristi. Takođe, u stanju je da pruži prikaz cele putanje do modula ili DLL-a čak i ako se verzija DLL-a učitana u memoriji razlikuje od DLL-a na disku. To je, veoma važno, jer praktično program prikazuje tačno onaj DLL, odnosno modul koji se koristi od strane aplikacije. Tako da sa ovim programom postoji mogućnost prepoznavanja nekih rootkit-ova, trojanaca i drugih malicioznih programa koji koriste tehniku DLL injection. U stvari ti maliciozni programi pokušavaju da učitaju sebe u memorijski prostor startovanog procesa da bi mogli da se startuju i izvrše, ali da se ne prikažu u listi procesa, jer su zapravo deo nekog drugog procesa. Takođe, moguće je uočiti i programe koji imaju za cilj anti-forenzičke aktivnosti kao na primer "duboko" formatiranje hard diska ili brisanje podataka pri restartu sistema, gašenju itd... Blagovremenim uočavanjem zlonamernog programa, moguće je povećati i bezbednost samog sistema i pronaći dokaz koji može biti važan deo konteksta istrage. Na slici 32. je dat primer izlaza komande Listdll u kome se vide imena procesa, Id procesa, na koji način se izvršava iz komandne linije (sa parametrom izvršenja po restartu) i pripadajući DLL-ovi sa putanjama.



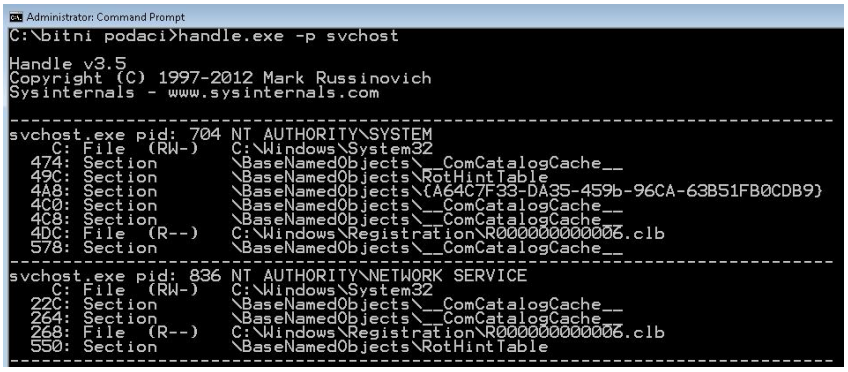
```
Eraser.exe pid: 3988
Command line: "C:\Program Files\Eraser\Eraser.exe" --atRestart

Base                Size      Path
0x0000000000330000  0xf4000   C:\Program Files\Eraser\Eraser.exe
0x000000077a10000   0x1a9000  C:\Windows\SYSTEM32\ntdll.dll
0x00000000f6390000  0x6f000   C:\Windows\SYSTEM32\MSCOREE.DLL
0x0000000077540000  0x11f000  C:\Windows\system32\KERNEL32.dll
0x00000000fdf20000  0x6b000   C:\Windows\system32\KERNELBASE.dll
0x00000000fe880000  0xdb000   C:\Windows\system32\ADVAPI32.dll
0x00000000fea90000  0x9f000   C:\Windows\system32\msvcrt.dll
0x00000000fe610000  0x1f000   C:\Windows\SYSTEM32\sechost.dll
0x00000000ffb20000  0x12d000  C:\Windows\system32\RPCRT4.dll
0x00000000f6300000  0x90000   C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscoreei.dll
```

Slika 32. *Prikaz izlaza komande Listdll*

Alatka handle[250] spada u red jako korisnih forenzičkih alatki za pregledanje procesa. Značajno je istaći da se ova alatka ne odnosi samo na prepoznavanje fajlova i foldera i

[249] Dostpuno na http://technet.microsoft.com/en-us/sysinternals/bb896656.aspx, 02.02.2013.
[250] Dostupno http://technet.microsoft.com/en-us/sysinternals/bb896655.aspx

njihovih putanja koji su u vezi sa procesima, već ide mnogo šire na otvorene portove, ključeve u Registry bazi, kao i procesorsko vreme. Tako ova alatka može da pruži informaciju o tome koje resurse koristi proces dok je aktivan. Na slici 33. je prikazan primer izlaza ovog alata sa komandom koja se odnosi samo na proces svchost "c:\handle.exe -p svchost" :



Slika 33. *Prikaz Alatke handle*

Ukoliko je neka od navedenih alatki pronašla sumnjiv proces, forenzičar može doneti odluku o tome da sazna više informacija o tom procesu, a to može uraditi dump-ovanjem onog dela memorije koje ispitivani proces koristi. U daljem tekstu biće izloženi neki alati koji mogu da izvuku sadržaj RAM memorije (kao i deo memorije nekog procesa). U forenzičkom ispitivanju taj postupak se zove memorijska analiza. Ovaj rad se neće detaljno baviti ovom vrstom analize, ali će biti izneti najbitniji načini i alati sa kojima se to može uraditi. Treba napomenuti da se onemogućavanjem nepotrebnih servisa na računarskom sistemu prilikom njegovog konfigurisanje ostvaruje dvostruki benefit : dobijanje na performansama i dobijanju na većoj bezbednosti računarskog sistema.

3.1.9 Podaci od značaja privremenog karaktera na Windows-u - Mapirani portovi od strane procesa

Ono što je značajno istaći je, da ukoliko na računarskom sistemu postoji uspostavljena mrežna konekcija ili su otvoreni određeni portovi na sistemu, to znači da iz njih stoje i određeni procesi. Da bi digitalni forenzičar utvdio vezu između portova i procesa, neophodni će mu biti određeni alati za tu namenu. Već pomenuta alatka koja je sastavni deo Windows operativnog sistema (počev od Windows XP) je netstat i može pomoći forenzičaru pri uspostavljanju korelacije između procesa i otvorenih portova. Nakon izlaska dodatnog paketa SP2 (eng. service pack) za Windows XP i dodatnog paketa SP1 za Windows 2003, ova alatka je dobila mogućnost korišćenja novog svič-a "-b", koji su izvršni programi odgovorni za otvaranje porta (u nekim slučajevima mogu biti prikazani i DLL-ovi koji koristi određeni proces). Prikaz komande netstat sa svič-evima „anob“ dat je na slici 34.

```
[mDNSResponder.exe]
  TCP    127.0.0.1:9656         0.0.0.0:0              LISTENING       2868
[iSCSIAgent.exe]
  TCP    127.0.0.1:27015        0.0.0.0:0              LISTENING       2028
[AppleMobileDeviceService.exe]
  TCP    127.0.0.1:27015        127.0.0.1:49308        ESTABLISHED     2028
[AppleMobileDeviceService.exe]
  TCP    127.0.0.1:49308        127.0.0.1:27015        ESTABLISHED     4284
[iTunesHelper.exe]
```

Slika 34. *Prikaz komande netstat sa dodatnim svičem -b (netstat -anob)*

Fport[251] je sjajna alatka koja ima jednostavnu upotrebu sa preglednim i razumljivim izlazom. Nedostatak je taj što ima podršku samo za Windows, Windows NT4, Windows 2000 and Windows XP i što forenzičar mora imati pristup administratorskom nalogu za pokretanje ovog alata. Izlaz ove alatke je sledeći :

```
C:\>fport.exe
Pid   Process        Port  Proto Path
92    svchost     -> 135   TCP   C:\WINNT\system32\svchost.exe
18    System      -> 139   TCP
28    System      -> 445   TCP
508   MSTask      -> 1025  TCP   C:\WINNT\system32\MSTask.exe
345   svchost     -> 135   UDP   C:\WINNT\system32\svchost.exe
86    System      -> 137   UDP
```

Fport mapira portove za pokrenute procese sa PID-om, imenom procesa i putanjom do slike procesa [145].

Još jedna jako dobra alatka (sa podrškom za NT4, Windows 2000 and Windows XP) jeste openports kompanije DiomondCS[252] koji ima podršku za više izlaznih formata (fport stil, csv stil ili netstat). Prilikom pokretanja ne zahteva administratorske privilegije. Daje prikaz ID procesa, ime procesa, broj porta, tip protokola i putanju do izvršnog programa prikazano na slici 35 :

[251] Dostupno na http://www.mcafee.com/apps/free-tools/termsofuse.aspx?url=/uk/downloads/free-tools/fport.aspx, 02.02.2013.
[252] http://www.diamondcs.com.au/openports/

```
C:\openports>openports.exe -fport
DiamondCS OpenPorts v1.0  (-? for help)
Copyright (C) 2003, DiamondCS - http://www.diamondcs.com.au/openports/
Free for personal and educational use only. See openports.txt for more details

Pid   Process            Port  Proto Path
4     SYSTEM         ->  445   TCP   SYSTEM
4     SYSTEM         ->  139   TCP   SYSTEM
1116  svchost        ->  135   TCP   C:\WINDOWS\system32\svchost.exe
1748  alg            ->  1029  TCP   C:\WINDOWS\System32\alg.exe

4     SYSTEM         ->  138   UDP   SYSTEM
4     SYSTEM         ->  445   UDP   SYSTEM
4     SYSTEM         ->  137   UDP   SYSTEM
868   lsass          ->  500   UDP   C:\WINDOWS\system32\lsass.exe
868   lsass          ->  4500  UDP   C:\WINDOWS\system32\lsass.exe
1256  svchost        ->  123   UDP   C:\WINDOWS\System32\svchost.exe
1256  svchost        ->  123   UDP   C:\WINDOWS\System32\svchost.exe
1304  svchost        ->  1152  UDP   C:\WINDOWS\system32\svchost.exe
1304  svchost        ->  1025  UDP   C:\WINDOWS\system32\svchost.exe
1304  svchost        ->  1153  UDP   C:\WINDOWS\system32\svchost.exe
1304  svchost        ->  1038  UDP   C:\WINDOWS\system32\svchost.exe
1372  svchost        ->  1900  UDP   C:\WINDOWS\system32\svchost.exe
1372  svchost        ->  1900  UDP   C:\WINDOWS\system32\svchost.exe
```

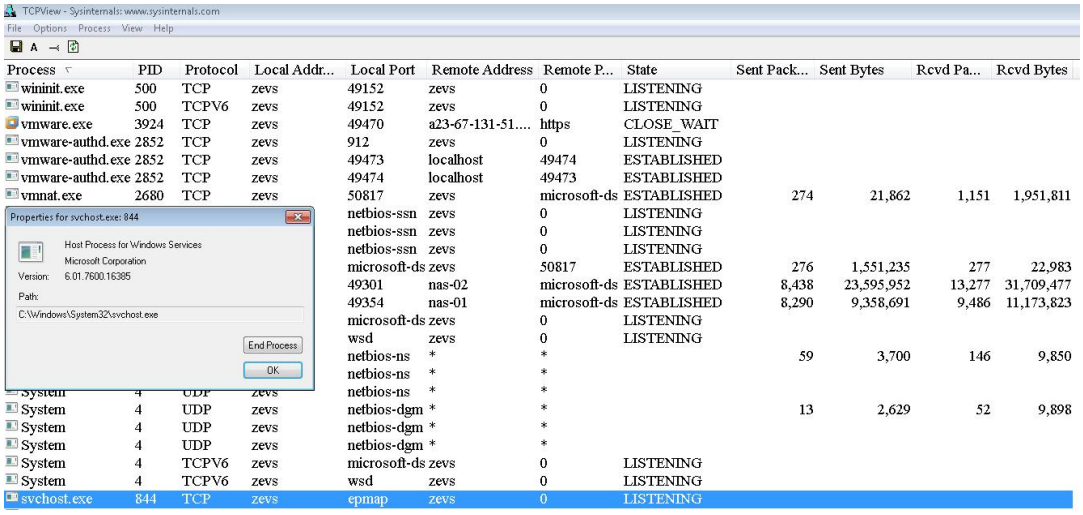
Slika 35. *Prikaz Izlaza programa opentports u f-prot stilu*

Alat Tcpvcon[253] je jedan od najboljih alata kada je reč o istraživanju otvorenih portova i procesa koji iza njih stoje. Ima mogućnost izlaza i u CSV formatu. Podržava Windows operativne sisteme od Windows XP i novije. Prikaz izlaza ove alatke dat je na slici 36.

```
C:\>tcpvcon.exe -a

TCPView v2.34 - TCP/UDP endpoint lister
Copyright (C) 1998-2003 Mark Russinovich
Sysinternals - www.sysinternals.com

[TCP] C:\WINDOWS\system32\svchost.exe
      PID:      1116
      State:    LISTENING
      Local:    winXPsp2:epmap
      Remote:   winXPsp2:0
[TCP] System
      PID:      4
      State:    LISTENING
      Local:    winXPsp2:microsoft-ds
      Remote:   winXPsp2:0
[TCP] C:\WINDOWS\System32\alg.exe
      PID:      1748
      State:    LISTENING
      Local:    winXPsp2:1029
      Remote:   winXPsp2:0
```

Slika 36. *Prikaz izlaza alata tcpvcon*

Alat TcpView[254] jedan jedan od najboljih alata ovog tipa i koristi grafički interfejs. Prikazuje detaljne informacije o svim TCP i UDP otvorenim portovima na sistemu, udaljene adrese sa kojima je ta konekcija ostvarena, kao i stanje TCP konekcije (slika 37.). Ima podršku za sve Windows operativne sisteme, počev od Windows XP-a. U paketu se isporučuje i prethodno opisana alatka tcpvcon koja je prilagođena za komandno okruženje.



Slika 37. *Prikaz TCPview alata sa apsolutnom putanjom određenog procesa*

[253] Dostupno kao deo paketa TCPView : http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx, 02.02.2013.

[254] Dostupan na http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx, 07.05.2012.

S obzirom da se radi o grafičkom alatu dokumentovati način na koji je pokrenuta aplikacija, zbog učitavanja u memoriju njega kao programa.

Naravno, forenzičar treba da zna da se ovi alati oslanjaju na API i DLL-ove iz sistema. To znači da ukoliko postoji dodatna sumnja (a ove alatke nisu našle sumnjive portove) treba uzeti u obzir i dodatno skeniranje portova od spolja, alatima kao što je NMAP[255], na ispitivanom sistemu. Takvim skeniranjem dodatno će se potvrditi da li je sistem bio kompromitovan (od strane nekog exploita ili rootkita) ili ne, odnosno da li mu je bezbednost ugrožena ili nije.

Rootkit kolekcija, odnosno komplet (eng. kit) alata, koju koristi zlonamerni napadač obično se sastoji od trojanskih alata, mrežnih snifera (prisluškivači mreže), skripte za čišćenje logova (eng. log cleaning scripts) kao i programa koji omogućavaju napadaču da ima root (najveće) privilegije na sistemu. Prema Kornblum-u svi rootkit-ovi imaju dva osnovna principa svarajući parados : prvi je potreba da budu skriveni a drugu je potreba da rade. Da bi rootkit bio skriven on mora da minimizira svoj trag na sistemu. Međutim da bi se rootkit pokrenuo operativni sistem mora da ga pronađe i izvrši [106]. U literaturi se mogu naći opisane sledeće mogućnosti ovih rootkit alata :

-skrivanje fajlova i direktorijuma;

-skrivanje procesa;

-skrivanje stavki iz Windows registra (eng. registry) kada je Windows OS u pitanju;

-sprečavanje brisanja fajlova;

-sprečavanje pokretanja antivirusnog sistema.

Kada je reč o rootkitovima iako se može pronaći veliki broj rootkitova oni se najčešće mogu podeliti na tri tipa :

- **Tradicionalni** - u ovu grupu rootkitova spadaju programi koji slušaju na nekom TCP/UDP portu, čime omogućavaju zlonamernom napadaču skriveni pristup računarskom sistemu tzv. Backdoor. Zatim postoje čistači logova (eng. log wipers) koji brišu log fajlove da bi se sakrilo prisustvo i aktivnosti zlonamernog napadača. Takođe u ovo grupu spadaju i programi dizajnirani da prisluškuju mrežu odnosno da nadgledaju i hvataju mrežne pakete od interesa kao i ddos agenti koji nevidljivo šalju UDP/ICMP pakete sa ciljem zagušenja mreže odnosno obaranja servisa.
- **Oni koji se integrišu u kernel** (eng. loadable kernel modules - LKM) Linux sistema - LKM je najčešće korišćeni rootkit protiv Linux sistema. Ovaj rootkit vrši transparentnu izmenu jezgra[256], izvršava preusmeravanje tako što premapira sistemske pozive, omogućava izvršavanje na daljinu (komandama preko mreže), omogućava promiskuitetan režim (eng. promiscous mode, skriveni režim) čime se prikriva mrežni interfejs računarskog sistema na mreži. Takođe ovim tipom rootkit-a, moguće je izvršiti kompromitovanje različitih task-ova na računarskom sistemu izmenama identifikacionog korisničkog broja (eng. user ID - UID) na sistemu[257], efektivnog identifikacionog korisničkog broja (eng. effective user ID - EUID)[258] kao i sistemski identifikacioni broj (eng. file system ID, FSUID) bilo kog procesa[259]. Takođe kada je o ovom tipu rootkit-a reč pouzdanost dobijanja dumpa odnosno slike memorije na ispitivanom sistemu dovodi se u pitanje. Ovaj problem razmatra se u radu Bradley Shatz [169].

[255] Dostupno na http://nmap.org/

[256] Postoje određene komande koje omogućavaju jezgru da se prikriju sve informacije o određenom procesu.

[257] UID na sistemu ima numeričku vrednost. preporuka iz bezbednosnih razloga je da vredsnost UID-a za korisničke naloge bude preko 1000. UID sa vrednošću 0 je specijalan i pripada root korisniku koji ima neograničen pristup sistemskim resursima.

[258] EUID služi da bi se odredio koji nivo pristupa ima trenutni proces. Kada EUID ima vrednost 0 implicira da taj proces ima neograničen pristup.

[259] FSUID se izričito koristi za kontrolu pristupa fajl sistemu. Povezan je sa EUID-om čije se promene propagiraju na FSUID. Uloga FSUID-a je da se dozvoli programima da se samoograniče putem prava na fajl sistemu prema dodeljenom UID-u, izvor http://en.wikipedia.org/wiki/User_identifier, 30.03.2012

- **Oni koji se integrišu u kernel Windows sistema** - ova vrsta rootkit-ova implementira određeni Device driver u kernel modu (eng. Device driver kernel mode)[260] na tzv. nultom prstenu procesora (na primer na CPU x86)[261] preko root.sys i pokretačkog program deploy.exe. Mogućnosti ovih rootkitova su kreiranje zadnjih vrata (eng. backdoor), skrivanje fajlova (na primer komanda dir neće prikazati skrivene zlonamerne fajlove), procesa i stavki iz registrija (eng. Windows registry) kao i presretanje aktivnosti sa tastature.

Neki od najpoznatijih rootkitova su sledeći : Vanquish[262], FU Rootkit[263], WinLogonHijack Rootkit[264], KIog Rootkit[265],]AFX Rootkit[266], BootKitBasic RootKit[267], KNARK[268], ADORE[269], Rustock.C, Skynet rootkit i drugi.

Detektovanje prisustva rootkita moguće je ostvariti sa posebnim alatima za tu namenu. Jedan takav alata je i **rootkit revealer[270]** koji je u mogućnosti da detektuje rootkit pretnju na osnovu analiza postojećih sistemskih datoteka i postojećih stavki u Windows registru (razlike ili neslaganja). Može se pokretati iz komandnog moda ili iz grafičkog moda, a može se pokrenuti i sa udaljenog sistema preko PSexec-a koji je sastavni deo PsTools suite-a. Dakle, alati za detekciju rootkit-ova u stvari otkrivaju one instalirane zlonamerne module koji presreću osnovne sistemske servise. Na te servise se oslanjaju svi programi kao i sam operativni sistem i ukoliko zlonamerni moduli postoje to znači da je ugrožena bezbednost sistema (odnosno da su aktivni određeni špijunski programi, virusi ili drugi zlonamerni programi) . U nastavku će biti navedeni još neki alati namenjeni otkrivanju rootkit-a :

- **chkrootkit** (Check rootkit)[271], otkriva prisustvo rootkita nakon njegove instalacije na Linux sistemu;
- **rkscan[272]** - je alat koji otkriva LKM rootkitove na Linux sistemima;
- **rkdet (Root Kit Detector)[273]** - njegova karakteristika je ta što se ovaj alat instalira pre zaraze rootkit-om. Predstavlja tip preventinog alata koji prepoznaje rootkit-ove na Linux sistemima i detektuje špijuniranje paketa (eng. packet sniffer);
- c**arbonite**[274] - Linux kernel modul koji izlistava sve procese na nivou kernela otkrivajući LKM rootkit-ove;

[260] U računarstvu hijerarhijska oblast zaštite se obično naziva i zaštitni prstenovi koji predstavljaju mehanizme zaštite podataka i funkcionalnosti od grešaka i zlonamernog ponašanja. Računarski operativni sistemi omogućuju različite nivoe pristupa resursima. Zaštitni prsten je jedna od dve ili više hijerarhijskih nivoa ili slojeva privilegija unutar arhitekture računarskog sistema. Prstenovi su organizovani hijerarhijski od najpovlašćenijih (obično su obeleženi brojem 0) do najmanje privilegovanih (obleženi su većim brojevima). Na većini operativnih sistema nulti prsten je nivo sa najvećim privilegijama i na najdirektniji način ima interakciju sa fizičkim hardverom kao što je CPU i memorija. dostupno na http://en.wikipedia.org/wiki/Ring_%28computer_security%29, 31.03.2012.

[261] Device drivers posebno na novijim računraskim sistemima Microsoft Windows platformi mogu da se pokrenu u kernel modu (nulti prsten na CPU x86) ili u korisničkom modu (treći prsten na CPU x86), dostupno na http://en.wikipedia.org/wiki/Device_driver, 31.03.2012

[262] Vanquish rootkit spada u alate koji vrše DLL injection odnosno ubacuju zlonamerni kod (DLL bibliteku) u određeni proces (odnosno u memorijski prostor tog procesa) menjajući mu originalnu funkicju. Realizuje skrivanje fajlova, foldera, stavki iz registarske baze i loguje šifre.

[263] FU rootkit je u stanju da sakrije procese, podigne privilegije procesu,, mrežne konekcije, mrežne portove, lažira Windows Event Viwer kako bi onemogićio forenzičku analizu i čak je moguće da sakrije drajver uređaja na osnovu DKOM-a (eng. Direct Kernel Object Manipulation) u memoriji. Ovaj sofisticirani rootikih omogućje LKM da ima direktan pristup kernelovoj memoriji, vršeći izmene nad objektima u memoriji pouzdano se skrivajući.

[264] Ovaj rootkit ubrizgava zlonamerni DLL u winlogon.exe kompromitujući Windows funkciju WlxLoggedOutSAS function a posledica je logovanje korisnika u nezaštićenom otvorenom tekstu (eng. plaintext)

[265] Ovaj rootkit je zapravo keylogger.

[266] Ovaj rootkit koristi ubrizgavanje zlonamernog koda omogućavajući skrivanje procesa, modula, portova, fajlova i registarskih ključeva.

[267]Ovaj rootkit je u suštini bootkit koji menja boot sektor sa ciljem onemogućavanja Windows NT bezbednosnog modela. Veoma je mali, podržava Windows 2000, XP, 2003 i pečuje kernel prilikom njegovog podizanja. Omogućava učitavnje dodatnih zlonamernih rootkit alata.

[268] Spada u Linux LKM rootkit-ove. Za analiziranje dostupan je na http://packetstormsecurity.com/files/download/24853/knark-2.4.3.tgz

[269]Spada u Linux LKM rootkit-ove. Za analiziranje dostupan je na http://packetstormsecurity.com/files/download/32843/adore-ng-0.41.tgz

[270] Dostupan na Windows Sysinternals sajtu : http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx, 09.12.2012

[271] Dostupan na http://www.chkrootkit.org/download.htm, 09.12.2012

[272] Dostupan na http://www.hsc.fr/ressources/outils/rkscan/index.html.en, 09.12.2012

[273] Dostupan na http://vancouver-webpages.com/rkdet/, 09.12.2012

[274] Dostupno na http://www.mcafee.com/apps/free-tools/termsofuse.aspx?url=/us/downloads/free-tools/carbonite.aspx, 09.12.2012

- **rootKit Hook Analyzer**[275]**-** ova bezbednosna alatka će proveriti da li na Windows OS postoji rootkit instaliran na operativnom sistemu koji se prikačio na sistemske servise kernela;
- **iceSword**[276] - u stanju je da prikaže skrivene procese i resurse koje Windows explorer nije u stanju da prikaže. Spada u sofisticirante alate koji se instaliraju pre rootkit infekcije i na preventivni način pruža zaštitu Windows operativnom sistemu.

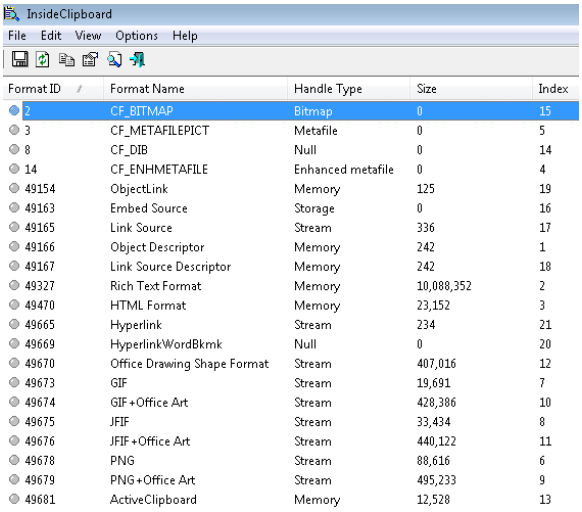
Tehnika koja se koristi za detektovanje rootkit-ova koji se integrišu u kernel OS-a u literaturi je poznata kao "cross-view" detekcija [87]. U ovoj tehnici upoređuje se spisak objekata dobijen sa dva različita izvora. Potvrđene razlike ukazuju na prisustvo rootkit-a. Ova metoda ima i svoje ograničenja, a to je da nije uvek moguće dobiti pouzdane informacije iz dve različite liste tako da ovaj pristup nije uvek primenjiv [87].

3.1.10 Podaci od značaja privremenog karaktera na Windows-u - Sadržaj privremene memorije

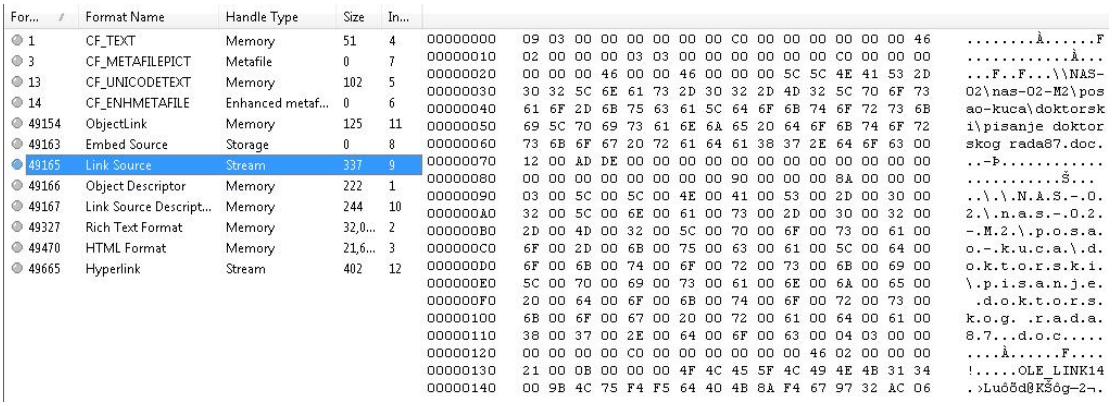
Sadržaj privremene memorije (u daljem tekstu clipboard) predstavlja prostor gde se podaci (tekstualni, binarni) privremeno odlažu za kasniju upotrebu. Većina Windows aplikacija omogućuju ovu funkcionalnost kroz svoju EDIT stavku na MENI baru putem CUT COPY i PASTE opcija (kopiranje i premeštanje dokumenata između aplikacija na Windows sistemu).

Clipboard na neki način olakšava kopiranje i premeštanje podataka (objekata) kako u samom dokumentu tako i samih dokumenata (tekstualnih i binarnih) između samih aplikacija. Razlog zašto je clipboard predmet forenzičke istrage je taj što podatak kopirani u clipboard ostaje u njemu do gašenja računara ili njegove zamene drugim podatkom. Na primer, ukoliko je na ispitivanom računaru iskopiran određeni tekst (ili web adresa ili skype konverzacija), pa zatim urađen paste u program u kome se piše elektronska pošta, ceo kopiran tekst će ostati dok se računar ne bude isključio (ili dok se korisnik ne odjavi eng. logout) odnosno dok ne bude urađen novo kopiranje u clipboard. To je još jedan veliki razlog koji ide u prilog vođenja digitalne forenzičke istrage "uživo", kada je u pitanju krađa intelektualnog vlasništva, prevare, uznemiravanja i razne druge informacije koje mogu pružiti dokaze koji mogu biti od značaja za istragu. Sadržaj clipboard-a nije "očigledno" vidljiv, ali je prisutan u sistemu što može biti i problem (jer u njemu mogu da se nađu osetljive informacije). Čak je i sam Microsoft napisao jedan članak na temu Kako sprečiti WEB sajtove da imaju pristup vašem clipbaord-u[277]. Da bi se prikupile informacije iz clipboarda postoje alati koji služe za tu namenu. Jedan dobar alat koji se pokreće iz komandnog okruženja je pclip.exe[278] koji može da izvuče tekstuelni sadržaj iz clipboard-a. Druga alatka je clipboard[279] koja može da se primeni i u Windows i u Linux okruženju koja može da izvuče tekstuelni sadržaj ili sadržaj fajla. Takođe sjajna alatka koja forenzičaru može da pruži uvid u osnovne clipboard formate kao tekst i bitmape jeste program InsideClipboard[280]. Program pruža mogućnost snimanja fajlova kao sliku, kao binarni fajl i pruža dodatne informacije o fajlu mogu se naći i informacije o putanji do fajla, veličini i tipu. Na slici 38. mogu se videti i detalji vezani za objekat u clipboardu (što ukazuje da se radi o slici). Na sledećoj slici 39. detalji iz clipboarda ukazuju da se radi o tekstu, a ono što je sjajno je to, što ovaj program pruža i uvid u putanju do samog fajla iz clipboard-a preko "Link source" pregleda.

[275] Dostupan na http://www.resplendence.com/hookanalyzer, 09.12.2012
[276] Dostupno na http://www.antirootkit.com/software/IceSword.htm, 09.12.2012
[277] Dostupno na http://support.microsoft.com/kb/224993, 09.12.2012
[278] Dostupno na http://unxutils.sourceforge.net/, 09.12.2012
[279] Dostupna na http://www.steve.org.uk/Software/clipboard/, 09.12.2012
[280] Dostupno na http://www.nirsoft.net/utils/index.html, 09.12.2012



Slika 38. *Izgled prozora programa InsideClipboard kada je u pitanju slika*



Slika 39. *Izgled prozora programa InsideClipboard sa prikazom putanje*

3.1.11 Podaci od značaja privremenog karaktera na Windows-u - Istorija pokrenutih komandi

Za digitalnog forenzičara vredan izvor informacija može da bude i istorija pokrenutih komandi na ispitivanom sitemu. Tragovi koji se mogu naću zavise od samog slučaja, na primer upotreba ftp, telnet, mapiranje drajvova, razne druge aktivnosti koje mogu da se dovedu u kontekst ispitivanog slučaja. Alatka doskey je sastvani deo operativnog sistema, upotrebljava se sa svičom "/history" i prikazana je na slici 40. :

Slika 40. *Prikaz komande doskey /history*

U registarskoj bazi moguće je takođe videti poslednju izvršenu komandu (uvek izvoditi iz proverenog komandnog okruženja) :
„HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU“

Alatka koja takođe može pomoći pri dobijanju istorije logovanja jeste alatka NTlast[281], ali oslanja se na Auditing politiku za istoriju logovanja i ukoliko ona nije omogućena, ova alatka neće pružiti potrebne informacije. To je signal da administratori na svojim sistemima obavezno omoguće auditing, jer u slučaju kompromitovanja sistema moguće je dobiti dragocene informacije. Alatka koja pruža detalje vezane za auditing na sistemu jeste Microsoft Auditpol.

Da bi se omogućio ili onemogućio auditing na sistemu, to se radi iz dva koraka. Prvi korak određuje šta da se kontroliše i šta će da se snima. To se uređuje grupnom polisom Audit Policy. Drugim korakom se određuju objekti, korisnici i grupe koje će biti kontrolisane. Na primer, ukoliko je potrebno da se prate svi neuspeli pokušaji pristupa određenom NTFS fajlu ili folderu mora da se podesi **Audit object access** policy na "**failure"**. Grupnoj polisi se pristupa preko konzolnog alata gpedit.msc. Nakon omogućavanja audit-inga na sistemu u event viewer-u pod opcijom Security, mogu da se vide stanja praćenih aktivnosti.

Event viewer-u se može pristupiti preko "**start-run-eventvwr.msc**" i u njemu možemo pregledati događanja na sistemu kroz logove aplikacija, bezbednosne logove (definisane kroz Auditing) i sistemske logove, kao i kroz druge logove koji mogu biti specifično definisani (kao na primer logove perfomansi računarskog sistema). Forenzičaru ovi bezbednosni logovi mogu ukazati na ime korisničkog naloga koji je bio ulogovan u toku računarskog incidenta [114]. Treba naglasiti da se ID-ovi događaja prijavljivanja i odjavljivanja sa sistema razlikuju između različitih verzija operativnih sistema. U prilogu 5. ovog rada dati su ID događaji koji se odnose na prijavljivanje i odjavljivanje na sistem i opisana je razlika u zavisnosti od verzije Windows operativnog sistema.

Bruce Schneier je jako lepo objasnio značaj Auditinga : "*Auditing je od vitalnog značaja gde god se bezbednost ozbiljno shvata. Postojanje Auditinga omogućava otkrivanje napada na sistem, pomaže da se razume šta se desilo nakon upada u sistem i može poslužiti za dokazivanje protivpravne aktivnosti na sudu*"[170].

3.1.12 Podaci od značaja privremenog karaktera na Windows-u - Mapirani drajvovi i deljeni resursi

Prilikom forenzičkog ispitivanja potrebno je utvrditi i koji drajvovi ili mapirani deljeni resursi postoje na sistemu. Ovi mapirani drajvovi mogu biti kreirani od strane korisnika, a mogu biti aktivnost zlonamernog korisnika koji je na neki način iskoristio administratorsku šifru. Ove informacije spadaju u privremene podatke i značajne su jer se mogu dovesti u korelaciju sa dobijenim informacijima sa već opisanim alatima u prethodnom delu rada.

Najjednostavnija komanda koja se može upotrebiti na Windows sistemima (počev od Windows-a XP) jeste putem WMI [282] (eng. Windows Management Instrumentation) komande:

„c:\wmic logicaldisk get
name,description,size,freespace,volumename,filesystem,providername"

Ovom komandom dobija se spisak drajvova koji se nalaze na sistemu, tip drajva (mrežni-mapirani, prenosni ili fiksni-lokalni drajv), ime drajva, kapacitet drajva i slobodan prostor, tip fajl sistema, i ime mapiranog drajva koji se može videtu na slici 41. :

[281] Dostupno na http://www.mcafee.com/apps/free-tools/termsofuse.aspx?url=/hk/downloads/free-tools/ntlast.aspx
[282] Dostupno na http://msdn.microsoft.com/en-us/library/Windows/desktop/aa394582%28v=vs.85%29.aspx

```
S:\forenzicki alati>wmic logicaldisk get name,description,size,freespace,volumename,filesystem,providername
Description                FileSystem  FreeSpace      Name  ProviderName                Size           VolumeName
3 1/2 Inch Floppy Drive                               A:
Local Fixed Disk           NTFS        10650468352    C:                                64020807680
CD-ROM Disc                                           D:
CD-ROM Disc                                           E:
CD-ROM Disc                UDF         0              H:                                1090861056     WFA2e
Removable Disk                                        Q:
Network Connection         NTFS        58572791808    S:    \\NAS-01\nas-01-M1          2951926571008  nas-01-M1
Network Connection         NTFS        56127721472    T:    \\NAS-01\nas-01-M2          2951926571008  nas-01-M2
Network Connection         NTFS        159937572864   X:    \\NAS-02\nas-02-M1          2951926571008  nas-02-M1
Network Connection         NTFS        1751629053952  Y:    \\NAS-02\nas-02-M2          2951926571008  nas-02-M2
```

Slika 41. *Prikaz postojećih drajvova na sistemu sa detaljima uz pomoć komande wmic*

Alatka koju je napravio Harlan Carvey i koja takođe forenzičaru može pomoći pisana je u perlu i prekompajlirana za Windows, zove se driveinfo.exe. Njen izlaz skoro isti je kao kod prethodne komande i prikazan je na sledećoj slici 42. :

```
S:\forenzicki alati>driveinfo.exe
Drive    Type        File System  Path                        Free Space
-----    -----       -----------  -----                       ----------
A:\      Removable                                            0.00
C:/      Fixed       NTFS                                     10.36 GB
D:/      CD-ROM                                               0.00
E:/      CD-ROM                                               0.00
H:/      CD-ROM      UDF                                      0.00
Q:/      Removable                                            0.00
S:/      Network     NTFS         \\NAS-01\nas-01-M1          54.55 GB
T:/      Network     NTFS         \\NAS-01\nas-01-M2          52.27 GB
X:/      Network     NTFS         \\NAS-02\nas-02-M1          148.95 GB
Y:/      Network     NTFS         \\NAS-02\nas-02-M2          1631.33 GB
```

Slika 42. *Prikaz izlaza programa driveinfo.exe*

U toku istrage takođe će se ukazati potreba za uvidom u deljene resurse ispitivanog računara. Ti podaci se nalaze u registarskoj bazi (eng. registry) pod ključem *"HKEY_LOCAL_MACHINE\System\CurrentConrolSet\Services\lanmanserver\Shares"* Postoji komanda koja je sastavni deo Windows operativnog sistema i njen izlaz dat je na slici 43. :

"c:\wmic share list brief"

```
S:\forenzicki alati>wmic share list brief
Description                Name                        Path
Remote Admin               ADMIN$                      C:\Windows
                           bitni podaci                C:\bitni podaci
Default share              C$                          C:\
                           Eraser-5.8.7_portable       D:\Eraser-5.8.7_portable
HP Photosmart C5200 series HP Photosmart C5200 series  HP Photosmart C5200 series,Localspl0nly
Remote IPC                 IPC$
Printer Drivers            print$                      C:\Windows\system32\spool\drivers
Default share              Q$                          Q:\
```

Slika 43. *Prikaz deljenih resursa na ispitivanom sistemu uz pomoć komande wmic*

Takođe jako korisna alatka sa kojom forenzičar može da proveri omogućene deljene resurse na ispitivanom računaru jeste Srvcheck (dostupna iz Windows Server 2003 Resource Kit). Srvecheck alatka nabraja korisnike i korisničke grupe koje imaju pristup uključujući i nivo pristupa. Forenzičar treba da bude svestan da ova alatka ima svoja ograničenje tj. može prikazati samo neskrivene deljene resurse.

3.1.13 Podaci od značaja privremenog karaktera na Windows-u - privremeni fajlovi

Za digitalnog forenzičara dodatan izvor relevantnih dokaza mogu sadržati i privremeni (eng. temporary) fajlovi. Veliki broj aplikacija kreiraju privremene fajlove i ostavljaju ih u računaru kada program završi sa radom ili ih brišu po zatvaranju aplikacije. Definicija privremenog fajla prema Microsoftu je da je to "fajl koji služi za privremeno smeštanje informacija da bi se oslobodila memorija za druge namene ili u funkciji bezbednosti za sprečavanje gubitka podataka kada program izvršava neke druge funkcije"[283]. To znači da je sa jedne strane omogućena najbolja iskorišćenost memorije koja je dodeljena

[283] Dostupno na http://support.microsoft.com/kb/44880

aplikaciji, a sa druge strane obezbeđena je zaštita integriteta podataka od grešaka prilikom memorisanja dokumenata, pa čak i prilikom naglog prestanka sa radom računara (nestanak struje kad je računar bez UPS-a).

Većina Windows programa kao i sam operativni sistem, zahtevaju privremeno skladišenje podataka na čvrstom disku. Ovi fajlovi se skladište u folderu "temp" i uglavnom (mada ne uvek) ovi fajlovi će imati ekstenziju .TMP. Kada operativnom sistemu ili programu oni ne budu više potrebni, brišu se od strane onog ko ih je kreirao (OS ili program) ali u praksi se dešava da to nije uvek slučaj, što forenzičaru može biti od koristi prlikom ispitivanja računarskog sistema. Na primer, Microsoft office prilikom otvaranja dokumenta automatski određuje gde i kada će se kreirati privremeni fajl. U slučaju regularnog isključivanja računara privremeni fajl se povezuje sa otvorenim dokumentom koji se memoriše i zatvara. U slučaju neregularnog isključivanja Microsoft Office programa privremeni fajl se ne briše što ostavlja prostor za forenzička ispitivanja. Fajlovi koji forenzičaru mogu biti od koristi su (kada je Microsoft office u pitanju) [130]:

1. *Word* : **~wrf0000.tmp**
2. *Word* : **~mfxxxxx.tmp**[284]
3. *Word* : **~dftxxxx.tmp**
4. *Word* : **wrf0001.tmp**
5. Kopiranje drugog dokumenta: **~wrcxxxx.tmp**
6. *Word* dokument: **~wrdxxxx.tmp**,
7. Fajl privremenog dokumenta**: ~wrfxxxx.tmp**
8. Rečnik: ~wrixxxx.tmp
9. *Clipboard*: ~**wrlxxxx.tmp**
10. Makroi: ~wrmxxxx.tmp
11. *Word OLE* dokument: **~wroxxxx.t**mp
12. *Scratch* fajl: **~wrsxxxx.tmp**
13. Konvertovani (*foreign*) dokument: **~wrvxxxx.tmp**
14. *PowerPoint*: **pptxxxx.tmp**
15. *Excel*: ~dfxxxx.tmp

Ispitivanjem ovih fajlova forenzičar može i da oporavi ove podatke koji mogu da budu potencijalni dokazni materijal. Pomenuti fajlovi se mogu pronaći na različitim lokacijama u zavisnosti od izvršene akcije nad fajlom. Najčešća mesta su u zavisnosti od verzije operativnog sistema :

„c:\Documents and Settings\<Korisnicko ime>\Local Settings\Temp” (Windows XP i ranije)
„c:\Documents and Settings\<Korisnicko ime>\Application Data\Microsoft\Word” (Windows Xp i ranije verzije)
„c:\Users<Korisnicko ime>*\AppData\Local\Temp“ (*ovde se smeštaju privremeni fajlovi od programa koje je pokrenuo korisnik, Windows Vista i kasnije verzije*)*
“c:\Windows\Temp” (ovde se smeštaju privremeni fajlovi kreirani od strane operativnog sistema)”

Takođe se mogu naći i na mestima gde je kreiran sam fajl. Prilikom pretraživanja privremenih fajlova drugih programa, (koji mogu biti smešteni na različitim lokacijama) forenzičar treba pregledati i sam folder sumnjive aplikacije koji može da sadrži veliki broj korisnih informacija od značaja za dalju istragu.

3.1.14 Postojani podaci od značaja na Windows-u -Vremenski pečati fajl sistema

U toku digitalne istrage vreme, datum i osumnjičeni predstavljaju tri ključna elementa [206]. To znači da forenzičar mora da zna kada su fajlovi od forenzičkog značaja kreirani, modifikovani ili obrisani i ko je to uradio. To je ključna stvar da bi se saznalo šta se dešavalo

[284] xxxx predstavlja broj sekvence.

na sistemu. Većina operativnih sistema održava tri vremenska pečata (eng. timestampa) za svaki fajl na sistemu, poznatih kao MAC vremena (eng. Modified, Accessed, Created)[121]. Da bi se dobili vremenski pečati svih podataka na fajl sistemu uglavnom se koristi alatka **dir.** U praksi se pokazalo da komanda „dir“ ne daje pregledan listing kao i da nije upotrebljiv na programima koji rade sa tabelama. Kao dobro rešenje alatka "find" koja je u stvari Linux alatka prilagođena za Windows dostupna u sklopu UnxUtils paketa[285].
Izlaz komande *c:\find.exe c:\ -printf*
"%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n"
je u formatu koji je upotrebljiv na svakom programu koji radi sa tabelama. Može prikazati dozvole nad fajlovima, poslednje vreme i datum pristupa, datum i vreme poslednje izmene kao i datum i vreme kreiranja fajla, zatim vlasiništvo, veličinu i punu putanju. Ovaj prikaz se uglavnom koristi u korelaciji sa već utvrđenim sumnjivim procesima i putanjama kao dodatni dokaz prisustva određenog malicioznog fajla. U nastavku sledi tabela 6. sa prikazom NTFS osobina pri određenim aktivnostima :

Tabela 6. NTFS osobine prilikom aktivnosti na sistemu

Aktivnost	Vreme kreiranja	Vreme izmene	Vreme pristupa
Izmeštanje (sa volume-na)	Ažurira se	Ne menja se	Ažurira se
Izmeštanje (u okviru volume)	Ne menja se	Ne menja se	Ne menja se
Kopiranje	Ažurira se	Ne menja se	Ažurira se
Cut & paste	Ne menja se	Ne menja se	Ažurira se

Kada je reč o vremenu izmene, sistem beleži vreme poslednje izmene datoteke, odnosno kada je datoteka poslednji put sačuvana. Vreme pristupa podrazumeva kada je datoteka poslednji put čitana i na većini operativnih sistema beleži se samo datum ne i vreme. Vreme kreiranja podrazumeva kada se fajl prvi put pojavio na sistemu. Individualne aktivnosti na računaru ostavljaju mnoge tragove pa se iz navedenih vremenskih pečata, koji se odnose na fajlove i foldere, mogu izvući veoma korisne informacije za digitalne forenzičare. Na primer, izmeštanje fajla u okviru volume-a ne menja vremena fajlu ; originalno obrisan directory entry[286] je identičan novom *directory entry*-ju. Na osnovu ove osobine forenzičari mogu da odrede gde su fajlovi izmešteni dok god postoji originalan *directory entry*. Ono što je interesantno primetiti jeste sledeće : kada su fajlovi kopirani u okviru volume-a ili premešteni sa hard diska na floppy, vreme kreiranja i vreme poslednjeg pristupa se ažuriraju, a vreme poslednje izmene ostaje isto. Za forenzičara značajan podatak jeste da se kod Windows Vista sistema ne prati vreme poslednjeg pristupa [28]. Razlog leži u činjenici da su se time povećale performanse računara. Praćenje vremena poslednjeg pristupa (koje u većini forenzičkih slučajeva nije omogućeno) može se omogućiti izmenom registarskog ključa :
"HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate".
Takođe forenzičari treba da budu svesni da vremena fajlova na sistemu ne moraju uvek biti tačni. Razloga ima dosta, a glavni koje je NIST izdvojio u svom dokumentu su sledeći [96]:

- računarski sat nema podešeno tačno vreme. Na primer, sat na računaru nije se sinhronizovao sa vremenskim serverom (ntp server) ;
- vreme ne može biti snimljeno sa očekivanim nivoom detalja. Na primer, izostanak minuta ili sekundi ;
- zlonamerni korisnik (napadač) je izmenio vremena nad fajlovima.

[285] Dostupno na http://unxutils.sourceforge.net/, 07.05.2012.
[286] Informacije o fajlovima čuvaju se u directory entry. Ove informacije zavise od operativnog sistema. Directory entry sadrži informacije kao što su vlasništvo nad fajlovm, lokacija, veličina, prava pristupa, i vremena aktivnosti (kreiranje pristup izmena)

Pomenuti vremenski pečati su samo jedna oblast fajla meta-podataka koji mogu biti od koristi prilikom utvrđivanja redosleda događaja i prirodu aktivnosti na sistemu.

3.1.15 Postojani podaci od značaja na Windows-u - Informacije o računarskom sistemu, verzija operativnog sistema i nivo ažuriranosti paketa

Kada se govori o postojanim podacima (eng. nonvolatile) misli se na podatke koji ostaju na računaru i posle reboot-ovanja ili gašenja računarskog sistema. U njih spadaju i informacije o računarskom sistemu i njegovim komponentama koje mogu biti značajne u toku istrage, jer mogu pružiti dodatan kontekst kada je reč o identifikovanju kompromitovanog odnosno malicioznog računara. U daljem tekstu biće navedeni načini na koje forenzičar može upotrebiti da bi prikupio informacije o računarskom sistemu.

Alatkom wmic (forenzički sigurna) možemo dobiti informacije o računarskom sistemu kao što su domen odnosno workgrupa kome sistem pripada, proizvođač ploče, model ploče, ime računarskog sistema, tip sistema (x86 ili x64,) ukpna RAM memorija i korisnika pod kojim je izvršena ova komanda. Izlaz ove komande dat je na sledecoj slici 43. :
"c:\wmic computersystem get domain,manufacturer,model,name,totalphysicalmemory,systemtype,username"

```
S:\forenzicki alati>wmic computersystem get domain,manufacturer,model,name,totalphysicalmemory,systemtype,username
Domain  Manufacturer                Model    Name  SystemType    TotalPhysicalMemory  UserName
NAS     Gigabyte Technology Co., Ltd.  X48-DQ6  ZEVS  x64-based PC  8588353536           zevs\vanja
```

Slika 43. *Prikaz detalja koji se odnose na postojeći sistem*

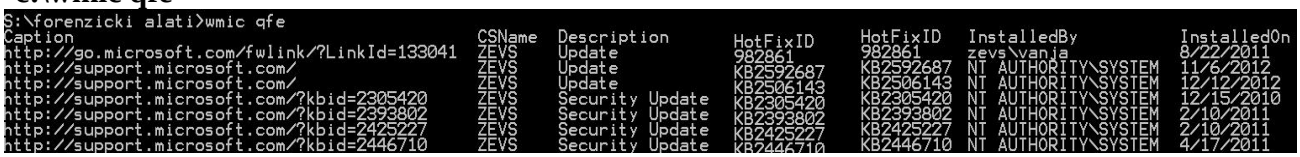
Takođe informacije koje se odnose na BIOS računara mogu se dobiti upotrebom sledeće komande :
"c:\wmic bios list full" ili "c:\wmic bios list brief"

Forenzička alatka volume_dump iz paketa Forensic Acquisition Utilities (FAU) čiji je autor George M. Garner Jr, jeste alaka sa kojom možemo dobiti informacije o uređajima za skladištenje podataka kao što su oznaka proizvođača, vendor ID, serijski broj, USN journal informacije[287] i ostale forenzički korisne sitemske informacije koje se odnose na pomenute uređaje. Izlaz ove alatke prikazan je na slici 44. :

[287]USN Journal jeste skraćeno od Update Sequence Number Journal i predstavlja funkciju u operativom sistemu koja snima promene na NTFS volume-u. Svrha USN journal-a jeste da loguje sva ažuriranja fajlova i foldera na volume-u. Zadržava se zapis operacija sistema datoteka koji se može iskoristiti za oporavak oštećenja usled neplaniranog pada sistema.

Slika 44. *Prikaz izlaza alatke volume_dump*

Informacije koje se odnose na prikaz instaliranih zakrpa (eng. hotfix) i servis pekova (eng. service pack) mogu biti prikazani preko wmi komandi i njenih argumenata kao na slici 45.:
"**c:\wmic qfe**"



Slika 45. *Prikaz instaliranih hotfix-ova i servis pack-ova sa detaljima*

Ove informacije mogu pomoći administratorima i forenzičarima da ustanove da li je potrebna zakrpa bila instalirana na ispitivanom računaru, što može dati kontekst u daljem toku istrage, odnosno ukazati na bezbednosni propust ukoliko je postojao, odnosno poboljšati sigurnost, ukoliko određena zakrpa ili servis ne postoji na sistemu.

3.1.16 Postojani podaci od značaja na Windows-u - Setovanja Registry baze

Forenzički gledano sadržaj ključeva iz registra kao i registarski fajlovi, spadaju u postojane podatke. Sa logičkog aspekta, registarsku bazu podataka koja se koristi za čuvanje sistemske konfiguracije i detalja o korišćenju, čine ključevi (eng. registry key) koji se mogu pretražiti u programu Registry editor. U fizičkom smislu se sve registarske informacije smeštaju u fajlove tzv. hive. U Windows 95 i Windows 98, registarski fajlovi ("hives") se zovu system.dat i user.dat, u Windows ME zovu se Classes.dat, User.dat, i System.dat. U Windows NT, Windows 2000, Windows XP, Windows 2003, Windows, Vista i Windows 7 operativnim sistemima postoje nekoliko registarskih fajlova bez ekstenzije koji su smešteni u folderu "*Windows\System32\Config*" i zovu se **Software**, **System**, **SAM**, **Security**, **Default**, a postoji i fajl **ntuser.dat** koji postoji za svaki korisnički nalog i nalazi se u folderu *"Documents and Settings\ime_korisnika"* (Windows XP i 2003), odnosno "*users\ime_korinika\"* (Windows Vista, 7)[288]. Hive lista sa registarskim fajlovima na sistemu nalazi se pod ključem *"HKLM\System\CurrentControlSet\Control\hivelist*[289]. Na forenzičaru je da donese odluku koje će informacije izvlačiti iz registra i koje će fajlove prikupiti za dodatnu analizu. U određenim slučajevima maliciozni korisnik može biti prijavljen na sistem u toku forenzičkog ispitivanja, pa forenzičar može doneti odluku da prati malicioznog korisnika uz očuvanje podataka - potencijalnih dokaza značajnih za istragu. Kada se sistem ponovo podiže može doći do određenih izmena nad već pomenutim podacima sa privremenim karakterom (mapirani drajvovi, startovani procesi, servisi i programi), pa te podatke forenzičar mora evidentirati i dokumentovati.

Određena podešavanja u Registry bazi mogu da se odraze na forenzička analizu i istragu. Ove podešene vrednosti u Registry-ju spadaju u postojane podatke i mogu na uticati način vođenja istrage.

Podešena registarska opcija "**Clearpagefileatshutdown**" govori sistemu da izvrši brisanje page fajla, kada se radi gašenje računara. Termin page fajl je dobio naziv na osnovu toga što se blokovi memorije koji se premeštaju nazivaju "pages". Page-ing aktivne memorije podrazumeva da se deo memorije koji nije trenutno neophodan premešta u swap odnosno page fajl, kako bi se aktivnom programu oslobodilo više memorije. Sa forenzičkog aspekta page fajl je fajl koji može sadržati vredne forenzičke informacije (šifre, delove konverzacije programa i druge značajne podatke), jer deo memorije nekog procesa (programa) može biti upisano u page fajl. To znači da po isključivanju računara informacije u page fajlu ostaju zapisane na hard disku. Ukoliko se ovaj fajl obriše prilikom isključivanja računarskog sistema, potencijalne vredne informacije mogu teško biti povraćene, a mogu biti i izgubljene. Ukoliko je vrednost *„HKLM\System\CurrentControlSet\Control\SessionManager\MemoryManagement\ ClearPageFileAtShutdown"* vrednost podešena na 1 page fajl neće biti apsolutno obrisan, već će biti prepisan sa nulama (eng. overwritten).

Windows operativni sistem poseduje mogućnost isključivanja praćenja vremena poslednjeg pristupa fajlu kroz registarsku opciju "**DisableLastAccess**". Prema Microsoftu njegovo podešavanje može uticati na perforamanse kod high-availability računarskih sistema, dok kod kućnih i kancelarijskih računara (lap-top ili desktop) nema uticaja na performanse. Mesto u Registry-ju gde se vrši podešavanje praćenja vremena poslednjeg pristupa je : *"HKLM\System\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate"*

Provera vrednosti koju ima DisableLastAccess moguće je uraditi preko alata koji je sastavni deo Microsoft operativnih sistema od (Windows XP):
"C:\Windows\system32>fsutil behavior query disablelastaccess"

[288] http://support.microsoft.com/kb/256986, 12.02.2013
[289] http://msdn.microsoft.com/en-us/library/Windows/desktop/ms724877%28v=vs.85%29.aspx, 12.02.2013

Izlaz komnde može biti DisableLastAccess = 0 ili DisableLastAccess = 1
ili reg.exe alatkom (koja je sastavni deo Windows operativnog sistema počev od Windows XP) prikazano na slici 46. :
"c:\ reg query HKLM\System\CurrentControlSet\Control\FileSystem\" **:**

```
C:\Windows\system32>reg query HKLM\System\CurrentControlSet\Control\FileSystem\

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem
    DisableDeleteNotification    REG_DWORD    0x0
    SymlinkLocalToLocalEvaluation    REG_DWORD    0x1
    SymlinkLocalToRemoteEvaluation    REG_DWORD    0x1
    SymlinkRemoteToLocalEvaluation    REG_DWORD    0x0
    SymlinkRemoteToRemoteEvaluation    REG_DWORD    0x0
    Win31FileSystem    REG_DWORD    0x0
    Win95TruncatedExtensions    REG_DWORD    0x1
    NtfsAllowExtendedCharacter8dot3Rename    REG_DWORD    0x0
    NtfsBugcheckOnCorrupt    REG_DWORD    0x0
    NtfsDisable8dot3NameCreation    REG_DWORD    0x0
    NtfsDisableCompression    REG_DWORD    0x0
    NtfsDisableEncryption    REG_DWORD    0x0
    NtfsDisableLastAccessUpdate    REG_DWORD    0x0
```

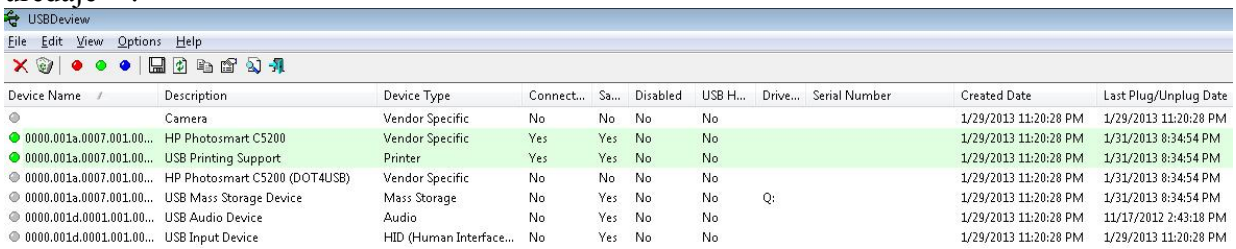
Slika 46. *Prikaz vrednosti NtfsDisableLastAccessUpdate uz pomoć komande reg.exe*

Ono što treba napomenuti je, da postavljena vrednost na 1 znači da je onemogućeno praćenje vremena pristupa fajlu na osnovu akcija čitanja i pregledanja osobina (eng. properties) fajla, ali će se vreme menjati ukoliko je došlo do izmena na samom fajlu (na primer prilikom upisa u fajl). Na Windowsu 2003 ova vrednost u registru nije podešena , na Windows Xp ova vrednost nije podešena, na Windows Visti ova vrednost je postavljena na 1, na Windows 7 ova vrednost postoji i postavljena je na 0.

Vrlo važna forenzička informacija može biti i ona koja pokazuje pristup poslednjem ključu registarske baze, što može indicirati da je ključ menjana vrednost iz nekog razloga. Ta informacija se nalazi u Registry bazi na sledećoj putanji :
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit"

Alatka **USBDeview** [290] koja forenzičaru može da pruži dragocene informacije o USB uređajima (u preglednom formatu) kako onih koji su priključeni tako i onih koji su bili priključeni na sistem. Mesto u Registry bazi koje sadrži ove informacije jeste :
"**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB**"

Detalje koje ova alatka može da prikaže, dati su na slici 47. Dobijene infomacije imaju veliki značaj s obzirom da je moguće ustanoviti, odnosno dokazati povezanost određenog perifornog USB uređaja sa ispitivanim sistemom. Mogu se uočiti : ime USB uređaja, opis, tip, da li je kontektovan ili nije, serijski broj uređaja, datum konektovanja na sistem i datum poslednje konekcije. Mana je ta, što ne podržava u potpunosti sve USB 3.0 uređaje[291].



Slika 47. *Prikaz detalja o USB uređajima uz pomoć alata USBDeview*

Druga alatka koja je besplatna i koja ima veću USB 3.0 kompatibilnost i omogućava forenzičarima dobijanje navedenih podataka jeste **Woanware USBDeviceForensics [292].** Od

[290] Dostupna na http://www.nirsoft.net/utils/usb_devices_view.html
[291] S obzirom da se alatka razvija i da često izlazi njena poboljšana verzija očekuju se poboljšanja kada je reč o kompatibilnostima sa USB 3.0 uređijima.
[292] Dostupna na http://www.woanware.co.uk/?p=280

komericijalnih programa tu su AccessData RegistryViewer[293] i besplatan alat USB Device History EnScript[294] čiji je autor Lance Mueller koji radi uz komercijalni program Guidance Software -EnCase Forensic. Mark Simms je uradio sjajnu studiju ovih alata kroz poređenje njihovih rezultata pri dobijanju informacija o USB uređajima na Windows operativnom sistemu[295].

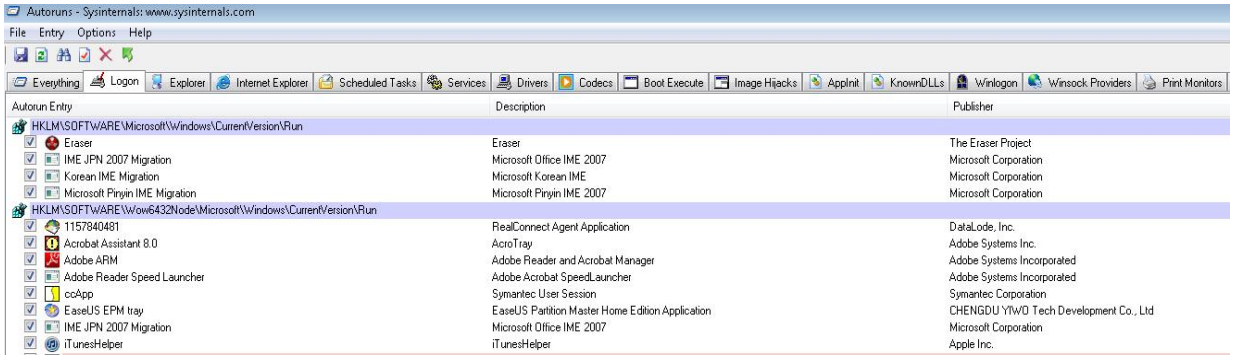
Značajne forenzičke oblasti u registru su i autostart lokacije u kojima je definisano automatsko pokretanje aplikacija, na primer pri podizanju sistema, prijavljivanju korisnika na sistem i različite akcije prilikom korisničkog pokretanja aplikacije. U slučaju da je u Registry-ju podešeno da će se prlikom pokretanja aplikacije od strane korisnika izvršiti određena akcija ili pokrenuti drugi program, to korisnik neće znati. Te lokacije nije jednostavno pronaći ali je moguće. Jedna od takvih alatki je i već pomenuta reg.exe koja je sastavni deo operativnog sistema a druga je alatka Marka Rusinovića (Mark Russinovich) i Brajsa Kogsvela (Bryce Cogswell) Autoruns koja postoji u GUI i CLI verziji sa istom funkcionalnošću. Alatka daje detaljan prikaz (slika 48.) autorun vrednosti iz Registry baze.

Autorun lokacije zapravo predstavljaju ključeve Registry baze koji aktiviraju programe u toku podizanja sistema. Uobičajene Autorun lokacije su sledeće :
"*HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce*"
"*HKLM\Software\Microsoft\Windows\CurrentVersion\policies\Explorer\Run*"
"*HKLM\Software\Microsoft\Windows\CurrentVersion\Run*"
"*HKCU\ Software\Microsoft\Windows NT\CurrentVersion\Windows\Run*"
"*HKCU\ Software\Microsoft\Windows\CurrentVersion\Windows\Run*"
"*HKCU\ Software\Microsoft\Windows\CurrentVersion\Windows\RunOnce*"
"*(Putanja do profila)\Start Menu\Programs\Startup*"

Na primer, moguće je proveriti oblast raspoređenih poslova (eng. task scheduler) koja može otkriti zlonamernu aktivnost. Raspoređeni poslovi imaju veliku korisnost za administratore u smislu održavanja sistema i mreže. Međutim, ova funkcionalnost je korisna i za napadače koji žele da se određeni maliciozni programi konstantno izvršavaju na sistemu (kao na primer Conficker-Downadup). Forenzički značajan podatak u otkrivanju takvih sigurnosnih pretnji može se naći u log fajlu rapoređenih poslova koji se zove schedlgu.txt. Ovaj fajl čuva zadatke koji treba da se startuju. U registarskoj bazi putanja do ovog fajla se može pronaći u :
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SchedulingAgent"
U Windows XP i Windows 2003 putanja do ovog fajla jeste :
"C:\Windows\SCHEDLGU.TXT"
Kod Windows Viste, Windows 7 i kasnije ta putanja jeste :
"C:\Windows\Tasks\SCHEDLGU.TXT"

Ukoliko administrator nije definisao ništa za raspoređene poslove , forenzičar može očekivati da vidi vremena startovanja i stopiranja Task Scheduler servisa. S obzirom da se ovaj servis startuje kada se startuje i sam sistem, forenzičar može imati pregleda o vremenu pokretanja i gašenja računara. Nažalost, puna putanja do izvršnog fajla neće biti prikazana u log fajlu, ali će ovaj log biti pokazatelj vremena kada je određen zadatak bio pokrenut.

[293] Dostpuno na http://www.accessdata.com/support/product-downloads
[294] Dostpuno na http://www.forensickb.com/2007/07/usb-device-history-enscript.html
[295] Mark Simms, Portable Storage Forensics: Enhancing the Value of USB Device Analysis and Reporting , Dosupno na http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&ved=0CFkQFjAE&url=http%3A%2F%2Faut.researchgateway.ac.nz%2Fbitstream%2Fhandle%2F10292%2F4687%2FSimmsM.pdf%3Fsequence%3D3&ei=lR0MUaP0IeLj4QTt2IGQDw&usg=AFQjCNFj7juCv0VaGZfLY0PB2gKz_gNsYw&bvm=bv.41867550,d.bGE , pristupljeno 01.02.2013.



Slika 48. *Prikaz mogućnosti alatke autoruns*

Prikaz raspoređenih poslova moguće je dobiti i alatkom koja je implementirana i u sam Windows sistem koja se zove "**at**".

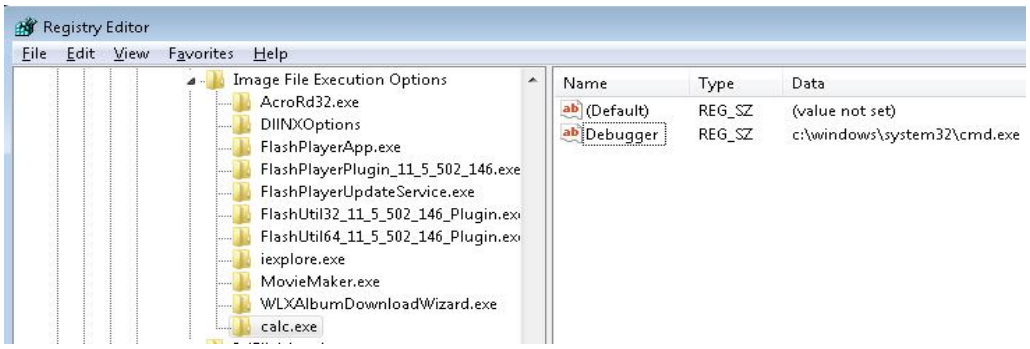
c:\at ,

gde izlaz može biti : "There are no entries in the list." ili detalji koji ukazuju na određeni posao koji treba da se obavi.

Važna oblast u registru je mesto gde je moguće sakriti program koji se zapravo startuje (maskiranje). Mesto koje forenzičar treba da ispita je zapravo sledeće :

"HKLM\Software\Microsoft\Windows NT\CurrentVersion\ Image File Execution Options"

Forenzičar treba da ispita da li je na ovom mestu kreiran neki sumnjiv podključ sa kreiranim stringom Debugger i vrednošću koja se odnosi na neki sumnjivi program. Na slici je radi demonstracije napravljen podključ sa imenom izvršnog programa calc.exe, kreiran je string sa imenom Debugger i vrednošću koja predstavlja putanju do aplikacije koja će se izvršiti (u ovom primeru je to komandni šel c:\windows\system32\cmd.exe), a to može biti neka maliciozna aplikacija.



Slika 49. *Maskiranje izvršenog program preko editor registra baze*

Posle pokrenute naredbe calc.exe u start-run-calc.exe otvoriće se komandni šel kao na slici 49.

Ova demonstracija je značajna, jer može postojati zamaskirana maliciozna aplikacija, tako da je preporuka da administratori i forenzičari obavezno pogledaju ovu oblast. Administratori mogu da otkriju napad i spreče potencijalne štete, a forenzičari mogu da pronađu dragocene informacije za dalji tok istrage.

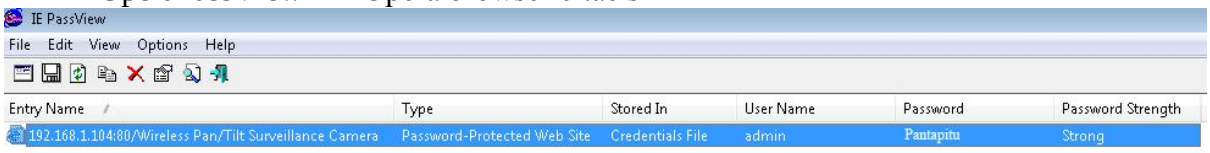
Još jedna važna oblast u registarskoj bazi koja može da pruži dragocene informacije jeste Protected storage oblast[296]. Podaci na ovom mestu se nalaze u šifrovanom obliku u registarskoj bazi. Alat koji može da dešifruje i oporavi ove podatke je forenzički alat AccessData FTK. Takođe pogodan alat za forenzičko istraživanje "uživo" je i

[296] Zaštićena oblast za skladištenje (eng. Protected storage area) jeste oblast memorije gde se osetljive korisničke informacije smeštaju. Kada je sistem isključen informacije se čuvaju u registarskoj bazi u šifrovanom obliku, dok se korisnik ne prijavi na sistem kada se te informacije prebacuju u memoriju. Te informacije su šifre i podaci iz autocomplete forme Internet Explorera ili Outlook imena naloga i šifre koji služe za odloženu upotrebu.

pstoreview.exe[297] koji može da omogući pregled ovih zaštićenih podataka, kao na primer snimljene šifre i imena korisnika u autocomplete formi putem Internet Explorera. Na primer, forenzičar može pronaći šifre i naloge određenih servisa korisnika kao i dodatne podatke usnimljene preko autocomplet forme (na primer HotMail[298], Yahoo[299], MSN[300], Paypal[301], Ebay[302] i mnogi drugi).

Sa jedne strane, može se reći da omogućavanje Autocomplete formi na sistemu može biti jedna od bezbednosnih pretnji o čemu je i pisao Brian Krebs[303] u svom članku o hakeru koji je kroz napisani Bot program kontrolisao 1000 računara dobijajući podatke upravo iz autocomplete formi kompromitovanih računara. Treba naglasiti da se zaštićena oblast za skladištenje, od verzije Windows explorera 7 više ne koristi za čuvanje naloga i korisničkih šifri, tako da alat **Passview.exe**[304] nije primenjiv posle verzije Internet explorera 6, već je forenzičaru na raspolaganju novi alat **IEpassview.exe**[305]. Na slici 50. prikazan je primer u kome su na Windows 7 operativnom sistemu ostali podaci iz Internet Explorera 9 kod korisnika koji toga nije bio svestan, tako da ukoliko bi zlonamerni korisnik imao pristup tom operativnom sistemu mogao bi dobiti korisničko ime i šifru za pristup IP kameri. To za posledicu može da ima kompromitovanje bezbednosti. Relevantni alati iste namene sa ciljem oporavka šifri iz popularnih Internet pretraživača su sledeći [185] :

- PasswordFox[306] - Mozilla Firefox čitač šifri
- ChromePass[307] - Google Chrome čitač šifri
- OperaPassView[308] - Opera browser čitač šifri



Slika 50. *Prikaz IE passview programa sa pronađenim korisničim imenom i šifrom na sistemu*

Prema tome, može se primetiti da je korisnost ovih alata dvostruka. Sa jedne strane omogućuje se digitlanom forenzičaru pristup osetljivim infomacijama "uživo" koji mogu biti značajni za dalji tok istrage (pogotovu kada se radi o krađama podataka, neovlašćenom distribuiranju podataka ili nestanku osobe), a sa druge strane tim istim alatima moguće je testirati i sopstvene slabosti na sistemu[309] što za posledicu ima povećanje bezbednosti na samom sistemu.

3.1.17 Postojani podaci od značaja na Windows-u - Tačka za oporavak sistema

Mesto gde se nalaze fajlovi potrebni za oporavak sistema (eng. System Restore Point) nalazi se pod *"c:\System Volume Information"*. Treba napomenuti da tom mestu nije moguće prići preko Windows explorera, čak ni sa administratorskim nalogom. Po difoltu sistem restore points kreira se nakon 24h i zadržava se 90 dana kod Windows Vista operativnog

[297] Dostupan na http://ntsecurity.nu/toolbox/pstoreview/
[298] http://www.hotmail.com
[299] http://www.yahoo.com
[300] http://www.msn.com
[301] http://www.paypal.com
[302] http://www.ebay.com
[303] Dostupno na http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html
[304] Dostupno na http://www.nirsoft.net/utils/internet_explorer_password.html
[305] Dostupno http://www.nirsoft.net/utils/internet_explorer_password.html#DownloadLinks
[306] http://www.nirsoft.net/utils/passwordfox.html
[307] http://www.nirsoft.net/utils/chromepass.html
[308] http://www.nirsoft.net/utils/opera_password_recovery.html
[309] Na primer moguće je uočiti postojeće šifre i osetljive informacije a da korinsik toga nije svestan, što može biti zloupotrebljeno od strane malicioznog korisnika.

sistema, dok se kod Windows 7 snapshot kreira svakih 7 dana. Oblast u Registry koja je odgovorna za sistem restore se nalazi u :

"HKLM\Software\Microsoft\WindowsNT\CurrentVersion\SystemRestore"

Fajl atributi (MAC), kao što su poslednje vreme izmene, pristupanja i kreiranja, se ne menjaju tokom kreiranja tačke za oporavak sistema. To znači da metadata MAC podaci ostaju netaknuti prilikom transfera u RP# folder[310]. MAC analizom moguće je brzo identifikovati fajlove koji se odnose na incident, na osnovu poređenja MAC vremena poznatih malicioznih fajlova i nepoznatih fajlova. Time se može pokazati kada su fajlovi uvedeni u sistem, kada su promenjeni i mogu pomoći prilikom utvrđivanja vremenskog okvira napada [77].

Sistem restore moguće je pokrenuti ručno, dok se automatski pravi pre ažuriranja Windowsa (eng. Windows update), pre instaliranja aplikacije koja poziva Snapshot API, pre restora samog sistema (u slučaju da je izabran pogrešan restore point)[311] i prilikom instaliranja nepotpisanih drajvera (eng. unsigned driver). Za digitalnog forenzičara važno je da zna da se proces vraćanja sistema na određeni datum loguje u event logu kao EVENT ID 110 i da VSS (eng. Volume Shadow Copy Service)[312] servis koji je odgovoran za restore, nadgleda sve fajlove. Takođe treba napomenuti, da restore points sadrži i prethodnu verziju same Registry baze.

Da bi digitalni forenzičar mogao da priđe podacima koje sadrži *"c:\System Volume Information"* i da ustanovi promene koje su se dešavale na sistemu na raspolaganju su mu određeni alati. Na samom Windows operativnom sistemu postoji alat vssadmin. Na primer : "c:\vssadmin list shadows" izlistaće se sadržaj *"c:\System Volume Information"*, odnosno tačke za oporavak sistema pre određene promene (slika 51.).

```
C:\Users\TouchSmart>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Contents of shadow copy set ID: {d2fb425c-311f-4cfe-b245-25000a51845c}
   Contained 1 shadow copies at creation time: 1/12/2013 2:10:59 PM
      Shadow Copy ID: {c63d21bf-5f92-4beb-8f0e-1437e051eff5}
         Original Volume: (C:)\\?\Volume{0db40ec4-3ca5-11e1-9652-806e6f6e6963}\
         Shadow Copy Volume: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
         Originating Machine: TouchSmart-PC
         Service Machine: TouchSmart-PC
         Provider: 'Microsoft Software Shadow Copy provider 1.0'
         Type: ClientAccessibleWriters
         Attributes: Persistent, Client-accessible, No auto release, Differential, Auto recovered
```

Slika 51. *Prikaz izlaza komande vssadmin*

Nakon listanja forenzičaru će biti potrebno da mount-uje određen *system restore point* na svoju forenzičku stanicu[313]. To se radi sa komandom :

"C:\>mklink/d C:\IME_I_LOKACIJA_SIMBOLICKOG_LINKA \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopyXXXXX\"

Na primer :

"C:\>mklink/d C:\snapshot10 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10\"

Ukoliko je simbolički link ispravno napravljen biće prikazano kao na slici 52. :

```
C:\Users\TouchSmart>mklink /d c:\snapshot999 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10
symbolic link created for c:\snapshot999 <<===>> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy10
```

Slika 52. *Prikaz kreiranja simboličkog linka na određenu lokaciju*

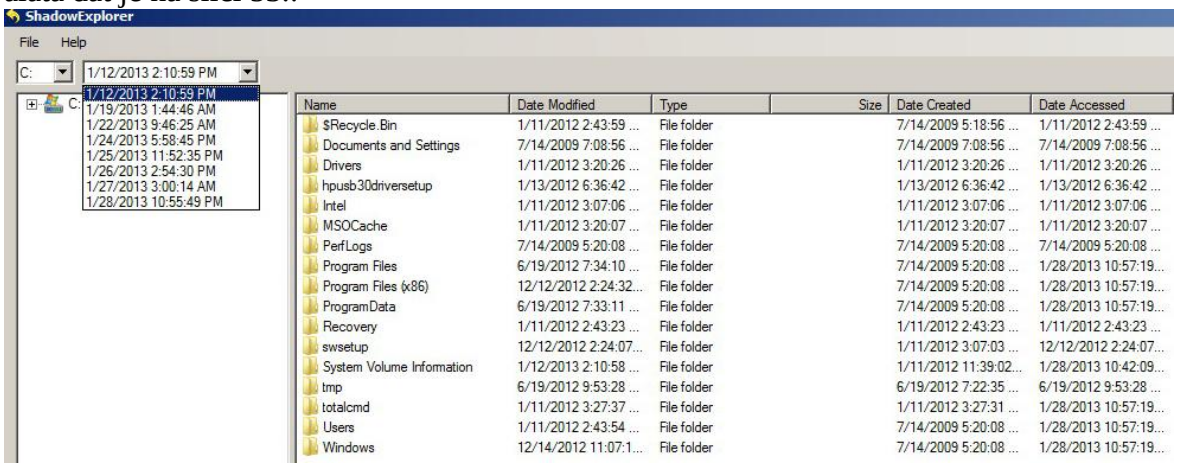
[310] Odnosi se na Windows XP.

[311] Dostupno na http://msdn.microsoft.com/en-us/library/Windows/desktop/aa378910%28v=vs.85%29.aspx

[312] Više o ovom servisu pogledati na http://msdn.microsoft.com/en-us/library/Windows/desktop/aa384649%28v=vs.85%29.aspx

[313] Ovaj način pretraživanja po mestima za oporavak sistema više je orijentisan na post-mortem analizu ili kako neki autori navode postmortem analizu kada se ispituje sumnjivi hard disk.

Nakon toga digitalnom forenzičaru će biti omogućeno ispitivanje tih mesta za oporavak sistema. Druga alatka koja daje dosta pregledniji prikaz shadows copy tj. snapshot-a, jeste Shadow explorer[314] koji funkcioniše na Windows Visti, 7 i 8. Ova alatka dopušta forenzičaru pretraživanje Shadow kopije koju kreira VSS, prikazuje datume svih snapshot-ova na sistemu i omogućava preuzimanje prethodnih verzija fajlova i foldera. Prikaz ovog alata dat je na slici 53.:



Slika 53. *Prikaz alata ShadowExplorer*

Na samom Windows sistemu moguće je na nekoliko načina onemogućiti kreiranje Shadow kopije tj. snapshot sistema ili obrisati snapshot-ove. Jedan od načina je onemogućavanje VSS servisa (eng. Volume Shadows Copy Service), zatim kroz opcije Disk Cleanup (koji omogućava brisanje svih snapshot-ova osim trenutnog). Takođe, preko opcija System protectio (My computer-system properties-system protection-configure) moguće je onemogućiti VSS servis i brisanje svih postojećih snapshot-ova. Postoji i alatka Vshadow koja dolazi sa Shadow Copy Software Development Kit[315], sa kojom se mogu obrisati svi snapshot-ovi[316] ukoliko se izvrši "**c\vshadow -da**".

Naravno navedeno maliciozni korisnik ovo može zloupotrebiti, ali digitalni forenzičar prilikom analize kompromitovanog sistema treba da uzme u obzir da će zlonamerni korisnik pokušati da ukloni tragove. Ova Microsoft VSS funkcionalost je jako dobra po pitanju zaštite podataka na sistemu i ukoliko je ona iz nekog razloga isključena, forenzičaru to može biti signal da je sistem kompromitovan (u korelaciji sa dodatnim pokazateljima), odnosno dokaz da je malicizoni korisnik pokušao da incidentnu radnju ili protivpravnu aktivnost prikrije.

3.1.18 Postojani podaci od značaja na Windows-u - Logovi na sistemu

Logovi događaja (eng. event log) su esencijalni fajlovi u operativnom sistemu. Pružaju uvid u korišćenje naloga na sistemu u svakom trenutku. Postoje sistemski, aplikativni i bezbednosni event logovi [149]. Ranije verzije Windows operativnih sistema (NT, 2000, XP i 2003) koriste sistem za logovanje poznat kao Event logging[317]. Ovaj sistem za logovanje se u Windows Visti i Windows 7 zamenio novim koji je izmenio strukturu zapisa o logovanom događaju. Novi format je postao malo kompleksniji od prethodnog i njegova struktura

[314] Dostupno na http://www.shadowexplorer.com/downloads.html

[315] Dostupno na http://www.microsoft.com/en-us/download/details.aspx?id=23490

[316] Naravno to nije jedina namena ovog alata već je proširio mogućnosti postojećeg vssadmin alata. Pomoću njega moguće je takođe izlistati sve snapshot-ove na sistemu, uraditi mount određenog snapshot-a i pristupati mu kroz određeni drajv na sistemu preko Windows explorera(eng. drive letter) i obrisati sve snapšotove sa komandom

[317] Informacije o strukturi generisanih Event logova u ovim operativnim sistemima može se naći na MSDN sajtu, dostupno na http://msdn.microsoft.com/en-us/library/Windows/desktop/aa363646%28v=vs.85%29.aspx , pristupljeno dana 30.01.2013

dostupna je na Microsoft MSDN sajtu[318]. Razlika u strukturi povlači za sobom korišćenje drugog tipa alata za analizu ovih log fajlova.

U zavisnosti na koji način je podešeno evidentiranje događaja na ispitivanom sistemu i na koji način se vrši odgovor na incident, odnosno protivpravnu aktivnost, svi pristupi sistemu biće evidentirani. Korisničkim nalozima omogućeno je dve vrste pristupa računarima : interaktivni pristup sistemu i pristup deljenim resursima. Sistemiski log fajlovi mogu sadržati informacije o korisničkim nalozima koji su korišćeni u maliciozne aktivnosti, a mogu ukazati i na to da je korisnički nalog "ukraden" odnosno zloupotrebljen bez znanja vlasnika tog naloga. Na primer, ukoliko se ispitivanom računaru pristupa od spolja (udaljen pristup ispitivanom sistemu može nekada biti jako važan da bi se sačuvali određeni podaci od izmena) i ukoliko je sistem za logovanje ispravno konfigurisan, u Security event logu će biti evidentiran svaki pristup od spolja. Lokacija (koja može da se promeni) gde se upisuju programski, bezbednosni i sistemski log fajlovi u Windows operativnim sistemima je definisana u registarskoj bazi na sledećem mestu :

"HKLM\System\CurrentControlSet\Services\Eventlog"

Za Windows Vista i Windows 7 operativne sisteme lokacija je :

"c:\widows\system32\winevt\logs\"

Za Windows XP operativne sisteme lokacije je :

"c:\widows\system32\config\"

Sistemski event logovi sadrže informacije o različitim delovima operativnog sistema. Na primer, tu se mogu pronaći informacije o učitanim drajverima, vremenima startovanja i gašenja računara, aktivnosti na CD ili DVD-u i druge aktivnosti. Aplikativni event log je na raspolaganju korisničkim aplikacijama da beleže događaje koji su od značaja za ceo sistem. Na primer, Antivirusni program može snimati informacije o ažuriranju, skeniranju ili pronađenom virusu. Bezbednosni event logovi beleže događaje vezane za upotrebu sistemskih resursa. Na primer, beleže se pokušaji koisničkih logovanja, mrežne konekcije, kreiranje otvaranje i brisanje fajlova (po difoltu bezbednosno logovanje nije uključeno).

Posle verzije Windows XP, format logova se promenio sa **.evt** na .**evtx.** Forenzičar treba da zna da svaki event log ima svoj event ID (na primer EVENT ID 540 ukazuje na logovanje dok event ID 538 ukazuje na odjavljivanje), vremenski pečat (eng. timestamp) i broj zapisa. Baza event logova koja daje dodatne informacije o određenom event log-u na osnovu njegovog ID broja, nalazi se na sajtu http://www.eventid.net/search.asp . U prilogu 5. su prikazani bezbednosni Event ID-ovi koji digitalnom forenzičaru mogu pružiti uvid u dešavanje na ispitivanom računaru, odnosno administratoru sistema mogu ukazati na potencijalni problem, odnosno poslužiti za poboljšanje bezbednosti na sistemu.

Podatke iz Event fajlova moguće je procesirati kroz log parsere (alati koji mogu preko sql komandi procesirati log fajl). Treba znati da je na Windows operativnom sistemu omogućeno logovanje programskih i sistemskih događaja, a da se po difoltu bezbednosni događaji ne loguju (ovaj podatak se odnosi na Windows XP i ranije)[319]. Kod Windows Viste i Windows 7 operativnih sistema važno je uključiti monitoring naloga na sistemu (uspešnih i neuspešnih prijava na sistem) što kao preventivna mera može podići nivo bezbednosti (otkrivajući pokušaje upada u sistem), a forenzičaru ukazati pružiti dodatan uvid u dešavanja na kompromitovanom sistemu. To se radi na sledeći način :

„start-run-secpol.msc-localpolicies-auditpolicy- Audit account logon events-properties - čekirati Success and Failure“

"start-run-secpol.msc-localpolicies-auditpolicy-Audit Logon events-properties - čekirati Success and Failure "

[318] Dostupno na http://msdn.microsoft.com/en-us/library/Windows/desktop/aa385785%28v=vs.85%29.aspx, pristupljeno dana 30.01.2013

[319] Detaljno uputstvo kako se na Windows XP omogućava bezbednosno logovanje dostupno je na http://www.microsoft.com/resources/documentation/Windows/xp/all/proddocs/en-us/els_start_security_log.mspx?mfr=true

Alati sa kojima se mogu dobiti zapisi iz logova su psloglist.exe [320] i dumpevt.exe[321] .Takođe, mogu se iskopirati svi *.evt fajlovi i forenzički se ispitivati (sve zavisi od toga koliki nivo privilegije digitalni forenzičar ima na ispitivanom sistemu "uživo"). Na slici 54. je prikazana upotreba alatke dumpevt.exe sa ispravnom sintaksom na Windows 7 x64 operativnom sistemu:

```
S:\forenzicki alati\event log\dumpevt>dumpevt.exe /logfile=sec /outfile=s:\temp.txt /reg=local_machine
1/28/2013 7:14:24 PM
Somarsoft DumpEvt V1.7.6, Copyright ⌐ 1995-2007 by Somarsoft, Inc.
LogType=Security
Computer=(local)
SystemRoot=C:\Windows
Outfile=s:\temp.txt
Use HKEY_LOCAL_MACHINE for saving record number
Format=yes
DateFormat=(locale dependent)
TimeFormat=HH':'mm':'ss
FieldSeparator=,
ReplaceFieldSeparator=  (blank)
ReplaceCR=^
ReplaceLF='
StringSeparator=;
MaxMessageLen=32000
MaxFragmentLen=32000
DumpData=none
SplitDateTime=yes
UseGmtTime=no
DumpRecnum=no
==>LastProcessed (0) < Oldest (27336), log records lost
process event log records starting with 27336
==>RegQueryValueEx rc=2 source=Microsoft-Windows-Security-Auditing type=CategoryMessageFile
==>Format message error, source=Microsoft-Windows-Security-Auditing type=Category msg=12544 rc=0
==>Format message error, source=Microsoft-Windows-Security-Auditing type=Category msg=12548 rc=0
==>Format message error, source=Microsoft-Windows-Security-Auditing type=Category msg=12545 rc=0
==>RegQueryValueEx rc=2 source=Microsoft-Windows-Eventlog type=CategoryMessageFile
```

Slika 54. *Prikaz upotrebe alatke dumpevt.exe za prikupljanje logova događaja iz sistema*

Kada su u pitanju sistemi pre Windows Viste, forenzičar može koristiti alatku (perl skriptu) za analizu log fajlova koja se zove evtrtp.exe[322]. Druga alatka koja je na raspolaganju forenzičaru je Grokevt[323] koja je takođe dobra za analizu log fajlova. Na slici 55. prikazan je izlaz alatke evtrtp.exe koja je dala analizu sysevent.evt fajla :

```
S:\forenzicki alati\event log>evtrpt.exe SysEvent.Evt
EVT file parsed: SysEvent.Evt (65536 bytes)

Total number of event records counted: 176
------------------------------
Event Source/ID Frequency

Source                                  Event ID    Count
----------                              --------    -----
EventLog                                    6005       10
EventLog                                    6006        7
EventLog                                    6009       10
EventLog                                    6011        2
HTTP                                       15007        1
MRxSmb                                      3019        1
Print                                         20        2
Print                                          3        8
Print                                          4        8
SRService                                    115        1
Serial                                         2        2
Service Control Manager                     7035       44
Service Control Manager                     7036       64
Setup                                      60054        1
Tcpip                                       4201        1
Tcpip                                       4202        1
USER32                                      1074        1
W32Time                                       35        2
W32Time                                       36        1
Workstation                                 3260        1
vmdebug                                        5        8

Total: 176
------------------------------
Event Type Frequency

Type                 Count
----------           -----
WARNING                 20
INFORMATION            156

Total: 176
------------------------------
Date Range (UTC)
Mon Jun 27 08:57:18 2011 to Wed Jan 30 13:35:39 2013
```

Slika 55. *Prikaz analize sysevent.evt log fajla alatkom evtrtp.exe*

Alatka koja može procesirati .evtx fajlove jeste log parser[324] i njen prikaz dat je na slici 56. :
Komanda se upotrebljava sa sql sintaksom :
"logparser.exe "SELECT * from application.evtx" -i:evt"|

[320] Dostupno na http://www.systemtools.com/somarsoft/?somarsoft.com

[321] Dostupno na http://www.systemtools.com/cgi-bin/download.pl?DumpEvt

[322]Dostupno na disku koji se dobija uz knjigu Windows Forensic Analysis od Harlana Carvey [78].

[323] Dostupna na http://projects.sentinelchicken.org/grokevt/download/ , pristupljeno dana 30.01.2013.

[324] Dostupno na Microsoft sajtu http://www.microsoft.com/en-us/download/details.aspx?id=24659#overview, 12.02.2013

Slika 56. *Izlaz alata log parser izvršenog nad fajlom application.evtx*

Osim event log fajlova na računaru je moguće pronaći log fajlove kako od strane sistema tako i od strane aplikacija i oni mogu biti jako dobar i koristan izvor podataka o dešavanjima na računaru.Windows XP pri instalaciji kreira negde oko 135 log fajlova ili osnovnih tekst fajlova koji rade kao log fajlovi [130]. Forenzičar u ovim log fajlovima može pronaći vrlo relevantne podatke o tome kada je program prvi put instaliran na sistem, vreme poslednjeg pokretanja programa, na koji način je konfigurisana i koja je bila kada je poslednji put startovana. Međutim, nije uvek očigledno na koje se procese ili aplikacije određeni log fajlovi odnose. Ponekad je potrebno da forenzičar pretraži ceo disk u potrazi za *.log fajlovima i da ih svaki ispita ponaosob. Takođe, u log fajlovima se mogu naći i informacije o mogućim problemima u vezi sa određenim programom ili procesom na sistemu pa blagovremenom reakcijom moguće je sprečiti protencijalni bezbednosni problem kako aplikacije tako i celog sistema.

Na Windows XP operativnom sistemu i Windows 2003, lokacija od forenzičkog značaja može biti log fajl koji generiše alatka Dr. Watson[325]. Ova alatka skuplja informacije o sistemu i programskim greškama u tekstualni log fajl. Taj fajl može se poslati na analizu stručnjacima za rešavanje problema na sistemu. Takođe, može biti značajna i forenzičarima prilikom istrage operativnog sistema. Nalaze se na lokaciji :
"c:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson"
Putanja ovog alata je definisana u registarskoj bazi pod sledededećim ključem :
"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DrWatson"

Ono što je značajno reći za alatku DrWatston jeste da kada se pojavi određena greška, informacije o njoj snimaju se u fajl drwtsn32.log fajl. Format ovog fajla sastoji se od putanje programa koja je uzrokovala grešku zajedno sa datumom i vremenom nastanka. Ove informacije su dragocene za istragu, pogotovo kada su u pitanju maliciozni programi ili posledice upada na sistem ili zloupotrebe. Sve te informacije forenzičar može staviti u kontekst dešavanja na sistemu, na primer : kada je maliciozni korisnik dobio pristup serveru, koji je proces pokrenut (što može da se vidi iz podataka o vremenu instalirane aplikacije), koji su DLL-ovi učitani od strane sumnjivog programa koji je izazvao određeno programsko odstupanje (eng. access violation odnosno eng. application exception). DrWatson takođe kreira i crash dump fajl (user.dump) koji se nalazi u istom direktorijumu baš kao i drwtsn32.log fajl. Ovaj dump fajl može se pročitati sa alatkom Windbg[326] koja je deo Microsoft Windows Debugging alata. Treba reći da fajl user.dump sadrži samo poslednje aplikativno odstupanje a prepisuje se njenim novim nastankom. Ovaj fajl izuzetno je dragocen, jer može da sadrži šifre, čiste tekstualne podatke (eng. plain text) ili dešifrovane podatke i podatke koji ukazuju na aktivnost malicioznog korisnika.

S obzorom da DrWatson32 alatka nije dostupna na Windows Vista/Server 2008/Windows 7/Server 2008 R2, moguće je koristiti podatke koje generiše WER (Windows Error Report). Kada nastane aplikativno odstupanje u event logu će se pojaviti EVENT ID sa brojem 1000 koji ukazuje da se radi o aplikativnoj grešci. Kada se desi da aplikacija ili servis krahiraju (access violation odnosno application exception) postoji nekoliko lokacija gde forenzičar može pronaći user.dmp fajl.

[325] Dostpuno na http://support.microsoft.com/kb/308538, 12.02.2013
[326] Dostupno na http://www.windbg.org/

Ukoliko je krahirala aplikacija koja je kontrolisana od strane UAC-a (eng. User Access Control) dump će biti smešten na :
"C:\ProgramData\Microsoft\Windows\WER\ReportArchive"
ili
"C:\ProgramData\Microsoft\Windows\WER\ReportQueue" u zavisnosti od toga, da li je mode queue podešen ili ne.
Ukoliko je krahirala aplikacija koja nije kontrolisana od strane UAC-a (eng. User Access Control) dump će biti smešten na :
"C:\Users\Ime_Korisnika\AppData\Local\Microsoft\Windows\WER\ReportArchive" ili
"C:\Users\ Ime_Korisnika \AppData\Local\Microsoft\Windows\WER\ReportQueue"
Za forenzičara najlakši način pretraživanja ovih fajlova je sa alatom dir :
*"c:\dir *.*dmp /s ProgramData\Microsoft\Windows\WER\"* i
*"c:\dir *.*dmp /s c:\users\"*

Ovi dump fajlovi mogu da se verifikuju alatkom dumpchk.exe o kojoj je već bilo reči, a učitavaju se sa, već pomenutom alatkom windbg.exe.

Svi ovi opisani logovi mogu biti izuzetno značajni prilikom dokazivanja i potkrepljivanja vremenskog okvira aktivnosti na sistemu. Na primer, napadač je iskoristio ranjivost određenog sistema, izvršio upload malicioznih alata i prilikom pokretanja došlo je do greške application exception. Na osnovu iznetog, moguće je pronaći logove pristupa napadača sistemu. Logovi pokazuju vreme kada je izvršen upload alata (zajedno sa IP adresom), Event logovi će ukazati na grešku application exception, a Drwatson log bi ukazao na aplikaciju koja je to izazvala. Sve ove informacije forenzičaru mogu pomoći da učvrsti svoj stav o tome koje su aplikacije već postojale na sistemu pre pristupa malicioznog korisnika sistemu, koje je programe on dodao i vreme kada su one pokrenute na sistemu. Sa bezbednosne strane gledišta logovi su korisni samo ukoliko se redovno pregledaju.

3.1.19 Postojani podaci od značaja na Windows-u - Recycle bin i obrisani fajlovi

Recycle bin ili korpa za otpatke se može posmatrati metaforično kao bacanje zgužvanih papira u korpu za otpatke. Papiri su bačeni, ali su još uvek tu. Prema analogiji podaci koji su obrisani sa sistema premeštaju se u oblast recycle bin i još uvek su prisutni na sistemu. Korisnost Recycle bin-a ogleda se u tome, da kada se određeni podatak slučajno obriše moguće ga je povratiti na njegovu prethodnu lokaciju. Dakle, kada se nešto obriše sa desktopa ili kroz Windows explorer to nije stvarno nestalo, već je premšteno u recycle bin. Ovaj recycle bin direktorijum je prisutan u fajl sistemu u korenskom (root) direktorijumu svakog hard diska. Za forenzičku istragu izuzetno je značajan, jer može sadržati dragocene podatke. Postoje razlike u formatu i načinu smeštanja izbrisanih fajlova kod određenih verzija Windows operativnih sistema. Kod Windows XP operativnog sistema kada se fajl obriše (ne računajući na komandu del i erase pod komandnim okruženjem) kreira se poddirektorijum za određenog korisnika u RECYCLER direktorijumu [57]. Naziv ovog poddirektorijuma se imenuje sa korisničkim bezbednosnim identifikatorima SID kao na primer :
"C:\RECYCLER\S-2-6-26-1839457583-836208765-1990"

Potrebno je reći da kada se otvori Recycle bin sa desktopa on će direktno pristupiti poddirektorijumu aktivnog korisnika prikazujući obrisani sadržaj. Ukoliko se vrši analiza preko forenzičke slike, moguće je dobiti informacije o korisničkim aktivnostima, koliko je često praženjen Recycle bin i identifikovanje tipa fajlova na osnovu razumevanja formata imenovanja[327]. Na primer, kada se preseli fajl u Recycle bin, biće preimenovan prema Microsoft konvenciji imenovanja u :
"D<original drive letter of file><#>.<original extension>"

[327] Dostupno na http://support.microsoft.com/kb/136517, 12.02.2013

Ime fajla počinje sa D, zatim slovo drajva sa kog je fajl obrisan, broj obrisanog fajla indeksiranog od nule i originalna ekstenzija. Prilikom brisanja fajla kompletna putanja i ime fajla čuva se u skrivenom fajlu INFO2 koji se nalazi u RECYCLER direktorijumu (ukoliko je u pitanju NTFS) odnosno RECYCLED (ukoliko je u pitanju FAT32). Ovaj fajl sadrži informacije o svim fajlovima koji su trenutno u Recycle bin-u. Zahvaljujući Keith Jones-u dokumentovan je format INFO2 koji je izuzetno dragocen za forenzičku analizu. Sadrži podatke koji se odnose na svaki fajl iz Recycle bin-a, ime drajva, vremenski pečat o vremenu nastanka fajla u Recycle bin-u, veličina fajla, ime i putanja fajla u ASCII i Unicode formatu [95]. Forenzički alati koji mogu pomoći za dobijanje svih pomenutih informacija iz INFO2 fajla su **Recbin.pl** alat čiji je autor Harlan Carvey, **Rifiuti.exe**[328] čiji je autor Keith Jones ili poboljšana alatka **Rifiuti2.exe** [329] . Ukoliko korisnički poddirektorijum u Recycler direktorijumu sadrži samo desktop.ini fajl i mali INFO2 fajl, vreme poslednje modifikacije INFO2 fajla koje može da se dobije pomenutim alatima, jeste vreme kada je Recycle bin ispražnjen. Sa bezbednosnog aspekta administratori i forenzičari moraju biti oprezni sa fajlovima koji se nalaze u Recycler direktorijumu ali koji se ne čuvaju pod korisničkim SID poddirektorijumom i sa onim fajlovima koji se ne poklapaju sa pomenutom konvencijom imenovanja obrisanih fajlova. Ovi fajlovi mogu ukazivati na zlonamerne programe (Autorun tipa) [104] ili aktivnosti zlonamernog korisnika sa ciljem prikrivanja fajlova [105]. Takođe, forenzičari moraju biti upoznati da određeni Antivirusni programi (kao na primer Symantec Norton Antivirus[330] koji kreira fajl nprotect.log[331]) mogu korisiti folder Recycler.

Kao što je već spomenuto implementirana arhitektura Recycle bin mehanizma promenjena je nakon Windowsa XP. Promene omogućuju poboljšanja koja se odnose na dobijanje više korisnih informacija o obrisanim fajlovima kada je u pitanju forenzička analiza. Kod Windows Viste i Windows 7, obrisani fajlovi se i dalje vezuju za korisnički SID kao i kod Windows XP, ali je promenjena lokacija i sada se nalaze u c:\$Recycle.Bin direktorijumu. Druga promena odnosi se na imenovanje obrisanog fajla. Nakon što se fajl obriše, kreiraju se dva fajla. Prvi fajl tzv. $R fajl, predstavlja kopiju sadržaja obrisanog fajla koji će biti preimenovan u "$R" uz seriju od 6 random karaktera (mada konvencija imenovanja pod Windows Vistom i Windows nije kompletno poznata [112]) i pridruženu ekstenziju (na primer $R3rkd37.doc). Drugi fajl tzv. $I fajl ($I3rkd37.doc) je fajl koji sadrži metadate podatke originalnog fajla (obrisanog fajla) sa informacijama sličnim kao kod INFO2 fajla kod Windows XP sistema. Ovaj $I fajl sadrži ime originalnog fajla, veličinu fajla, datum i vreme brisanja fajla [111]. Dakle, rezultat brisanja jednog fajla, za posledicu ima kreiranje dva fajla u Recycle bin-u što može predstavljati potencijalni problem. Timothy Leschke u svom radu [112] ukazao je upravo na taj problem sa kojim se susreću forenzičari prilikom analize ovih fajlova u Windows Vista i 7 okruženju, a to je generisana velika količina fajlova od strane sistema koje je potrebno analizirati. Na primer, sprovodi se forenzička analiza na Windows 7 operativnom sistemu u kome je zlonamerni korisnik obrisao 200 različitih fajlova. Od ovih 200 fajlova nastaje 400 fajlova ($R+$I). S obzirom da Windows 7 ima VSS (eng. VOLUME SHADOW COPY SERVICE, o kome je već bilo reči) tj. sistem za arhiviranje stanja sistema (eng. snapshot), ovi fajlovi će se arhivirati svako veče (ukoliko je sistem konfigurisan da pravi snapshot svaki dan) i posle 30 dana broj fajlova će narasti sa 400 na 12000 fajlova jer kopija svakog fajla iz $Recycle.Bin foldera biće kreirana u svakom novom snapshot-u. Upravljanje tolikom količinom podataka jeste problem za forenzičara. Na koji način forenzičar na Windows 7 operativnom sistemu može prikupiti dragocene informacije za dalji tok istrage iz Recycle bin-a i generisanih fajlova od strane

[328]Dostupno na http://www.mcafee.com/hk/downloads/free-tools/rifiuti.aspx

[329] Alatka Rifiuti2.exe ima podršku za Windows lokalizovan na različitim jezicima, strožiju proveru na greške i može prozvesti izlaz u XML format. Dostupno na http://code.google.com/p/rifiuti2/

[330] Dostupno na http://www.symantec.com/index.jsp

[331] Ovaj log fajl moguće je pročitati sa alatkom Nprotect viewer kompanije StepaNet Communications Inc. (http://stepanet-communications-inc.software.informer.com/) koja je deo paketa DataLifter.

VSS mehanizma, biće ilustrovan sledećim primerom. Pretpostavimo da se radi o malicioznom korisniku za koga se sumja da je učesnik u distribuiranju fajlova zabranjenog pornografskog sadržaja ili određenih malicioznih alata. On je ove fajlove obrisao kako bi sakrio dokaze protivpravne aktivnosti i ti fajlovi su dospeli u Recycle bin. Pod pretpostavkom da je priključio svoj externi USB hard disk na operativni sistem radi manipulacije sa fajlovima, operativni sistem će instalirati nove drajvere za eksterni USB hard disk. To će biti okidač za VSS mehanizam da kreira snapshot. To znači da će svi podaci Recycle bin-a takođe biti sačuvani u snapshotu. U ovom trenutku ukoliko maliciozni korisnik isprazni Recycle bin, sa namerom da se trajno izbrišu kompromitujući falovi, to se neće ostvariti. Kopija ovih kompromitujućih fajlova će biti sačuvana u snapshot-u. S obzirom da je preostali dokaz arhiviran u snapshotu, sledeći korak forenzičara je realizovanje uspešnog pristupa ovom dokazu kako bi se on detaljno ispitao. O mogućem načinu pristupa snapshot-u kroz VSS već je bilo reči.

Fajlove koji su izbrisani iz Recycle bin-a moguće je potpuno ili delimično oporaviti u offline forenzičkom postupku. Nakon brisanja fajlova u modernim operativnim sistemima, fajlovi nisu zaista obrisani. Umesto toga, mesto gde se fajl nalazio, fajl sistem obeležava kao raspoloživo za upisivanje drugih fajlova. Sve dok taj rapoloživ prostor nije prepisan (eng. overwriten) drugim fajlom, stari fajl moguće je iščitati specifičnom alatima. Oporavljanje ovakvih fajlova naziva se karving (eng. Data carving). Karving podataka podrazumeva tehniku prepoznavanja obrisanih fajlova ili delova fajlova na osnovu hedera podataka. Na primer, ukoliko je obrisan fajl veličine 200 MB i kasnije upisan novi 80 MB fajl u memorijski prostor (koristeći istu početnu memorijsku adresu fajla od 200 mb) preostalih 120 MB će predstavljati slek prostor (o kome je već bilo reči u prethodnom delu rada) koji može da se identifikuje specijalnim alatima i oporavi deo fajla. Dakle, prepisujući izbrisane fajlove drugim informacijama, izbrisani fajlovi će biti nečitljivi „za gotovo sve praktične upotrebe“ [50]. Defragmentacija jeste jedan od primera gde se na brz i lak način mogu prepisati podaci. Forenzičar takođe, treba da ima na umu da su mnogi sistemi konfigurisani da rade periodičnu defragmenticiju, ali da korisnik može i ručno nju pokrenuti što se može uraditi sa ciljem prikrivanja dokaza. Forenzičkim ispitivanjem se može prepoznati ta razlika. Jednom prepisani podaci nekada nisu dovoljni za njihovo potpuno uništenje i sa specijalnim forenzičkim alatima moguće je njihovo oporavljanje ili oporavak bar jednog njihovog dela. Postupci sa kojima je moguće kompletno brisanje fajlova, a koje forenzičar mora da zna da bi ih prepoznao kao nameru prikrivanja i uništavanja dokaza su sledeći :

a. Automatski wipe-ing – U literaturi se navodi da je prepisivanje podataka 10 do 12 puta dovoljno da se onemogući oporavak podataka koristeći sve aktuelne tehnike i alate. Obično se postiže korišćenjem komercijalnih programa koji naizmenično popunjava raspoloživ prostor nulama i jedinicama ili upisom slučajnih (eng. random) podataka. Digitalni forenzičar može prepoznati, da li je korišćena ova metoda za uništavanje dokaza.
b. Ručni wipe-ing (eng. File churning)- podrazumeva brisanje određenih podataka, kopiranje velike količine „legitimnih“ podataka (nekada do popunjavanja hard diska) , brisanje tih podataka i postupak defragmentacije, ponovljenih nekoliko puta. Ovaj postupak je teže uočljiv forenzičarima.
c. Fizičko uništavanja medija – jedini način definitivnog uništenja podataka, jeste fizičko uništenje medija na kom se podatak nalazi.

3.1.20 Postojani podaci od značaja na Windows-u - Print spooler fajlovi

Glavna komponenta u Windows okruženju za štampanje je print spooler (eng. Simultaneous peripheral operations on-line). On u privremenom fajlu čuva stranu koju je

određena aplikacija poslala na štampanje. Aplikacija i štampač mogu simultano upisivati i isčitavati fajlove u print spooler-u [130]. Na primer kada se fajl šalje štampaču, lokalni printer provajder (localspl.dll) upisuje sadržaj u spool fajl (.spl) i kreira poseban grafički fajl (.emf) za svaku stranu. Za forenzičko ispitivanje je važno ono što localspl.dll prati, a to su informacije o korisničkom imenu, imenu fajla (i drugi detalji vezani za dokument koji se šalje na štampu) i smešta ih u shadow fajl (.shd). Po difoltu fajlovi .spl i .shd su upisiju u spool folder. U zavisnosti od konfiguracije štampača ovi fajlovi se mogu smeštati u Windows virtualnu memoriju na hard disku ili u keš memoriju operativnog sistema.
"C:\Windows\System32\spool\PRINTERS"

U zavisnosti od konfiguracije štampanja, s obzirom da se ovi fajlovi .spl, .shd i .emf fajlovi brišu nakon što se završi štampanje forenzičaru će biti potrebno izvlačenje ovih fajlova iz nealociranog prostora.

Jedan od programa koji to uspešno radi je AccessData FTK [332] u post-mortem forenzičkoj analizi. Međutim, forenzičar može pronaći ove fajlove ukoliko je postojalo neuspelo štampanje ili je štampanje bilo prekinuto isključivanjem ili restartom računara.

3.1.21 Postojani podaci od značaja na Windows-u - Fajlovi linkova i najčešće korišćeni fajlovi

Windows fajlovi linkova (eng. shortcut file) ili prečice za digitalnog forenzičara mogu biti korisni jer mogu sadržati bitne informacije za dalji tok istrage. Ovi fajlovi predstavljaju linkove do određenih fajlova, programa, i sistemskih obejkata izvan fajl sistema (kao na primer mrežni uređaji, štampači, skeneri, eksterni diskovi, kamere i druge periferne uređaje). Linkovi čuvaju poslednje vreme pristupa ili izmene ciljnog fajla odnosno datoteke, što može biti od izuzetne koristi kada je ciljani fajl obrisan. To znači da, iako datoteka ne može biti oporavljen link fajl, može da pruži informaciju o tome kada je datoteka poslednji put bila prisutna na sistemu. Ovi fajlovi imaju ekstenziju .lnk i zbog toga se deklarišu kao LNK fajlovi. U praksi najčešće se nalaze na desktopu operativnog sistema, u Windows rescent folderu, u Windows start meniju, u omiljenim lokacijama (eng. favourites) Internet pretraživača.
Takođe, jedna od značajnih lokacija koja sadrži link fajlove do mrežnih resursa jeste :
"C:\Users\(User Name)\AppData\Roaming\Microsoft\Windows\Recent Items\Network Shortcuts"
Ova lokacija može pokazati forenzičaru kojim fajl serverima je osumnjičeni pristupao i vreme kreiranog linka.

Detaljnijim ispitivanjem fajlova linkova, forenzičar može steći sliku o tome kako je računarski sistem personalizovan (na koji način korisnik pristupa programima, folderima i fajlovima). LNK fajlovi mogu biti kreirani na različite načine, kao na primer od strane samog korisnika, prilikom instalacije operativnog sistema ili u toku instalacije ili izvršenja programa. Jesse Hager je odradio veliki posao obradivši strukturu LNK fajlova i njegov rad se može naći na sajtu Google code[333]. LNK fajlovi sadrže vremenske pečate i sadrže punu putanju fajla, do fajla na koga se link odnosi. Ove informacije nisu toliko očigledne pa se zahteva od forenzičara dodatno dekodiranje, na osnovu relevantnog offseta bajta (koji ukuzuje da se radi o lnk fajlu). Jedna od alatka koja može forenzičaru pomoći u analizi lnk fajla, jeste JAFAT perl skripta (koja radi pod Linuxom)[334]. Druga alatka, koja takođe analizira lnk fajl jeste linkextractor[335] koja radi u komandnom okruženju i izlaz fajla dat je na slici 57. :

[332] Dostupno na http://www.accessdata.com/products/digital-forensics/ftk
[333] Dostupno na http://code.google.com/p/8bits/downloads/detail?name=The_Windows_Shortcut_File_Format.pdf&can=2&q=, 12.02.2013
[334] Dostupono na http://sourceforge.net/projects/jafat/files/lnk-parse/lnk-parse-1.0/, 12.02.2013
[335] Dostupno na http://www.tarasco.org/security/Lnk_Analyzer/index.html, 12.02.2013

```
S:\forenzicki alati\lnkextractor>lnk.exe -o FileZilla.lnk
Rkdetector v2.x : LNK Plugin Analyzer
(c) 2006 Andres Tarasco Acu±a - atarasco@gmail.com
Url: http://www.rootkitdetector.com

Size: 1211
LOW: 0x00000000
LOW: 0x000004bb
[+] Block Device FileZilla.lnk opened (1211 Bytes)
guuid       : {00021401-0000-0000-c00-0000046}
Attributes  :   MODIFIED_SINCE_BACKUP
Creation    : 08/01/2012 13:41
Modification: 27/07/2012 08:43
Access      : 08/01/2012 13:41
File Size   : 8185344 Bytes
IconNumber  : 0
Window Param: SW_NORMAL
HotKey      : 0
FileLocation Flags    : LOCAL_VOLUME
LocalVolumetype: Fixed (Hard disk)
LocalVolumeSerialNumber: 7e8c0f00
Path:  C:\Program Files (x86)\FileZilla FTP Client\filezilla.exe
Global File Offset:     0x1
```

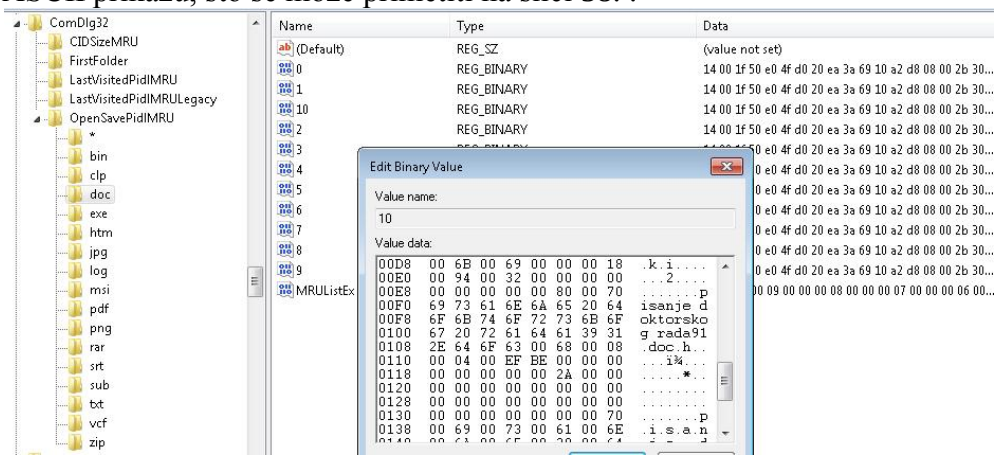
Slika 57. *Prikaz alata lnk.exe koji analizira LNK fajl*

U forenzičkom ispitivanju uvek je korisno pretražiti ove fajlove kako u alociranom tako i u nealociranom prostoru diska i page fajlu. Razlog jeste taj, što se ispitivanjem ovih lnk fajlova može obezbediti povezivanje fajla sa logičkim diskom na kojem je fajl smešten, a zatim na logički disk gde je smešten sam operativni sistem što može indicirati da je moguće korišćenje eksternog diska.

Treba naglasiti da Windows rescent folder može sadržati dragocene informacije za digitalnog forenzičara, jer se u njemu nalaze prečice do svih fajlova koji su najčešće bili korišćeni. U Windows 7 operativnom sistemu pristup Windows rescent folderu je preko : *"C:\Users\(User Name)\AppData\Roaming\Microsoft\Windows\Recent Items"*
Najčešće korišćene komande u "RUN" baru mogu se pronaći u Windows registru na sledećem mestu :
"*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU*
"

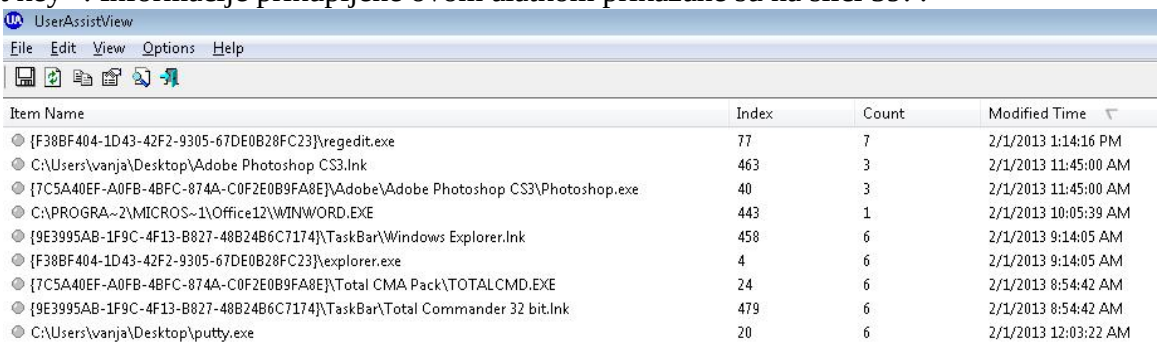
Ovde se mogu naći korisne informacije o tome koje je komande osumnjičeni koristio putem "RUN-a" (hronološki prikazanih u „DATA“ koloni „MRUList“ vrednosti). Međutim, na novijim operativim sistemima korisnici sve više koriste bar "Search and programs" koji se ovde ne registruju. Ukoliko forenzičar želi saznati koji su se to fajlovi otvarali i snimali pri pokretanju prozora (eng. open/save dialog) to može videti u registarskoj bazi pod sledećim ključem :
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU"

Treba napomenuti da su vrednosti koje sadrže podključevi u HEX zapisu, ali se mogu videti u ASCII prikazu, što se može primetiti na slici 58. :



Slika 58. *Prikaz otvaranih fajlova u Windows 7 iz Registarske baze*

Isto tako moguće je kroz registarsku bazu videti i poslednje otvarane foldere na sistemu :
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU"
U Registry bazi moguće je videti i poslednje otvarane dokumente (kao na primer .bin, .clp, .csv, .doc, .docx, .dotm, .htm, .jpg, .log, .pdf, .png, .rar, .srt, .sub, .txt, .vcf, . xls, .zip). Lokacija koju forenzičar treba da ispita jeste :
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs"
Interesantno mesto u Registry bazi takođe predstavlja i :
"HKEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" koji sadrži listu otvaranih izvršnih fajlova na sistemu. Ovi podaci mogu biti dragoceni, kako administratoru sistema da ispita bezbednost samih izvršnih fajlova, tako i forenzičaru koji dobija novi izvor podataka u rekonstruisanju zlonamernih aktivnosti. Ukoliko forenzičar želi da sazna detalje o izvršnim fajlovima (.exe) i linkovima koji su se često otvarali na operativnom sistemu, to je moguće uraditi altatkom UserAssistentView[336] koja vrši dešifrovanje zapisa koji se nalaze u Registry bazi pod ključem :
"HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist key" . Informacije prikupljene ovom alatkom prikazane su na slici 59. :



Slika 59. *Prikaz informacija dobijenih iz Registarske baze koje se odnose na ključ UserAssist*

Pretraživanje User Assist ključeva veoma je korisno u slučaju da na ispitivanom sistemu postoji više korisničkih naloga s obzirom da prefetch fajl ne može da identifikuje koji je korisnik startovao određenu aplikaciju. Takođe, sa UserAssist ključem digitalni forenzičar može doći do informacija koje ukazuju na određene tipove fajlova i programa kojima je pristupano. Iako ovi podaci nisu konačni (jer se ne mogu povezati za tačno određen datum i vreme) oni ipak mogu ukazati na specifične korisničke aktivnosti. User Assist podključevi su šifrovani ROT-13 algoritmom koji je izuzetno slab prema današnjim standardima [60]. U nastavku sledi tabela 7. [4] koja prikazuje listu istorije sa podključevima u Registarskoj bazi.

Tabela 7. Lista istorije na osnovu potključeva iz Registarske baze

Lista istorije prema tipu	Potključ koji ukazuje na listu istorije
URL-ovi iz Microsoft Internet Explorera	*HKEY_USERS\S-1-5-21-{User Identifier}\Software\Microsoft\Internet Explorer\TypedURLs*
Datoteke Microsoft Word-a	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft\Office\12.0\Word\File MRU*
Datoteke Microsoft Excell-a	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft \Office \12.0\Excel\File MRU*
Datoteke Microsoft Power Point-a	*HKEY_USERS\S-1-5-21-{User Identifier}\Software\Microsoft*

[336] Dostupno na http://www.nirsoft.net/utils/userassist_view.html

	\Office\12.0\PowerPoint\File MRU
Datoteke Acrobat Reader-a	*HKEY_USERS\S-1-5-21-{User Identifier} \Software\Adobe\Acrobat Reader\9.0\AVGeneral\cRecentFiles*
WinRAR datoteke	*HKEY_USERS\S-1-5-21-{User Identifier} \Software \WinRAR \ArcHistory*
Datoteke .GIF	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.gif*
Datoteke .JPG	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg*
Datoteke .TXT	*KEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt*
Datoteke .ZIP	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft \Windows\CurrentVersion\Explorer\RecentDocs\.zip*
Folderi	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder*
Najskorije korišćena mapirana mreža	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft \Windows\CurrentVersion\Explorer\Map Network Drive MRU*
Najskorije korišćen Wallpaper	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft \Windows\CurrentVersion\Explorer\Wallpaper\MRU*
Najskorije upotrebljena komanda u RUN dijalogu	*HKEY_USERS\S-1-5-21-{User Identifier}\Software \Microsoft \Windows \CurrentVersion\Explorer\RunMRU*

3.1.22 Postojani podaci od značaja na Windows-u - Fajlovi Internet aktivnosti

Veoma važan korak u digitalnoj forenzici računarskih sistema jeste ispitivanje Internet aktivnosti osumnjičenog za incidentnu odnosno protivpravnu aktivnost. Ove informacije mogu biti dragocene za forenzičko ispitivanje kršenja politike kompanije, korporativne špijunaže (insajderska trgovina), krađa intelektuelnog vlasništva i drugih krivičnih dela.

Ovi podaci forenzičaru mogu da pruže značajne informacije kada je u pitanju istraživanje tragova pristupa Internetu na ispitivanom računaru. Praksa je pokazala da kada je reč o visokotehnološkom kriminalu u većini slučajeva se koristi neki aspekt Interneta. Upravo zato digitalni forenzičar mora razumeti funkcionisanje Interneta i poznavati sva značajna mesta u operativnom sistemu u kojima se mogu pronaći incidentne/protivpravne aktivnosti.

Windows operativni sistem isporučuje svoj operativni sistem sa svojim Internet pretraživačem Internet explorerom IE.

IE ima svoje dve oblasti značajne za forenzičare gde skladišti svoje podatke. Prva oblast je index.dat fajl odnosno baza koju koristi IE pretraživač i keš IE-a. Index.dat fajlovi su struktuirani u MS IE cache File (MSIECF) formatu. Ovaj fajl sadrži zapise posećenih URL lokacija, uključujući upite, pristupe Web mail servisima i druge bitne podatke za digitalnu istragu. Relevantni tipovi iz strukture index.dat fajla koje će forenzičar identifikovati prilikom rekonstrucije Internet aktivnosti jesu sledeći :

- **Tip REDR** - Ovaj tip zapisa o aktivnostima na Internetu ukazuje da se radi o redirekciji, odnosno da je korisnički Internet pretraživač preusmeren na drugu Internet lokaciju.
- **Tip URL** - Ovaj tip zapisa o aktivnostima na Internetu čini skup podataka koji predstavljaju URL adresu ili WEB sajt koju je korisnik posetio.
- **Tip LEAK** - Ovaj tip zapisa o aktivnostima na Internetu takođe ukazuje na sajt koji je korisnik posetio.

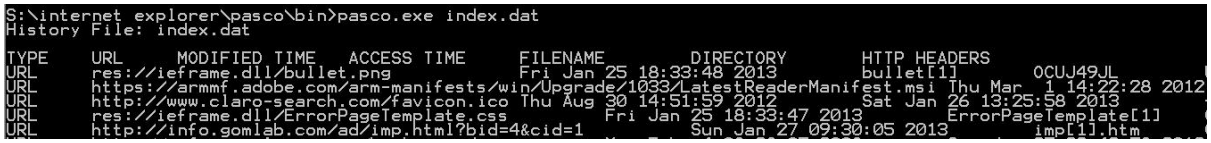
Na Windows XP i Windows 2003 sistemima lokacija koja je od forenzičkog značaja gde se nalazi index.dat fajl jeste :

"c:\Documents and Settings\Ime_Korisnika\Local Settings\Temorary Internet Files\Content.IE5"

Na Windows Visti i Windows 7 ta lokacija je :

"c:\Users\Ime_Korisnika\AppData\Local\Microsoft\Windows\Temorary Internet Files\Content.IE5"

Forenzičaru mogu biti od koristi različiti alati kada je reč o prikupljanju informacija iz index.dat fajla, a najpoznatiji alat za tu namenu je Pasco.exe[337] autora Keith J. Jones-a, koja može da radi i na obe platforme (i Windows i Linux) [94]. Izlaz iz ove komande prikazan je na slici 60. :



Slika 60. *Izlaz Pasco komande*

Takođe dobra alatka za prikupljanje podataka iz index.dat fajla je i alatka libmsiecf čiji je autor Joachim Metz, koja se sastoji iz dva programa, msiecfinfo i msiecfexport. Msiecinfo prikazuje osnovne podatke iz MSIECF fajla, dok msiecfexport prikazuje detaljnije podatke ovog fajla. Mana je ta, što je ova alatka dostupna samo za Linux sisteme.

Većina forenzički značajnih informacija o Internet aktivnostima može se pronaći i u specifičnim folderima koji pripadaju profilu (profilima) ispitivanog korisnika (Keš, Favoriti, Istorija, Kolačići). Oni su uglavnom locirani hijerarhijski ispod korisničkog imena unutar „Documents and Settings" kada je reč o sistemima Windows XP/2000/2003. Međutim zlonamerni korisnici mogu da promene podrazumevane lokacije ovih direktorijuma. Da bi forenzičar potvrdio stvarnu lokaciju ovih foldera potrebno ih je proveriti u ključevima Registra [38]:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Cache
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Cookies
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\History
- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Favorites

Dragocene podatke forenzičar može dobiti iz privremenih Internet fajlova, odnosno keš fajlova (eng. Internet cache) koji ostaju na računarskom sistemu nakon pristupa korisnika WEB lokacijama na Internetu. Pre nego što se korisniku prikaže stranica kojoj želi da pristupi, računar prethodno preuzima fajlove koji čine tu Web stranicu i smešta ih u Internet keš na disku, da bi nakon toga bila prikazana na ekranu korisnika. Ukoliko se kontaktira ponovo isti sajt kontaktira se keš fajl (neki Internet pretraživači vode evidenciju koliko je puta posećen određeni sajt kod IE se ti podaci nalaze u fajlu index.dat u u Netscape-u se nalazi u Netscape.hst, kod Mozilla se taj podatak nalazi u _CACHE_001_). Internet keš predstavlja oblast na hard disku (serija foldera) što znači da sistem sve te upise registruje. Internet keš je osmišljen sa namerom da ubrza vreme prikaza web stranice na ekranu, a sa druge strane obezbeđuje forenzičaru dodatan izvor informacija i dokaza. Naravno, korisnik može odrediti veličinu Internet keša na 0mb što zapravo znači da se informacije o posetama na Internetu ne keširaju, a mogu se i obrisati fajlovi koji ulaze u sastav keša. To takođe može biti i signal forenzičaru, da je namera zlonamernog korisnika na sistemu bila takva da želi prikriti svoje aktivnosti. Na Windows XP sistemima ovi fajlovi su na lokaciji :
"c:\Documents and Settings\Ime_Korisnika\Local Settings\Temorary Internet Files\Content.IE5"

[337] Dostupno na http://www.mcafee.com/hk/downloads/free-tools/pasco.aspx

Na Windows Visti i Windows 7 ta lokacija je :
"c:\Users\Ime_Korisnika\AppData\Local\Microsoft\Windows\Temorary Internet Files\Content.IE5"
Za forenzičara je važno da zna da se ovi keš fajlovi smeštaju u jedan od 4 proizvoljno kreirana poddirektorijuma. Informacije koje sadrže ovi folderi su keširani fajlovi kojima mogu da se potvrde aktivnisti na Internetu (na primer URL adrese i putanje do određenog fajla) uz korelaciju sa podacima dobijenim iz index.dat fajla.

Dodatne informacije od značaja za istragu se mogu takođe dobiti iz **Omiljenih lokacija** Internet pretraživača (eng. Favourites). Ove omiljene lokacije predstavljaju obeležene lokacije od značaja (eng. Bookmarks) i mogu biti pokazatelj kretanja korisnika na Internetu. Omiljene lokacije ne Windows XP nalaze se na :
"c:\Documents and Settings\Ime_Korisnika\Favorites"
Na Windows Visti i Windows 7 ta lokacija je :
"c:\Users\Ime_Korisnika\Favorites

Omiljene lokacije se pojavljuju nakon kreiranja korisničkog profila i njegovog logovanja na sistem. Ove lokacije predstavljaju skup URL prečica (eng. shortcut). Sadržaj URL prečice se mogu lako videti text editorom ili izlazom komande "type" na konzoli Windows sistema ili comande "cat" na Linux sistemima. Pored sadržaja URL, forenzičar može naći vrednosti kao što su, kada je fajl kreiran, modifikovan i kada mu je poslednji put bilo pristupano, što indicira koje je lokacije osumnjičeni posećivao kao i njihovo vreme. Ove informacije mogu biti dragocene prilikom forenzičke istrage. Ali treba napomenuti da ulaze u Omiljene lokacije unosi i sam sistem, a ne samo korisnik, što se mora uzeti u obzir. Zato je najvažnija informacija zapravo URL adresa lokacije na koju se prečica iz Omiljenih lokacija odnosi. Dodatan kontekst istrazi mogu pružiti informacije iz unetih URL adresa iz trake za pretrživanja (eng. Navigation toolbar). To je lista onih URL ulaza koje je korisnik napravio u prozoru pretraživača. Ova lista se čuva u registarskoj bazi u ključevima i lako ih je identifikovati. Lokacije koje forenzičar treba da ispita u Registry bazi su :
"HKCU\Software\Microsoft\InternetExplorer\TypedURLs"
"HKCU\Software\Microsoft\InternetExplorer\Download"

Treba napomenuti da korišćenje registarskog ključa TypedURLs zavisi od verzije Windows operativnog sistema i Internet explorera. Na primer, kod Internet explorera 6 u ključu će biti upisana vrednost, samo ukoliko je Interenet explorer ugašen na pravilan način (ukoliko je IE proces iexplore.exe ubijen iz Taks menadžera neće biti upisa u ključ). Kod Internet explorera 8 vrednost će se upisati u ključ u realnom vremenu nezavisno od toga na koji je način Internet explorer ugašen.

Kod Windows-a XP sa SP2 i SP3 i Windows Viste [28] podaci o unetim URL adresama se upisuju u ključ TypedURL, dok se kod Windows 7 ovi podaci ne upisuju.

Prethodno razmatranje odnosi se na Internet pretraživač Internet explorer koji dolazi zajedno sa instaliranim Windows operativnim sistemom. Brojni drugi pretraživači (Firefox, Opera, Chrome, Safari, Netscape) koji nisu predmet ovog rada, funkcionišu na vrlo sličan način ili poseduju sopstveni sistem skladištenja Internet fajlova.
Isto tako dodatan kontekst istrazi mogu pružiti i fajlovi koji se nazivaju **Kolačići** (eng. Cookies). Za digitalnog forenzičara oni predstavljaju izvor dodatnih informacija o Internet aktivnostima korisnika. Njihova karakteristika je da korisnik nema punu kontrolu nad njima. To su mali tekst fajlovi koji se skladište na hard disku i dolaze kao posledica Internet aktivnosti kroz posete WEB lokacijama. Njih je moguće otvoriti sa tekst editorom direktno ali određena polja su šifrovana. Šifrovana polja 5 i 6 odnose se na vremenski rok kolačića, a polja 7 i 8 predstavljaju vreme kreiranja kolačića.U Windows XP sistemima lokacija kolačića je :
"c:\Documents and Settings\Ime_Korisnika\Cookies"
Na Windows Visti i Windows 7 ta lokacija je :
"c:\Users\Ime_Korisnika\AppData\Roaming\Microsoft\Windows\Cookies"

Da bi se uspešno prikazala sva polja neophodno je korišćenje alata. Alat Galleta[338] , čiji je autor takođe Keith J. Jones (autor Pasco alata), daje odličan prikaz i izlaz ovog alata učitan u Microsof Excell fajl dat je na slici 61. :

Cookie File: PRSPC8UR.txt					
SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
a2a.lockerz.com/	ivc	1	Thu Jan 31 14:08:12 2013	Fri Feb 1 14:08:12 2013	2147484752
a2a.lockerz.com/	__utma	132044255.554491166.1359641293.1359641293.1359641293.1	Thu Jan 31 14:08:13 2013	Sat Jan 31 14:08:13 2015	2147484752
a2a.lockerz.com/	__utmb	132044255.2.10.1359641293	Thu Jan 31 14:08:13 2013	Thu Jan 31 14:38:13 2013	2147484752
a2a.lockerz.com/	__utmz	132044255.1359641293.1.1.utmcsr=ipmart-forum.com|utmccn=(referral)|utmcmd=referral|utmcct=/showthread.php	Thu Jan 31 14:08:13 2013	Fri Aug 2 02:08:13 2013	2147484752

Slika 61. *Prikaz izlaza alata Galleta nakon analize kolačića na Windows 7 OS*

Ova alatka dizajnirana je za proveru sadržaja *cookie* fajlova i izgrađena je za rad na više platformi (*Windows* (kroz *Cygwin), MacOSX, Linux, i*BSD*) [120].

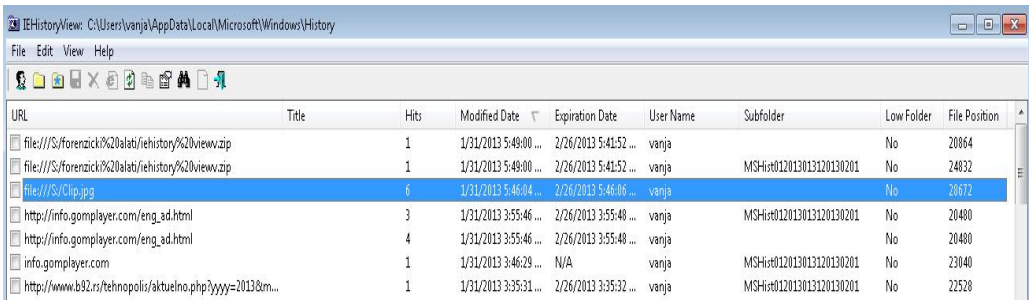
Istorija aktivnosti na Internetu (eng. Internet History), omogućuje evidentiranje lokacija koje je korisnik posetio sa svog operativnog sistema u toku Internet pretraživanja. Ispitivanjem Internet istorije moguće je obezbediti ključne dokaze u rešavanju slučaja. Istrage koje se odnose na nazakonito korišćenje ili nepropisno korščenje Interneta, zahtevaju stručnu analizu informacija sačuvanih od strane Internet pretraživača. Te informacije su rezultat Internet aktivnosti osumnjičenog. Na primer, istorija aktivnosti može uključivati imena posećenih Internet lokacija, FTP sajtova, novinskih grupa (eng. news group). Na osnovu istorije aktivnosti i prethodno opisanih bitnih WEB elemenata za ispitivanje, forenzičar može rekonstruisati aktivnosti osumnjičenog sa sledećih lokacija :

"c:\Documents and Settings\Ime_Korisnika\Local Settings\History" – odnosi se na Windows XP a na Windows Visti i Windows 7 ta lokacija je :

"*C:\Users\ Ime_Korisnika \AppData\Local\Microsoft\Windows\History "*

Sistem ovde pravi podelu istorije aktivnosti na dnevne i nedeljne. Moguće je pronaći, kako one aktivnosti koje se odnose na Internet aktivnosti, tako i one koje se odnose na pristup fajlovima samog računara (pristup lokalnim fajlovima na hard disku). Internet istorija ima opciju za korisnička podešavanja i difoltno vreme vođenja istorije je 20 dana. Onemogućavanje vođenja istorije forenzičaru može biti signal o prikrivanju potencijalnih dokaznih informacija.

Besplatna alataka IEHistoryView[339] čita sve podatke iz istorije datoteka na računaru i prikazuje listu svih URL adresa koje su posećene u poslednjih nekoliko dana u jako preglednom formatu. Na slici 62. dat je izlaz alatke IEHistoryView :



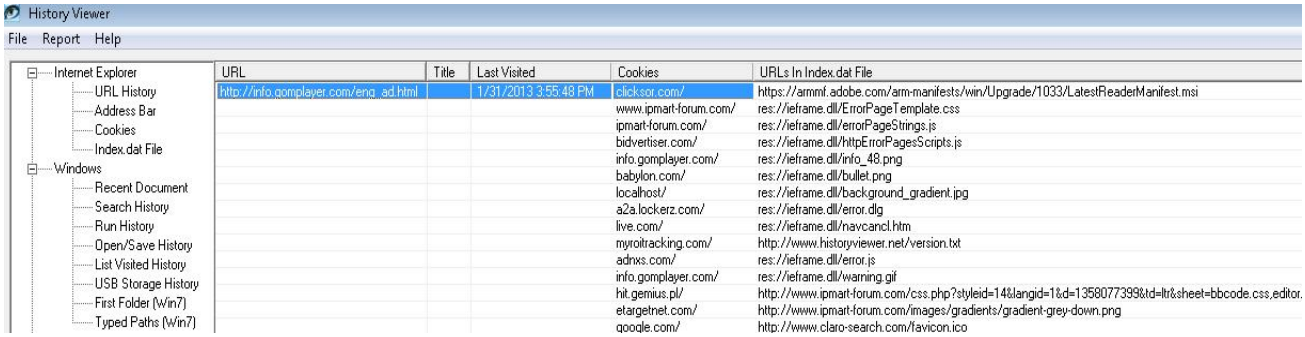
Slika 62. *Prikaz izlaza alatke IEHistoryView sa detaljima istorije Internet aktivnosti*

Druga alatka sa kojom je moguće dobiti informacije vezane ze istoriju Internet aktivnosti, ali podržava i druge Internet pretraživače i daje dodatne korisne istorijske informacije na ispitivanom sistemu jeste alatka History Viewer[340]. Njen izlaz dat je na slici 63. :

[338] Dostpuno na http://www.mcafee.com/us/downloads/free-tools/galleta.aspx

[339] Dostupna na http://www.nirsoft.net/utils/iehv.html

[340] Dostupno na http://www.historyviewer.net/download.htm, 12.02.2013



Slika 63. Prikaz izaz alatke History Viewer

Treba istaći da se postojani podaci na sistemu osim "uživo "mogu prikupiti i analizirati u post-mortem forenzici. Na osnovu iznetih informacija o postojanim podacima može se zaključiti da su za pronalaženje potencijalnih tragova, forenzički najznačajnija sledeća mesta na Windows sistemu :

- keš pretraživača
-metadata fajlovi (eksterni, interni i link fajlovi)
-log fajlovi (logovi događaja programa, bezbednosni logovi i sistemski logovi, logovi programa za komunikaciju)
-obrisani fajlovi
-Windows Registry baza (informacije o vremenskoj zoni, MRU lista, UserAssist, bežične mreže, USB uređaji, Internet explorer, Windows šifre, IM programi)

3.1.23 Postojani podaci od značaja na Windows-u - Fajlovi aktivnosti elektronske pošte

Fundamentalni nedostatak kod e-mail-a je taj, što se pojedina zaglavlja (eng. header) mogu falsifikovati. Upravo to je ono što omogućava napredovanje spam-ova i ostalih e-mail prevara i pored sofisticiranih filtera i programa za njihovo detektovanje [89].

Da bi forenzička istraga bila uspešna, forenzičar mora da razume način funkcionisanja elektronske pošte, pa će ono biti prikazano na ilustrativan način :

Elektronska poruka se kreira sa određenim e-mail klijentom (na primer Gmail, Outlook, Yahoo). E-mail klijent šalje kreiranu elektronsku poruku do MTA (eng. Mail transfer agent) odnosno do e-mail servera na kome je pokrenut servis SMTP (eng. Simple mail transfer protocol). MTA pronalazi odgovarajući mail server za primaoca elektronske poruke i prenosi je. Kroz svaki MTA koji elektronska poruka prođe, pridoda joj se vremenski pečat. Upravo su ovi vremenski pečati od izuzetne važnosti u forenzičkoj istrazi. Primer :

„ *Apr 21 06:16:27 turing sendmail{29573}: r3L4GOmb029573:*
from=<yqxadathqk@assupport.eu>, size=1059, class=0, nrcpts=1,
msgid=<001001ce3e46$e4b39410$94bb4ebd@systemro7vpq>, proto=SMTP,
daemon=MTA, relay=triband-del-59.177.175.107.bol.net.in {59.177.175.107} “

U poslednjem koraku, primalac kontaktira svoj e-mail server koristeći određeni protokol za pristup elektronskoj pošti na serveru (na primer POP3, IMAP) i preuzima elektronske poruke svojim e-mail klijentom.

Na osnovu forenzičke analize aktivnosti elektronske pošte, forenzičar treba da dobije odgovore na pitanja : ko je poslao e-mail, kada je e-mail poslat i odakle je poslat. Važno je istaći da se e-mail dokazi obavezno pregledaju na računaru koji nije povezan sa Internetom, odnosno namenjenom za off-line ispitivanje. Razlog jeste taj, što ukoliko je podešena potvrda o pročitanom e-mailu, nakon pregledanja e-maila poslaće se pošiljaocu informacija da je e-

mail pročitan, što može ugroziti istragu (u slučaju da je računar na kome se vrši ispitivanje povezan sa Internetom).

Na osnovu podataka koji se dobijaju forenzičkim ispitivanjem fajlova elektronske pošte moguće je da se locira računar sa kog je mailiciozni korisnik izvršio incidentnu odnosno protivpravnu aktivnost. Svaki e-mail ima tzv. zaglavlje u kome se opisuje trasa poruke [195]. Zaglavlje elektronske pošte (eng. e-mail header) može sadržati veoma važne informacije, kao što su jedinstveni identifikacioni brojevi (eng unique ID), IP adrese servera sa kog je slata elektronska pošta, kao i vreme slanja. Pregledanje zaglavlja elektronske pošte može biti izvedeno iz grafičkog e-mail klijenta, klijenata komandnog okruženja ili iz Webmail klijenata. Istraživanje elektronskih poruka može da se bazira na pristupu ispitivanom (kompromitovanom) računaru uz prikupljanje dokaza i/ili pristupu logovima e-mail servera. Upotrebom e-mail klijenta sa ispitivanog računara moguće je pronaći i iskopirati dokaze iz elektronske poruke. Takođe mogu se pronaći zaštićena i šifrovana dokumenta. Sve e-mailove koji sadrže potencijalne dokaze treba odštampati. Ukoliko se može doći i do logova sa e-mail servera pre nego što se oni izmene moguće je ispratiti tačna vremena i datume ispitivane elektronske pošte [198].

Način prikupljanje zaglavlja iz grafičkih e-mail klijenata :

- **Microsoft Outlook** - Otvoriti ispitivanu poruku, odabrati opciju "Message Options", selektovati sve i iskopirati heder u određeni tekstualni editor.
- **MS-Outlook Express** - Otvoriti ispitivanu poruku, odabrati opciju " message properties ", odabrati "Message Source", iskopirati heder u određeni tekstualni editor.
- **Web orijentisani servisi** za poštu (eng. Webmail) tipa Yahoo[341], snimaju IP adrese sistema (u zaglavlje poruke) sa kojih je sastavljana elektronska pošta. U daljem tekstu daje se prikaz načina prikupljanja e-mail zaglavlja (eng. header) u forenzičkoj praksi iz najkorišćenijih Webmail klijenata:
- **prikaz i kopiranje e-mail hedera u Gmail**-u[342] - Ulogovati se u Gmail, otvoriti ispitivanu poruku, odabrati opciju "MORE", odabrati opciju "SHOW ORIGINAL", selektovati ceo heder, kopirati i snimiti sve u određeni fajl.
- **prikaz i kopiranje e-mail zaglavlje u AOL**-u[343] - Ulogovati se u AOL, otvoriti ispitivanu poruku odabrati link "DETAILS", selektovati ceo heder, kopirati i snimiti sve u određeni fajl.
- p**rikaz i kopiranje e-mail hedera u Yahoo mail**-u[344] - Ulogovati se u Yahoo mail, otvoriti ispitivanu poruku, odabrati "FULL HEADER", selektovati ceo heder, kopirati i snimiti sve u određeni fajl.
- p**rikaz i kopiranje e-mail hedera u Hotmail**-u[345] - Ulogovati se u Hotmail, kliknuti desnim klikom na ispitivanu poruku, odabrati "VIEW MESSAGE SOURCE", selektovati ceo heder, kopirati i snimiti sve u određeni fajl.

Kada je reč o telu poruke (eng. Message Body), ono sadrži isključivo podatke koje je pisao pošiljalac (u smislu nema dodatih podataka od strane servera kao kod zaglavlja poruke). Treba napomenuti da, iako je telo poruke u tekstualnom obliku, e-mail klijenti ili serveri njih mogu sačuvati u binarnom formatu. Zato je jako važno da se koriste specijalizovani alati za forenzičku analizu elektronske pošte koji mogu da procesiraju različite formate fajlova i baza u kojima se smeštaju elektronske poruke.

U nastavku će biti prikazane određene karakteristike najkorišćenijih emal klijenata (Microsoft Outlook, Microsoft Outlook Express, Windows mail, Mozilla thunderbird i webmail) koji su od važnosti za forenzičku istragu.

[341] Dostupno na http://www.yahoo.com/
[342] www.gmail.com
[343] www.aol.com/
[344] www.yahoo.com
[345] www.hotmail.com/

Microsoft Outlook - ovaj klijent smešta elektronsku poštu u fajl sa .PST ekstenzijom. Arhiva elektronske pošte se nalazi na sledećim lokacijama :
Kod Windows XP i ranijih operativnih sistema u folderu :
<korisničko_ime>\Local Settings\Application Data\Microsoft\Outlook
Kod Windows Vista i kasnijih operativnih sistema :
<korisničko_ime>\AppData\Local\Microsoft\Outlook
Registarski ključevi koji ukazuju koje su arhive korišćene smešteni su u :
„HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook“
Veličina arhive može biti do 20 GB.

Microsoft Outlook Express - ovaj klijent smešta elektronsku poštu u fajl sa .DBX ekstenzijom (folder.dbx je indeksni fajl)
Pre Windows Viste ovaj klijent dolazio je instaliran sa operativnim sistemom.
Arhiva elektronske pošte se nalazi na sledećim lokacijama :
<korisničko_ime>\Local Settings\Application Data\Identities\<GUID>\Microsoft\Outlook Express
Forenzički značajan je fajl cleanup.log koji govori o vremenu poslednjeg pakovanja. Obrisane poruke su označene sa „deleted“. Takođe moguće je pronaći obrisane .DBX fajlove u nealociranom prostoru.

Windows Mail - ovaj klijent smešta elektronsku poštu u fajl sa .EML ekstenzijom (.FOL predstavlja indeksni fajl). Dolazi instaliran sa Windows Vista OS. Arhiva elektronske pošte se nalazi na sledećim lokacijama :
<korisničko_ime>\AppData\Local\Microsoft\Windows Mail
Obrisana elektronska pošta smešta se u “Deleted Items” folder u „locale store“, postoje kao individualni .EML fajlovi i ne brišu se po difoltu.

Mozilla Thunderbird - ovaj klijent smešta elektronsku poštu u fajl INBOX nema ekstenzije (.msf predstavlja indeksni fajl). Arhiva elektronske pošte se nalazi na sledećim lokacijama :
Kod Windows XP:
C:\Documents andSettings\{Korisničko Ime}\ApplicationData\Thunderbird\ Profiles\<random 8 karaktera>.default\Mail\Local Folders
Kod Windows Vista i Windows 7 operativnih sistema :
C:\users\{Korisničko Ime}\Application Data\Thunderbird\Profiles\<random8 karaktera>.default\Mail\ Local Folders
Ukoliko je portable verzija, nalazi se pod
„ \Data\Profile\mail\ime_servera”
Proces pakovanja (eng. compaction) se sprovodi ručno (auto proces je onemogućen po difoltu). Folderi imaju limit od 4GB

Webmail - Elektronska pošta je uobičajeno smeštena na serveru provajdera (eng. ISP – Internet Service provider), osim ukoliko klijent koristi POP3 ili IMAP protokol za pristup pošti što forenzičaru može biti od koristi čime se znatno može ubrzati proces istrage. Korisničke IP adrese i informacije o pretplatniku (na primer ADSL pretplatnik ili pretplatnik kablovskog Interneta). Značajno je istaći da je moguće oporaviti keširane fajlove.

Posle prikupljenih header i body informacija iz e-mail poruka sledi njihovo ispitivanje i praćenje tragova kao što su : povratne putanje, e-mail adrese primaoca, tip servisa za slanje elektronske pošte, ime servera elektronske pošte, jedinstveni identifikacioni broj elektronske pošte, datum i vreme slanja elektronske pošte, informacije o prikačenim fajlovima (eng. attachment) pretraživanje tela poruke prema određenom stringu i druge korisne informacije

od značaja za istragu. Potrebno je utvrditi, da li su poruke sačuvane na lokalnom računaru ili su ostavljene na serveru. Računari koji predstavljaju e-mail servere, smeštaju elektronsku poštu na dva načina ili u fajl ili u bazu podataka. Forenzički značajni fajlovi su .pst i .ost (Microsoft Outlook) fajlovi koji mogu sadržati sačuvane elektronske poruke, kalendarska dešavanja kao i raspored obaveza. Pst fajlovi koriste se pri upotrebi POP3, IMAP i web orijentisanih e-mail naloga[346]. OST fajlovi se, zapravo, koriste ukoliko se upotrebljava Exchange nalog u offline režimu i predstavljaju kopije objekata sa servera. Kada su u pitanju web orijentiasni fajlovi elektronske pošte, tu pre svega forenzičar treba da istraži fajlove i fodere koji se odnose na history, kolačiće, keš, i privremene fajlove (eng. Temp files). Kada se forenzička istraga odnosi na ispitivanje elektronske pošte, dodatno će se koristiti i mrežni logovi da bi se potvrdila e-mail ruta. Na primer, konsultovani će biti logovi sa rutera, logovi dolaznog i odlaznog saobraćaja na e-mail serveru, fajervol logovi.
Najupotrebljavaniji forenzički alati koji se koriste prilikom forenzičkog ispitivanja elektronske pošte su : AccessData's FTK[347], EnCase Forensic[348], Paraben E-mail Examiner [349], FINALeMAIL[350], DBXtract[351], Fookes MailBag Assistant[352][1]. Kada je reč o sudskoj praksi u Srbiji e-mail kao dokazno sredstvo korišćeno je naročito kada je u pitanju bila krađa Internet vremena i Internet piraterije. U slučajevima Internet piraterije sva komunikacija (slanje kataloga i naručivanje diskova) išla je preko mejlova i oni su korišćeni u dokaznom postupku [154].

3.2 Forenzički odgovor na protivpravnu / incidentnu aktivnost "uživo" na Linux platformi

Linux je besplatan UNIX orijentisan operativni sistem otvorenog koda (eng. open source) izvorno kreiran od strane Linus Torvaldsa uz pomoć programera iz celog sveta. Postoje različite verzije Linuxa koje se nazivaju distribucije i najprisutnije su Red Hat, Centos, Fedora, Debian, Suse, Ubuntu, Kubuntu, Slackware. Svaka od njih ima svoje prednosti i mane. Ove distribucije se međusobno razlikuju i prema tipovima. Postoje serverske, desktop i live distribucije. Serverske distribucije primarno su orijentisane biznis okruženju, mada mogu da se konfigurišu i da budu odgovarajući i za kućnu upotrebu. Desktop distribucije su pogodne više za kućnu upotrebu, podrazumevaju grafičko okruženje i veliki broj aplikacija. Live distribucije podrazumevaju butabilne verzije operativih sistema koje se učitavaju direktno u RAM memoriju i rade nezavisno od postojećeg računarskog operativnog sistema. Ono što forenzičar mora da zna jeste način na koji Linux podiže svoj operativni sistem (eng Linux boot sequince). Boot sekvenca otpočinje učitavanjem kernela. Uobičajeno slika kernela (eng. kernel image) se nalazi po difoltu u /boot direktorijumu. Takođe, link ka slici kernela se nalazi u /boot direktorijumu i referencira se iz konfiguracionog fajla Linux loadera LILO (/etc/lilo) ili GRUB (/etc/grub.conf). Poslednji korak jeste inicijalizacija. Fajlovi koji kontrolišu inicijalizaciju nalaze se u fajlu /etc/inittab. Fajl odgovoran za započinjanje procesa jeste /sbin/init. Tada se inicijalizuje runlevel i startup

[346] http://office.microsoft.com/en-001/outlook-help/introduction-to-outlook-data-files-pst-and-ost-HA010354876.aspx
[347] http://www.accessdata.com/products/digital-forensics/ftk
[348] http://www.guidancesoftware.com/encase-forensic.htm
[349] http://www.paraben.com/email-examiner.html
[350] http://www.finaldata.com/Products/?s=PRD&c=6&n=21
[351] http://www.oehelp.com/dbxtract/
[352] http://www.fookes.com/mailbag/

skripte kontrolisane od strane terminalskog procesa. Kada je reč o Linux fajl sistemu, potrebno je istaći da Linux tretira sve uređaje kao fajlove i njih smešta u folder /dev. Za forenzičara je bitno da zna, da većina Linux distribucija ima organizovane fajlove sa sličnom strukturom direktorijuma (tabela 8.) :

Tabela 8. Linux struktura direktorijuma

/bin	Zajedničke izvršne komande na nivou sistema
/boot	Potrebni fajlovi prilikom podizanja sistema uključujući slike kernela zajedno sa linkovima koji na njih upućuju definisanih u LILO ili GRUB
/usr	Lokalni programi, biblioteke, igre
/var	Logovi i drugi promenljivi fajlovi
/dev	Interfejs fajlovi koji omogućavaju jezgru komunikaciju sa hardverom i fajl sistemom
/home	Direktorijumi svih korisnika na sistemu sa ličnim korisničkim i konfiguracionim fajlovima
/mnt	Priključna tačka za spoljašnje, udaljene i i Mount points for external, remote, i prenosive fajl sisteme
/etc	Konfiguracioni fajlovi i skripte za administraciju
/root	Direktorijum root korisnika
/sbin	Administrativne izvršne komande koje treba da budu dostupne samo root-u odnosno administratoru
/lib	Osnovne sistemske biblioteke
/opt	Opcioni i drugi programi

Osnovne komande koje forenzičaru mogu pomoći za dobijanje osnovnih informacija o ispitivanom sistemu su sledeće :

#uname - a - pokazuje ime računara i verziju Linuxa
#ls - prikazuje spisak fajlova
#ls -l - pokazuje spisak fajlova sa njihovim dozvolama
#ls -ul ime_fajla - daje vreme pristupa fajlu
#cp - kopira fajlove
#mv - premešta fajlove
#chmod - izmena dozvola nad fajlovima
#ps - prikazuje pokrenute procese
#netstat -s - prikazuje informacije o protokolima
#ifconfig - prikazuje informacije o mrežnim uređajima na sistemu
#find - pretraživanje informacija na sistemu
#grep - pretraživanje fajlova ili pretraživanje sa ključnim rečima
#less - izlistava sadržaj fajla
#more - izlistava sadržaj fajla
#cat - izslistava sadržaj fajla takođe,
#diff - daje poređenje dva fajla
#df - daje prikaz mount- ovanih fajl sistema

Na Linuxu, da bi neki fajl sistem mogao da se koristi, mora biti montiran - dodeljen (eng. mount) sistemu. Svi fajl sistemi na particijama koje su definisane tokom instalacije Linux operativnog sistema će biti automatski montirane prilikom svakog podizanja sistema. Forenzičar mora da zna, da podaci mogu biti upisani na uređaj (eng. device) iako sam uređaj nije montiran. Periferne uređaje za skladištenje podataka, uređaj prepoznaje kao SCSI uređaje.

Ukoliko se koristi IDE disk na primarnom kontroleru kao master, sistem će ga nazvati "hda", ukoliko je priključen kao slave nazvaće se "hdb", dok će na sekundarnom kontroleru oni biti "hdc" i "hdd". Da bi se videla kompletna lista raspoloživih particija na sistemu koristi se komanda :

#fdisk -l /dev/hda

Svaka particija ima svoje dodeljeno Linux ime. Oznaka "*" označava da se radi o boota-bilnoj particiji. Izlaz fdisk komande uključuje i informacije o početnom i poslednjem cilindru svake particije, kao i broj blokova koji sadrže, ID particije i tip fajl sistema.

Forenzičar tokom istrage mora voditi računa o tome, da sledi sledeće mere predostražnosti kao što su :

- izbegavati pokretanje programa na kompromitovanom računarskom sistemu;
- ne pokretati programe koji mogu izmeniti metadata podatke o fajlovima i direktorijumima;
- dokumentovati sve preduzete aktivnosti i rezultate tokom istrage;
- izračunati heš vrednosti podataka da bi se obezbedio integritet nad podacima.

Kao što je već bilo opisano u prethodnom poglavlju, očuvanje podataka na "živom" sistemu često je potrebno da se blagovremeno utvrdilo da li postoji određena incidentna/protivpravna aktivnost (indikatori će biti opisani u poglavlju 3.5.2). Na primer, maliciozni program može ugroziti, kako bezbednost samog sistema, tako i sistema sa kojima je povezan. Odgovor "uživo" na incidentnu/protivpravnu aktivnost na Linux platformi uz svoje specifičnosti vrlo je sličan kao i odgovor "uživo" opisan u prethodnom poglavlju (koje se odnosi na Windows platformu). S obzirom da je značaj prikupljanja podataka, kako onih postojanih, tako i onih sa privremenim karakterom, već opisivan u prethodnom poglavlju u daljem tekstu će biti opisivani alati koji se odnose na njihovo prikupljanje na Linux platformi. Baš kao i kod forenzičkog ispitavanja Windows sistema, za forenzičara je neophodno da ima svoj "komplet" alata za prikupljanje privremenih podataka (eng. volatile data) sa komporomitovanog sistema. Razlog je taj, što određene komande na kompromitovanom sistemu mogu biti takođe ugrožene, pa se ne mogu smatrati pouzdanim i interakcija sa ispitivanim sistemom svodi se na minimum. Korišćenjem sopstvenih alata moguće je otkriti dragocene podatke koji su skriveni određenim malicioznim programom (na primer, rootkit-om). Naravno, u nekim slučajevima kada se radi rootkitu koji se učitava kao modul u kernel (eng. Loadable Kernel Module - LKM), ovi alati neće dati očekivane rezultate pa će biti potrebno uraditi forenzičko ispitivanje memorije i fajl sistema. Ovo poglavlje će pružiti opštu metodologiju za očuvanje privremenih podataka na Linux platformi na forenzički ispravan način, koristeći određene primere iz prakse i ukazujući na prednosti i nedostatke tako prikupljenih podataka kao i njihov uticaj na bezbednost sistema.

Linux ima jednu dobru alatku koja može snimati pokrenute komandne i njihove izlaze čime se lako dokumentuje ono što se radilo na živom sistemu. Alatka se zove "Script" i ona kešira podatke u memoriji i upisuje sve informacije prilikom njenog prekida u fajl typescript. Ukoliko se želi snimanje posle svake komande, onda se alataka **script** upotrebljava sa svičom "-f" :

#script ili #script -f

Baš kao što je bilo prikazano u poglavlju koje se tiče prikupljanja podataka sa Windows platforme može se pokrenuti netcat odnosno cryptcat komanda[353]. Pre pokretanja bilo kojih komandi na ispitivanom Linux sistemu iz pouzdanog komandnog okruženja (eng. command shell[354]), pokreće se alatka **script** (prethodno iskompajlirana u proverenom

[353] Ukoliko se želi obezbediti slanje podataka sa ispitivanog računara na forenzičku radnu stanicu, može se koristiti Netcat sa enkripcijom koji se zove cryptcat. Cryptcat koristi poboljšanu verziju Twofish blokšifarsku enkripciju sa simetričnim ključem. Više o ovoj enkripciji može se videti na Schneier sajtu : http://www.schneier.com/twofish.html

[354] Šel eng. shell predstavlja interfejs između jezgra operativnog sistema i korisnika. Ima veliki broj funkcijia od kojih se ističu interpretacija komandne linije, pokretanje programa, ulazno izlazna redirekcija, međusobno povezivanje komandi (eng. pipe) i shell programiranje. Najpoznatiji shell komandni interpreteri su Bourne shell (sh), C shell (csh), Bourne-again shell (bash), Korn shell (ksh).

okruženju). Na forenzičkom sistemu (koji može biti i Linux i Windows radna stanica) pokrenuti :
#netcat -v -l -p 9898 > izlaz_komandi_sa_kompromitovanog_racunara.txt

Podaci koji se šalju preko porta 9898 na forenzičku stanicu će biti sačuvani u fajlu izlaz_komandi_sa_kompromitovanog_racunara.txt. Na ispitivanom računaru (Linux) će se pokretati komande sa kojima će se prikupljati podaci od značaja za forenzičku istragu a njihovi izlazi slaće se na forenzičku radnu stanicu preko porta 9898 :
#/mnt/cdrom/komanda | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898

Sa komandom CTRL-C prekida se netcat sesija. Sledeće što treba uraditi je da se nad dobijenim podacima generiše heš vrednost MD5, SHA-1 ili SHA-256. Isto tako, iskopirati i dobijeni typescript fajl i nad njim izvršiti generisanje heš vrednosti.

U daljem tekstu biće prikazano kako se prikupljaju podaci privremenog karaktera, kao i oni podaci koji su postojani na sistemu, a koji su od izuzetnog značaja za forenzičku istragu. Da bi se dobili odgovori na pitanja "ko, šta, gde, kada" i kako se desila incidentna/protivpravna aktivnost, potrebno će biti prikupiti sledeće podatke :
Podaci sa privremenim karakterom
a. Sistemsko vreme i datum;
b. Postojeće mrežne konekcije;
c. Ovoreni TCP i UDP portovi;
d. Izvršni fajlovi koji otvaraju TCP i UDP portove;
e. Pokrenuti procesi;
f. Otvoreni fajlovi;
g. Interna tabela rutiranja;
h. Učitani moduli u kernel LKM;
i. Pridruženi fajl sistemi (eng. mounted file systems).

Postojani podaci od značaja :
a. Verzija operativnog sistema i nivo ažuriranosti paketa;
b. Vremenski pečati fajlsistema;
c. MD5 checksum fajl sistema;
d. Ulogovani korisnici na sistem;
e. Istorija logovanja na Linux sistem;
f. Logovi na sistemu;
g. TCP Wrappers;
h. Korisnički nalozi;
i. Korisnički fajl sa istorijom izvršenih komandi;
j. Sumnjivi fajlovi.

3.2.1 Podaci od značaja privremenog karaktera na Linux-u - Sistemsko vreme i datum

Sistemsko vreme i datum se dobija upotrebom komande koja označava i početak forenzičkog prikupljanja vremena:
#date
a izlaz ove komande je : **Sun Feb 3 13:54:31 CET 2013**
Upotrebom forenzičke netcat komande to se radi na sledeći način :
#netcat -v -l -p 9898 > datum_kompromitovanog_racunara
#/mnt/cdrom/date -u | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum datum_kompromitovanog_racunara > datum_kompromitovanog_racunara.md5

Takođe, prilikom završetka forenzičkog prikupljanja, preporuka je da se markira i vreme završetka prikupljanja podataka sa kompromitovanog računara.
#netcat -v -l -p 9898 > vreme_kraj_kompromitovanog_racunara
#/mnt/cdrom/date -u | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum vreme_kraj_kompromitovanog_racunara > vreme_kraj_kompromitovanog_racunara.md5

3.2.2 Podaci od značaja privremenog karaktera na Linux-u - Postojeće mrežne konekcije

Ovi podaci su važan pokazatelj aktivnosti na ispitivanom sistemu. Na osnovu ovih dobijenih podatka forenzičar može utvrditi da li je zlonamerni korisnik još uvek priključen na sistem, koji port koristi. Takođe, moguće je ustanoviti i inicijalnu tačku upada, odnosno omogućene (eng. enable) ranjive servise na sistemu koji su mogli biti kompromitovani, a time bi se omogućio upad u sitem. Komanda koja može da izlista postojeće mrežne konekcije jeste netstat komanda i prikazana je na slici 64. :
#netstat -na

```
root@ubunt1104srvx86:~# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
```

Slika 64. *Prikaz izlaza komande netstat -an*

3.2.3 Podaci od značaja privremenog karaktera na Linux-u - Otvoreni TCP i UDP portovi

Forenzičko ispitivanje otvorenih portova (TCP i UDP[355]) na sistemu je fokusirano na detektovanje ranjivih portova ili zadnjih vrata (eng. backdoor) uspostavljenih na sistemu koji omogućuju realizovanje incidentne/protivpravne aktivnosti. Komanda koja omogućava prikaz kako portova IP adresa, tako i procesa i njegovog ID-a koji je odgovoran za otvaranje određenog porta, jeste (slika 65.):
#netstat -plant

```
root@ubunt1104srvx86:~# netstat -plant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:993             0.0.0.0:*               LISTEN
619/dovecot
tcp        0      0 0.0.0.0:995             0.0.0.0:*               LISTEN
619/dovecot
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
733/mysqld
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
619/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
619/dovecot
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
1185/apache2
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
941/vsftpd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
892/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
743/cupsd
```

Slika 65. *Prikaz izlaza komande netstat -plant*

[355] Može se očekivati da se na sistemu pored TCP i UDP portova pojavi i RAW port i treba znati da se on odnosi na Linux kernel.

Forenzičar pomoću netcat-a može prikupiti na živom sistemu ove informacije na sledeći način :
#netcat -v -l -p 9898 > open_port_TCP_UDP_kompromitovanog_racunara

#/mnt/cdrom/netstat -plant | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum open_port_TCP_UDP_kompromitovanog_racunara > open_port_TCP_UDP _kompromitovanog_racunara.sh256

Najbolji način zaštite od otvorenih portova (jer nose potencijalne rizike upada u sistem) jeste da se otvore samo oni portovi koji su potrebni za pravilno funkcionisanje sistema. Takođe, servise koji rade na tim nepotrebnim portovima treba izbaciti iz sistema, čime se povećava bezbednost samog sistema.

3.2.4 Podaci od značaja privremenog karaktera na Linux-u - Izvršni fajlovi koji otvaraju TCP i UDP portove

U Windows okruženju prikazana je alatka fport.exe koja je linkovala otvoreni port sa startovanim procesom. Pod Linux-om to se može uraditi sa alatom koji se zove lsof[356] (eng. List Open Files) koja daje listu aktivnih procesa. Karakteristika ove alatke je ta, što ne samo da daje prikaz procesa koji otvara određeni port, već daje i prikaz fajlova koji pokreću određeni proces. U slučaju da je zlonamerni napadač kompromitovao sistem i preneo određene maliciozne fajlove, on će te fajlove pokušati da sakrije od sistema markirajući ih kao skrivene. Sledeće što će uraditi, jeste kreiranje procesa koji će nakon otvaranja fajla raskinuti vezu sa fajlom tzv unlink, a proces će nastaviti da radi zlonamerne aktivnosti. Programi tipa "ls" neće prikazati ove informacije o fajlu i procesu, jer su sakriveni od administratora. Dakle, veoma je važno da forenzičar ili administrator, poznaju ograničenja programa koje upotrebljavaju. Lsof je program koji će pružiti detaljne informacije o fajlovima uključujući i fajlove sa raskinutim vezama. Ono što treba istaći je da poznavanje dostupnih alata i odabir onog pravog, jeste od ključne važnosti, kako za forenzičko ispitivanje, tako i za ustpostavljanje bezbednog sistema.

Može se koristiti kao :
#lsof -n , gde se daje detaljan prikaz o fajlovima, procesima i portovima na sistemu ali možemo pretragu suziti na one procese koji se odnose na TCP i UDP Internet socket-e prikazanoj na slici 66. sa komandom "#lsof -i"

```
root@ubunt1104srvx86:~# lsof -i
COMMAND    PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
avahi-dae  385    avahi   13u  IPv4   6655      0t0  UDP *:mdns
avahi-dae  385    avahi   14u  IPv6   6656      0t0  UDP *:mdns
avahi-dae  385    avahi   15u  IPv4   6657      0t0  UDP *:44263
avahi-dae  385    avahi   16u  IPv6   6658      0t0  UDP *:38650
smbd       476     root   24u  IPv6   7615      0t0  TCP *:microsoft-ds (LISTEN)
smbd       476     root   25u  IPv6   7617      0t0  TCP *:netbios-ssn (LISTEN)
dovecot    592     root    6u  IPv4   7673      0t0  TCP *:imap2 (LISTEN)
dovecot    592     root    7u  IPv4   7674      0t0  TCP *:imaps (LISTEN)
dovecot    592     root    8u  IPv4   7675      0t0  TCP *:pop3 (LISTEN)
dovecot    592     root    9u  IPv4   7676      0t0  TCP *:pop3s (LISTEN)
mysqld     703    mysql   10u  IPv4   7979      0t0  TCP localhost:mysql (LISTEN)
cupsd      741     root    5u  IPv6   7943      0t0  TCP ip6-localhost:ipp (LISTEN)
cupsd      741     root    6u  IPv4   7944      0t0  TCP localhost:ipp (LISTEN)
```

Slika 66. *Prikaz izlaza komande lsof -i*

Upotreba ove komande na forenzički ispravan način kojim se mogu prikupiti sve informacije o svim procesima na sistemu, otvorenim portovima i fajlovima jeste sledeći :

[356] Dostupno na Purdue Univerzitetu : http://ftp.cerias.purdue.edu/pub/tools/unix/sysutils/lsof/

#netcat -v -l -p 9898 > lsof_kompromitovanog_racunara

#/mnt/cdrom/**lsof -n -P -l** | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum lsof_kompromitovanog_racunara > lsof_kompromitovanog_racunara.sh256

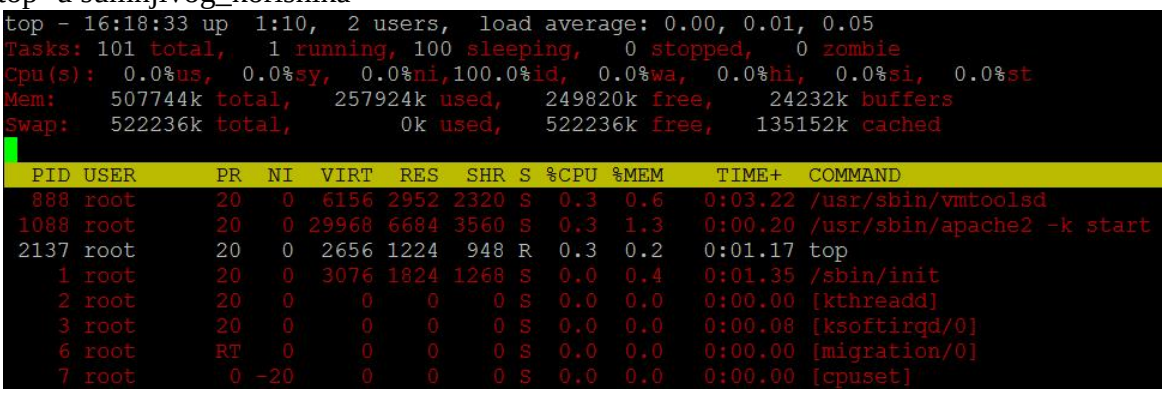
Treba napomenuti da, podatke dobijene pomoću netstat i lsof komandi treba međusobno uporediti, jer upravo u njihovim razlikama forenzičar može pronaći skrivene procese od strane kernela sa LKM-om. Ovaj rad neće ulaziti u analizu LKM-a jer to spada u posebnu oblast koja može biti predmet posebnih radova. Blagovremenim uočavanjem sumnjivih portova od strane digitalnog forenzičara dobiće se dodatni podaci o incidentnoj/protivpravnoj aktivnosti, a uočavanjem od strane administratora moguće će biti sprečiti nanošenje dodatne štete na sistemu.

3.2.5 Podaci od značaja privremenog karaktera na Linux-u - Pokrenuti procesi i servisi

Da bi sistem bio bezbedan mora se znati koji su procesi i servisi pokrenuti na njemu. Pokrenute procese možemo u Linux-u videti na nekoliko načina. Jedan je korišćenjem komande "Ps":
#ps -auxwww , koja lista sve procese na sistemu sa pripadajućim korisnicima koji su ga startovali.

INETD je proces koji upravlja standardnim Internet servisima na sistemu. Startuje se kada se sistem podiže i koristi konfiguracioni fajl u kome je definisano koje servise treba da omogući. Glavni konfiguracini fajl inetd koristi /etc/inetd.conf (mesto i ime zavise od tipa Linux distribucije). Za bezbednost sistema je važno da se razume na koji način inetd radi i koje informacije on sadrži u konfiguracionom fajlu [43].
Drugi način je pokretanje komande "top" :
#top

Program top će generisati ceo ekran sa spiskom postojećih procesa koji se stalno ažuriraju prema stepenu iskorišćenja CPU-a. Na vrhu ovog spiska nalaze se podaci o vremenu koliko je operativni sistem bio podignut, broj pokrenutih procesa na sistemu, statistika o raspoloživoj memoriji i swap prostoru. Prikaz se može formatirati na različite načine sa tasterom "SHIFT+o" tako da se procesi mogu sortirati prema zauzeću CPU (SHIFT+p), memorije (SHIFT+m) , swap-a, ID-u procesa itd... Radi lakšeg uočavanja procesa koji je aktivan, koristi se taster "z" koji boji sve procese u crveno, a belom bojom iskače proces koji je najintenzivniji prema definisanim parametrima (slika 67.). Takođe, moguć je i prikaz startovanog procesa od strane određenog korisnika :
#top -u sumnjivog_korisnika



Slika 67. *Prikaz izlaza top komande*

Ono što je forenzičaru važno jeste prikaz apsolutnih putanja startovanih procesa i to se radi sa tasterom "c" nakon pokretanja top komande. Slučaj u praksi je bio sledeći. Http server Organizacije je prestao odjednom sa radom. Analizom podataka na serveru došlo se do zaključka da nije bilo napada već je http server Zope bio ažuriran sa bagovitim fajlovima i generisao je veliku količinu log fajlova, koji su zauzeli 100% prostora na disku. Analizom top komande došlo se do procesa koji je generisao greške i fajla u koji je te greške upisivao. Nakon zaustavljanja top procesa, brisanjem prepunjenog log fajla i korigovanjem bagovitih fajlova, Zope http server uspešno je startovan i problem je bio rešen. Pokrenute servise na sistemu možemo utvrditi i pomoću komande :

#service --status-all

#ps -A

3.2.6 Podaci od značaja privremenog karaktera na Linux-u - Otvoreni fajlovi

Komandom lsof može se dobiti lista otvorenih fajlova na sistemu. Za forenzičko ispitivanje ovo mogu biti dragoceni podaci. Na primer, mogu se uočiti skriveni fajlovi, odnosno maliciozni alati koji mogu biti password crackeri, exploiti i drugi maliciozni programi, koji mogu iskoristiti resurse samog servera uperene kako protiv samih korisnika na sistemu tako i protiv drugih sistema, za distribuciju ili hostovanje, dečije pornografije, distribucija sadržaja zaštićenih autorskim pravima i mnoge druge vrste visokotehnološkog kriminala.

Komande koje forenzičaru mogu biti od koristi su sledeće :

#lsof -u root - prikazuje sve otvorene procese i otvorene fajlove od strane root korisnika

#lsof -p 3333 - prikazuje sve otvorene fajlove od strane procesa sa ID 3333

#lsof /var/log/auth.log prikazuje proces koji otvara određeni fajl kao na slici 68. :

```
root@ubunt1104srvx86:/var/log# lsof /var/log/auth.log
COMMAND  PID   USER   FD   TYPE DEVICE SIZE/OFF   NODE NAME
rsyslogd 366 syslog    1w   REG    8,1     7300 665417 /var/log/auth.log
root@ubunt1104srvx86:/var/log#
```

Slika 68. *Prikaz izlaza lsof komande nad fajlom /var/log/auth.log*

#lsof /home može se pokazati kao jako korisna informacija ukoliko sistem prikazuje grešku zauzeća (eng. Device or resource busy), jer može prikazati koji su procesi odgovorni za montiranje tačke /home na sistem.

3.2.7 Podaci od značaja privremenog karaktera na Linux-u - Interna tabela rutiranja i keš tabele

Da bi administrator ili forenzičar ustanovili da li je ruting tabela menjana iz istih navedenih razloga kao što su napisani u delu rada koji opisuje podatke od značaja privremenog karaktera na Windows-u to se radi isto sa netstat komandom (ili sa route komandom) kao na slici 69. :

#route

ili

#netstat -nr

```
root@ubunt1104srvx86:~# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
```

Slika 69. *Prikaz izlaza komande netstat -rn*

Address Resolution Protocol ili skraćeno ARP je TCP/IP protokol koji se koristi da pretvori IP adresu u fizičku adresu odnosno MAC adresu. Za digitalnog forenzičara značajno je ispitivanje ARP keša ispitivanog računara, jer je moguće identifikovati druge sisteme koji su trenutno ili nedavno uspostavili vezu sa ispitivanim računarom. Prema tome informacije prikupljene putem ARP keša se koriste za otkrivanje dodatnih računara na mreži koji su možda kompromitivani kao posledica incidentnih/protivpravnih aktivnosti. Takođe, sa stanovišta bezbednosti ispitivanje ARP keša koristi se i za identifikovanje sumnjivih računarskih sistema na mreži koji mogu biti korišćeni za pokretanje internih napada u mreži. Da bi se na sistemu prikazao sadržaj ARP keša koristi se komanda "arp" (slika 70):
#/mnt/cdrom/arp

```
[root@turing ~]# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
147.91.96.190            ether   a0:f3:c1:a2:0c:05   C                     eth0
147.91.96.208            ether   a0:f3:c1:a2:41:b3   C                     eth0
147.91.96.148            ether   00:19:99:d3:90:33   C                     eth0
147.91.96.149            ether   00:19:99:e4:cf:d6   C                     eth0
147.91.96.146            ether   50:26:90:a1:46:f6   C                     eth0
```

Slika 70. *Prikaz ARP keša komandom arp*

Ova komanda prikazaće sve IP adrese koje su konektovane ili bile konektovane sa ispitivanim računarom. To može biti veoma korisna informacija jer može pokazati da li je zlonamerni napadač došao sa Internet mreže i koja je IP adresa korišćena [183].
Forenzičar pomoću netcat-a može prikupiti na živom sistemu ove informacije na sledeći način :

#netcat -v -l -p 9898 > ARPkeš_kompromitovanog_racunara
#/mnt/cdrom/arp | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum ARPkeš_kompromitovanog_racunara > ARPkeš_kompromitovanog_racunara.sh256

Trenutno aktivne rute na sistemu čuvaju se u tzv. ruting kešu, odnosno ruting keš tabeli (eng. kernel route cache table). Treba napomenuti da se ruting keš tabela razlikuje od ruting tabele. Naime, ruting keš tabela prikazuje trenutno aktivne (uspostavljene) rute na sistemu. Ruting tabela se koristi za donošenje odluke oko rutiranja, a ruting keš tabela daje prikaz ruta koje su uspostavljene. I upravo to je ono što može biti značajno za forenzičku istragu, jer prikupljene informacije iz ruting keš tabele mogu pomoći u otkrivanju računara na mreži kako onih koji su možda kompromitivani, tako i onih sa kojih je incidentna/protivpravna aktivnost izvršena. Takođe, sa stanovišta bezbednosti prikupljanje informacija iz ruting keš tabele može se koristiti i za identifikovanje sumnjivih računarskih sistema na mreži koji mogu biti korišćeni za pokretanje internih napada u okviru mreže. Ruting keš tabela (eng. Kernel route cache table) daje prikaz izvorne adrese (eng. source) i odredišne adrese (eng. destination), mrežni izlaz (eng. gateway) i interfejs, koji se koristi da bi se veza uspostavila.
Na Linux sistemima ispitivanje rute keša može se dobiti pomoću komande "route" (slika 71.):
#route -Cn

```
root@emis:~# route -Cn
Kernel IP routing cache
Source          Destination     Gateway         Flags Metric Ref    Use Iface
66.249.76.226   147.91.102.6    147.91.102.6    l     0      0       49 lo
147.91.102.6    66.249.76.162   147.91.102.1          0      0        1 eth0
147.91.102.6    66.249.76.226   147.91.102.1          0      0        7 eth0
147.91.102.6    66.249.76.14    147.91.102.1          0      0       14 eth0
147.91.102.6    147.91.96.2     147.91.102.1          0      2        0 eth0
147.91.102.6    147.91.96.2     147.91.102.1          0      0        4 eth0
192.168.2.4     192.168.2.255   192.168.2.255   ibl   0      0       11 lo
```

Slika 71. *Prikaz sadržaja Ruting keš tabele uz pomoć komande route -Cn*

Forenzičar pomoću netcat-a može prikupiti na živom sistemu ove ruting keš informacije na sledeći način :
#netcat -v -l -p 9898 > ruting_kes_tabela_kompromitovanog_racunara
#/mnt/cdrom/route -Cn | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum ruting_kes_tabela_kompromitovanog_racunara > ruting_kes_tabela_kompromitovanog_racunara.sh256

3.2.8 Podaci od značaja privremenog karaktera na Linux-u - Učitani moduli u kernel LKM

Ukoliko postoji osnovana sumnja od strane forenzičara da je postojeći kernel ispitivanog sistema kompromitovan određenim rootkit-om odnosno, trojancom potrebno će biti izlistati učitane module u kernel. To se može uraditi na sledeće načine :
#netcat -v -l -p 9898 > moduli_kompromitovanog_racunara
*#/mnt/cdrom/cat **/proc/modules** | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898*
#sh256sum moduli_kompromitovanog_racunara >
moduli_kompromitovanog_racunara.sh256
ili sa proverenom komandom lsmod :
#netcat -v -l -p 9898 > moduli_kompromitovanog_racunara
#/mnt/cdrom/lsmod | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum moduli_kompromitovanog_racunara >
moduli_kompromitovanog_racunara.sh256

Izlaz komande lsmod prikazan je na slici 72. :

```
root@ubunt1104srvx86:~# lsmod
Module                  Size  Used by
vesafb                 13449  1
snd_ens1371            24722  0
gameport               15027  1 snd_ens1371
snd_rawmidi            25269  1 snd_ens1371
snd_seq_device         14110  1 snd_rawmidi
snd_ac97_codec        105614  1 snd_ens1371
ac97_bus               12642  1 snd_ac97_codec
snd_pcm                80244  2 snd_ens1371,snd_ac97_codec
ppdev                  12849  0
vmw_balloon            12729  0
psmouse                59039  0
snd_timer              28659  1 snd_pcm
```

Slika 72. *Prikaz trenutno učitanih modula u kernel uz pomoć komande lsmod*

Dodatno /sys/modules folder sadrži podfoldere za svaki modul učitan u kernel. U ovom folderu se mogu pronaći opširnije informacije u odnosu na „lsmod“ izlaz, što može pružiti bolju ideju o mogućnostima kernela koji se ispituje [149].

Ono što forenzičar treba da ima na umu je da u praksi postoje određene tehnike kojima se maliciozni modul može učitati u kernel i sakriti ga nakon toga. Jedan takav rootkit zove se Knark (više informacija o Knarku[357] može se saznati na SANS[358] sajtu). Nakon skrivanja učitanog modula ne postoji šansa da se on otkrije forenzičkim ispitivanjem "uživo".

[357] Dostupno na http://www.sans.org/security-resources/idfaq/knark.php
[358] http://www.sans.org/

3.2.9 Podaci od značaja privremenog karaktera na Linux-u - Dump memorije i memorijskih procesa

Da bi forenzičar mogao da analizira memoriju sa kompromitovanog računara potrebno je da se "snimi" (eng. capture u daljem tekstu) fizička memorija o čemu je već bilo reči u poglavlju koje govori o Dump-u memorije na Windows operativnom sistemu. Treba imati u vidu da kada se vrši „snimanje“ memorije, takođe se i remeti trenutno stanje memorije, a razlog je pokretanje programa i čitanje podataka. Dodatan problem takođe predstavlja upisivanje fajla sa snimljenim stanjem fizičke memorije. To znači da će bilo koji izlaz fajla biti keširan u memoriji, zamenjujući možda veoma važne informacije značajne za digitalnu istragu. Zato korišćenje forenzičkog računara jeste najbolji način da se sačuvaju podaci sa minimalnim uticajem na memoriju. Zapravo, kada je reč o "snimanju" memorije, forenzičar se susreće sa jednom dilemom : želja da se sačuva što veća količina veoma promenljivih podataka, ali njihovim prikupljanjem mogu se uništiti dodatni dokazi. Odluka forenzičara u vezi sa ovom dilemom mora biti takva da značaj prikupljenih podataka mora biti veći od značaja onih podataka koji će se izgubiti, a to veoma zavisi od iskustvene procene samog forenzičara.

Zbog obaveznog dokumentovanja celog postupka, preporuka je da se prikupe osnovne informacije o memoriji. Fajl koji sadrži ove podatke jeste /proc/meminfo. To se radi na sledeći način :

#netcat -v -l -p 9898 > mem_info_kompromitovanog_racunara
#/mnt/cdrom/cat < /proc/meminfo | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum mem_info_kompromitovanog_racunara > mem_info_kompromitovanog_racunara.sh256

Najjednostavniji način, mada ne i univerzalan, za "snimanje" kompletne fizičke memorije na Linux sistemima jeste pokretanje proverene statički kompajlirane dd komande[359].

#netcat -v -l -p 9898 > fiz_mem_kompromitovanog_racunara
#/mnt/cdrom/dcfldd < /dev/mem | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum fiz_mem_kompromitovanog_racunara > fiz_mem_kompromitovanog_racunara.sh256

Ovaj postupak funkcioniše na Linux sistemima, međutim neki od Unix sistema (na primer FreeBSD, Solaris) tretiraju fizičku memoriju na drugačiji način, što za posledicu može imati nekompletan sadržaj fizičke memorije [61]. Postoji alatka "memdump" u okviru The Coroner's Toolkit-a (TCT) [360] koja uspešno razrešava pomenuti problem koristići pritom minimalno memorije sa minimalnim uticajem na nju. Forenzički ispravan način primene ovog progama jeste na sledeći način :

#netcat -v -l -p 9898 > fiz_mem_kompromitovanog_racunara
#/mnt/cdrom/memdump | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum fiz_mem_kompromitovanog_racunara > fiz_mem_kompromitovanog_racunara.sh256

[359] http://dcfldd.sourceforge.net/

[360] The Coroner's Toolkit (TCT) predstavlja kolekciju forenzičkih alata čiji su autori Wietse Venema i Dan Farmer , dostupno http://www.porcupine.org/forensics/tct.html , 05.04.2013

Sadržaju fizičke memorije može da se pristupi i preko fajla /proc/kcore. Ovaj fajl sadrži podatke iz fizičke memorije koji se nalaze u ELF[361] core fajl formatu. Opšte je mišljenje da je vrlo preopručljivo prikupiti sadržaj ovog fajla, pored sirovih (eng. raw format) podataka iz memorije. Razlog je taj, što se ovaj format može ispitati sa GNU debbuger-om tzv. GDB[362] uz pomoć "System map" fajla i slike kernela iz /boot direktorijuma. Ovaj postupak opisao je Mariusz Burdach u svojim radovima [363] [364][21][22].

Kada je o memoriji reč takođe, forenzički je značajan i swap prostor na sistemu. Swap prostor predstavlja prostor u kome se delovi memorije - stranice[365] (eng. pages) privremeno smeštaju u slučaju potrebe oslobađanja dela RAM memorije[366] (ili je sistemu potrebno više memorije, nego što je raspoloživo postojećim RAM-om). Zbir RAM memorije i swap memorije predstavlja ukupuno količinu virtuelne memorije na sistemu. Swap prostor može postojati u formi swap particije (što je preporučljivo), swap fajla ili kombinacije swap fajla i particije. Ovaj prostor može sadržati značajne informacije za forenzičku istragu (iako sistem retko swap-uje). Ovaj prostor se može jednostavno iskopirati korišćenjem alata "dd" ili "cat" nad swap particijom ili fajlom uz pomoć "netcat" alatke i posle pretraživati određenim alatima u potrazi za određenim stringom (na primer hexdump[367]).

Dump memorije startovanih procesa moguće je uraditi pomoću alatke pcat koja se nalazi u sastavu pomenutog The Coroner's Toolkit-a (TCT)[368] (može da se preuzme sa sajta prikazanog u tabeli 11. ovog rada). Forenzički ispravna upotreba ove komande jeste :

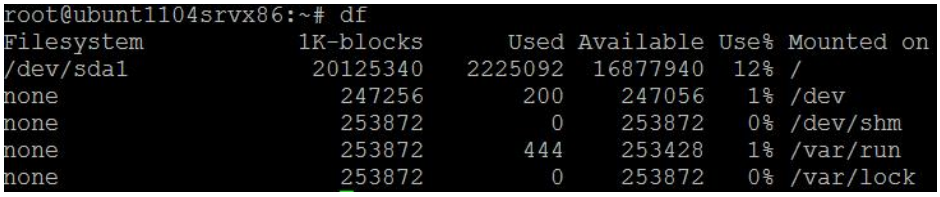
#netcat -v -l -p 9898 > pcat_kompromitovanog_racunara
#/mnt/cdrom/pcat proc_id | /mnt/cdrom/netcat ip_adresa_forenzicke_radne_stanice 9898
#sh256sum pcat_kompromitovanog_racunara > pcat_kompromitovanog_racunara.sh256

Poznavanje načina na koji sistem upotrebljava memoriju (keširanje fajlova i stranice sa virtuelnom memorijom (eng. memory page) čiji je cilj poboljšanje performansi računara), veoma je važan za analizu same memorije. Iz navedenog može se videti da se mogu pronaći i identifikovati značajni delovi memorije na sistemu što za digitalnu istragu može predstavljati veliku korist.

3.2.10 Podaci od značaja privremenog karaktera na Linux-u - Montirani fajl sistemi

Za forenzičko ispitivanje, važno je da se ustanovi koji su fajl sistemi montirani (eng. mounted) u ispitivanom operativnom sistemu. Postoje određene komande kojima se to može ustanoviti. Prva komanda je **mount** komanda:
#mount čiji izlaz prikazuje uređaje (na primer hard disk) tačku montiranja i tip fajl sistema.
Druga komanda jeste **df** komanda :
#df čiji izlaz prikazuje montirane uređaje, tačku montiranja, veličinu i raspoloživi kapacitet i veličinu zauzeća (slika 73.).

[361] ELF - Executable and Linking *Format*
[362] https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/s2-proc-kcore.html
[363] http://www.symantec.com/connect/articles/detecting-rootkits-and-kernel-level-compromises-Linux
[364] http://www.symantec.com/connect/articles/forensic-analysis-live-Linux-system-pt-2
[365] U Linux sistemima RAM memorija se deli na delove memorije koji se nazivaju stranice (eng. pages)
[366] Kernel može da izmešta na swap prostor one delove memorije koji se manje koriste (neaktivne) i da tu oslobođenu memoriju dodeli tekućem programu odnosno procesu kome je potrebna memorija.
[367] http://Linux.about.com/library/cmd/blcmdl1_hexdump.htm
[368] http://www.porcupine.org/forensics/tct.html



Slika 73. *Izlaz df komande*

Prethodne dve komande ne mogu videti montirane deljene resurse mrežnog fajl sistema ili skraćeno NFS (eng. Network File System). Komanda koja može prikazati NFS deljene resurse jeste showmount :
#showmount -a localhost ili showmount -e koja pokazuje exportovane sisteme
#showmount -a localhost
All mount points on localhost:
192.168.1.104:/nfs/slike
192.168.1.101:/nfs/filmovi

Prikazuje spisak računarskih sistema koji su konektovani na lokalni sistem njihove tačke pristupa. Ova komanda forenzičarima može omogućiti prikupljanje dragocenih podataka na ispitivanom operativnom sistemu, pogotovu kada je u pitanju neovlašćena distribucija zaštićenih autorskih dela ili zabranjenih pornografskih sadržaja.

3.2.11 Postojani podaci od značaja na Linux-u - Verzija operativnog sistema i nivo ažuriranosti paketa

Za forenzičku istragu značajno je saznati o kojoj se verziji operativnog sistema radi (i koji je kernel u pitanju) da bi se primenio forenzički alat adekvatan verziji Linux operativnog sistema. Vezrija operativnog sistema na većini Linux distribucija može se dobiti alatom uname sa svičem "-a" :
#**uname -a** koji izlistava ime računara, verziju kernela, Linux distribuciju, vreme i tip sistema (x86 ili x64), ali ne izlistava verziju Linux distribucije
#Linux ubunt1104srvx86 2.6.38-8-generic-pae #42-Ubuntu SMP Mon Apr 11 05:17:09 UTC 2011 i686 i686 i386 GNU/Linux

Na primer, na Debian i Ubuntu distribucijama moguće je videti i verziju Linux distribucije alatom "**lsb_release**"sa svič-em "-a" :
lsb_release -a koji daje sledeći izlaz :
Description: Ubuntu 11.04
Release: 11.04
Codename: natty

Na Red Hat distribuciji verziju Linux distribucije moguće je videti izlistavanjem fajla "**/etc/redhat-release**" sa alatkom "**cat**"
#**cat /etc/redhat-release** koji daje sledeći izlaz :
Red Hat Enterprise Linux Server release 6.3 (Santiago)

Nivo ažuriranosti paketa (eng. patch level) je teže dobiti i razlikuje se od distribucije do distribucije. Na Red Hat distribuciji moguće je dobiti spisak instaliranih paketa komandom "**rpm -qa**"
rpm -qa koja daje sledeći izlaz :
libXxf86misc-1.0.2-1.el6.x86_64
openjpeg-libs-1.3-9.el6_3.x86_64
libcroco-0.6.2-5.el6.x86_64
evolution-data-server-doc-2.28.3-15.el6.noarch
libSM-devel-1.1.0-7.1.el6.x86_64

...

Na Ubutntu ili Debian distribuciji nivo ažuriranosti moguće je dobiti komandom : #**dpkg --get-selections** koja daje sledeći izlaz :

adduser install
apache2 install
apache2-mpm-prefork install
apache2-utils install
apache2.2-bin install
apache2.2-common install
apparmor install

Prikupljanjem ovih informacija moguće je dobiti vrlo korisne početne informacije o bezbednosti sistema, odnosno njegovoj ranjivosti na osnovu instaliranih paketa.

3.2.12 Postojani podaci od značaja na Linux-u -Vremenski pečati fajlsistema

Vremenski pečati fajlova na sistemu mogu da se dobiju na različite načine. Jedan od načina je korišćenje alatke "stat". Ukoliko želimo da utvrdimo određene informacije o nekom fajlu na primer o dozvolama nad fajlom, datumu i vremenu poslednjeg pristupa fajlu, datumu i vremenu poslednje izmene na fajlu, datumu i vremenu promene inoda, o vlasništvu nad fajlom (korisnik i grupa), o veličini fajla i putanji do fajla (ukoliko se radi pretraga celog sistema), moguće je uraditi na sledeći način :

#stat /etc/passwd dobija se izlaz :

File: `/etc/passwd'
Size: 1467 Blocks: 8 IO Block: 4096 regular file
Device: 801h/2049d Inode: 1058850 Links: 1
Access: (0644/-rw-r--r--) Uid: (0/ root) Gid: (0/ root)
Access: 2013-02-03 17:13:19.650908871 +0100
Modify: 2013-02-03 17:13:19.610908872 +0100
Change: 2013-02-03 17:13:19.618908872 +0100

Ukoliko forenzičar želi dobiti ove podatke za sve fajlove koji se nalaze u sistemu u čitljivom formatu, mora se pretražiti ceo fajl sistem, a to se može uraditi na sledeći način :

#find / -printf "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%U;%G;%s;%p\n"

Izlaz ove komande su informacije o fajlovima razdvojene sa ";" u formatu koji je kompatibilan sa većinom programa koji rade sa tabelama na primer Microsoft Excell :

"755;02/04/2013;14:43:12.0258794640;07/07/2011;07:59:13.3346548330;07/07/2011;07:59:13.3346548330;0;0;4096;/usr/src/Linux-headers-2.6.38-8/scripts/basic"

Forenzičar treba da zna da Linux ne poznaje vreme kreiranja fajla već vreme promene "inoda" poznato kao "ctime" i ono je najbliže vremenu stvaranja (eng. creation time).

Prikupljene informacije treba koristiti u korelaciji sa dobijenim podacima iz prethodnih postupaka da bi se dobila što potpunija slika o mogućem incidentu odnosno protivpravnoj aktivnosti. Na primer, moguć scenario može biti takav da je izlaz komande "lsof" izlistao određene skrivene foldere koji se nisu prikazali u pomenutoj pretrazi (find /), što forenzičaru može biti indicija da se radi o kompromitovanom kernelu. U tom slučaju najbolje je uraditi forenzičku duplikaciju i analizirati skrivene fajlove i foldere. Dodatno forenzičar može primetiti kada su fajlovi /etc/passwd i /etc/shadow menjani što može biti dragocen forenzički podatak jer se on odnosi na korisničke naloge i šifre na sistemu. Ovi fajlovi su od krucijalnog značaja za bezbednost sistema. Više o ovom fajlu govoriće se u delu o korisničkim nalozima na sistemu.

Naravno, prikupljeni podaci mogu ukazati i na prisutvo određenih perl modula koji nisu instalirani od strane administratora, pa bi forenzički fokus mogao da bude i njihova

analiza . Najjednostavniji način izlistavanja perl modula na sistemu je sa alatkom "instmodsh" :
#instmodsh - ova interaktivna komanda ima sledeći izlaz :

l - List all installed modules
m <module> - Select a module
q - Quit the program
cmd? l
Installed modules are:
Perl
cmd?

Treba naglasiti da bi određeni maliciozni program funkcionisao (pod pretpostavkom da se oslanja na određene perl module), perl moduli ne smeju biti sakriveni, već moraju biti vidljivi malicioznom programu.

3.2.13 Postojani podaci od značaja na Linux-u - Checksum fajl sistema

Jedan od načina da se proveri integritet sistemskih fajlova ili prikupljenog imidža hard diska sa ispitivanog računara, jeste korišćenje MD5 ili SHA-1 heširanja nad njima. Treba napomenuti, da prema radu Wang Xiaoyun i njenih saradnika sa Beijing's Tsinghua University i Shandong University of Technology, postoje tri pravila koja se odnose na forenzička heširanja [202]:

a. Ne može se predvideti heš vrednost fajla ili uređaja.
b. Ne postoje ista heš vrednost za dva različita fajla (u istraživanju kolizije su nastale upotrebom superračunara).
c. Ukoliko se bilo šta promeni u fajlu ili uređaju, heš vrednost se mora promeniti.

SHA-1 jeste zamena za MD5 i CRC-32 mada se MD5 još uvek najčešće koristi. Mora se reći da su se i u MD5 i u SHA-1 desile kolizije, odnosno da su dva različita fajla imale iste vrednosti. Kolizije su retke, međutim uprkos nedostacima MD5 i SHA-1, oba algoritma za heširanje su korisna za utvrđivanje integriteta digitalnih dokaza prikupljenih iz fajlova ili uređaja za skladištenje podataka. Ukoliko se sumnja na koliziju, preporuka je da se radi byte-by-byte poređenje, da se utvrdi da li su svi bajtovi identični [140].

Kreiranje heš vrednosti nad svim sistemskim fajlovima, sistem administratoru može pomoću pri kasnijem detektovanju izmenjenih fajlova na sistemu i time preventivno delovati na bezbednost postojećeg sistema. Digitalnom forenzičaru je na raspolaganju i heš baza poznatih sistemskih fajlova na NIST sajtu[369] u okviru projekta " National Software Reference Library " koji se mogu uporediti sa prikupljenim fajlovima sa ispitivanog sistema. Time se štedi vreme za forenzičku istragu, jer pomenuta baza eliminiše poznate sistemske fajlove i uzimaju se u obzir samo oni izmenjeni i nepoznati. Takođe, forenzičar može izgraditi sopstven bazu na primer bazu malicioznih programa (poznatih password crackera ili exploita) i uporediti sa fajlovima na ispitivanom računaru. Ukoliko se nađu fajlovi koji se poklapaju, to zapravo znači da na sistemu postoji takav maliciozni fajl. Izračunavanje heš vrednosti svih fajlova na Linux sistemu moguće je na sledeći način :

 # find / -xdev -type f -exec md5sum -b {} \; > svi_fajlovi.md5

Izlaz ove komande daje 128-bitnu heš vrednost i putanju do fajla :

*22bfb8c1dd94b5f3813a2b25da67463f */home/vanja/.bash_logout*
*55dc7ec44bb9d0f7a1bbadd46509a6cc */home/vanja/.bashrc*
*3cb2fb7972b22f773570327937fd4c2b */boot/vmlinuz-2.6.38-8-generic-pae*
*2081983a66f424b8827816747e629f4f */boot/vmcoreinfo-2.6.38-8-generic-pae*
*cdc81e7f4589b6b0665dbdeccf905e43 */boot/initrd.img-2.6.38-8-generic-pae*
*7f8688690cf286e6d8a1466114b30383 */boot/System.map-2.6.38-8-generic-pae*

[369] http://www.nsrl.nist.gov/

*f55e50847b31e1adebd938452573c380 */boot/grub/ohci.mod*

Takođe moguće je zbog veće bezbednosti koristiti i SHA-256 heš to se radi na sledeći način :

 # find / -xdev -type f -exec sha256sum -b {} \; > svi_fajlovi.sha1

Izlaz ove komande jeste SHA-256 256-bitna heš vrednost i putanja do fajla :

*dc216ac4a4c232815731979db6e494f315b507dd */home/vanja/.bash_logout*
*7a2dd812db7465d93fd0c0567123ef7a4d7c86ed */home/vanja/.bashrc*
*3a08ac3ce95404186b72647d7a88bf18a06acf98 */boot/vmlinuz-2.6.38-8-generic-pae*
*45ba33a6642c9994c2bb09564b4dd2c2224f2ed8 */boot/vmcoreinfo-2.6.38-8-generic-pae*
*fb9eb00af37da053c29e31206a7eb3e13031117b */boot/initrd.img-2.6.38-8-generic-pae*
*352afe195c4484eb80e6f7fef9a377c3d3d72580 */boot/System.map-2.6.38-8-generic-pae*
*86d46047f90cce4984bfd0dbbd7e12cec897c812 */boot/grub/ohci.mod*

Postoji i alatka md5deep (sha1deep) kojom se može uraditi MD5 ili SHA-256 na sistemu :

#sha256deep -r -s /ispitivani_direktorijum > heš_direktorijum.sha256

Ovom alatkom lako se mogu utvrditi razlike u heš vrednostima na sledeći način:

#sha256deep -r -X heš_direktorijum.sha256 /ispitivani_direktorijum

Alatka će imati izlaz samo ukoliko se pronađu razlike u heš vrednostima. Sa stanovišta bezbednosti sistema, ova alatka ima veliku upotrebnu vrednost, jer se mogu utvrditi podaci koji su izmenjeni na sistemu.

3.2.14 Postojani podaci od značaja na Linux-u - Ulogovani korisnici na sistem

Informacija o tome koji su korisnici trenutno ulogovani na sistem, čuva se u /var/run/utmp, ali nije u čitljivom obliku već u binarnom. Najbolje je koristit komandu "w" koja daje sledeći izlaz na sistemu:

 # w
9:38:16 up 1 day, 4:28, 2 users, load average: 0.00, 0.01, 0.12

USER	*TTY*	*FROM*	*LOGIN@*	*IDLE*	*JCPU*	*PCPU*	*WHAT*
root	*tty1*		*Sun15*	*27:46m*	*0.27s*	*0.21s*	*bash*
root	*pts/0*	*zevs.local*	*11:47*	*0.00s*	*1.51s*	*0.00s*	*w*

Ova komanda prikazuje korisnike koji su trenutno ulogovani (na konzoli *tty* ili preko pseudo terminala *pts* na primer ssh, xterm, screen) na Linux sistem. Takođe, moguće je trenutno ulogovane korisnike videti i komandom last :

#last -f /var/run/utmp

Problem za forenzičara je taj, ukoliko je napadač pokrenuo određeni program za prikrivanje svoje prave IP adrese kojom se prijavio na sistem (kao na primer određene Antilog skripte[370])[93]. U tom slučaju jedini način da se utvrdi prava ip adresa je detaljna pretraga nakon dupliciranja hard diska.

3.2.15 Postojani podaci od značaja na Linux-u - Istorija logovanja na Linux sistem

Istorija validnih korisničkih prijava i odjava sa Linux sistema čuva se u takođe binarnom fajlu /var/log/wtmp, a neuspela logovanja na sistem čuvaju se u binarnom fajlu /var/log/btmp.

Ovaj fajl čuva podatke iz prošlosti o prijavljivanju na sistem, odjavljivanju sa sistema, gašenju sistema i restartovanju sistema sa prikazanim vremenom.

[370] Dostupno na http://www.packetstormsecurity.org/UNIX/penetration/log-wipers/

U toku forenzičkog ispitivanja "uživo" ovi podaci, se mogu videti alatkama last i lastlog. Lastlog čuva svoj sadržaj u fajlu /var/log/lastlog.
last daje izlaz :

```
root     pts/0        zevs.local      Mon Feb  4 20:24   still logged in
reboot   system boot  2.6.38-8-generic Mon Feb  4 20:22 - 20:24  (00:02)
root     pts/0        zevs.local      Mon Feb  4 11:47 - down   (08:34)
root     pts/0        zevs.local      Sun Feb  3 17:11 - 11:01  (17:50)
root     pts/0        zevs.local      Sun Feb  3 15:54 - 17:06  (01:12)
root     pts/0        zevs.local      Sun Feb  3 15:09 - 15:53  (00:44)
root     tty1                         Sun Feb  3 15:08 - down  (1+05:13)
root     tty1                        Sun Feb  3 15:08 - 15:08  (00:00)
reboot   system boot  2.6.38-8-generic Sun Feb  3 15:07 - 20:22 (1+05:14)
```

Ukoliko bi forenzičar hteo da pročita fajl o neuspešnim logovanjim na sistem sa alatima “cat“ ili “vi“ dobio bi nerazumljiv tekst. Način na koji forenzičar (ili administrator) može doći do dragocenih podataka koji se odnose na neuspešna logovanja na sistem, jeste sa komadnom “last“ :

```
#last -f /var/log/btmp
root@turing ~# last -f /var/log/btmp
miska    ssh:notty    localhost       Tue Feb 12 18:38    gone - no logout
miska    ssh:notty    localhost       Tue Feb 12 18:38 - 18:38  (00:00)
pera     ssh:notty    localhost       Tue Feb 12 18:34 - 18:34  (00:00)
root     ssh:notty    localhost       Tue Feb 12 18:18 - 18:34  (00:15)
vanja    tty1         :0             Tue Feb 12 18:15    gone - no logout
```

Alatka lastlog daje podatke o korisničkom imenu, portu, vremenu poslednje prijave na sistem :
#lastlog

Username	*Port*	*From*	*Latest*
root	*pts/0*	*zevs.local*	*Mon Feb 4 20:24:45 +0100 2013*
daemon			***Never logged in***
bin			***Never logged in***
sys			***Never logged in***
sync			***Never logged in***

Informacije koje forenzičar može otkriti opisanim alatkama su sledeće : koji su korisnici i kada bili prijavljeni (ili su još uvek) na sistem, sa kojom IP adresom i preko kog terminala. Takođe, može se videti i vreme kada je sistem bio restartovan. Ove informacije mogu pomoći forenzičarima, baš kao i administratorima da otkriju da li neko koristi naloge za koje nije ovlašćen, a pažljivom analizom moguće je otkriti malicioznog korisnika i njegovu pravu IP adresu. Takođe, forenzičkom analizom moguće je i otkriti datapipe alate[371] koji omogućuju radirekciju portova sa namerom zaobilaska firewala na sistemu. Može se reći da je analizom pomenutih fajlova moguće pravovremeno uočiti određene bezbednosne pretnje i time sprečiti nastanak veće štete, a forenzičarima pružiti dragocene podatke za dalji tok istrage.

3.2.16 Postojani podaci od značaja na Linux-u – Logovi na sistemu

Syslog je standard za logovanje na Linux sistemima. Kao što Windows ima svoj event loging mehanizam, tako Linux ima svoj sistem za logovanje koji procesira logove prema određenom tipu. Može se koristiti za upravljanje računarskim sistemom, za nadzor bezbednosti na sistemu, kao i za pružanje generalnih informacija za analizu i otklanjanje grešaka. Može se smatrati centralizovanim sistemom za praćenje događaja. Ima svoj proces

[371] Neki od ovih alata moguće je naći na http://packetstormsecurity.com/search/files/?q=datapipe

(eng. daemon) koji sluša poruke koje generišu drugi programi (ili serveri na Internetu) i skladišti ih prema konfiguracionom fajlu /etc/syslog.conf odnosno /etc/rsyslog.conf[372]. U ovom konfiguracionom fajlu opisani su podsistemi koji generišu poruke za logovanje i putanje do fajlova u kome će se te poruke smestiti. Podsistemi su sledeći [149] : auth i authpriv (odnose se na proveru sigurnosnih događaja i proveru identiteta), cron (odnosi se na raspored poslova na sistemu), daemon (odnosi se na servise odnosno daemon procese na sistemu), kern (odnosi se na informacije iz kernela tj. jezgra sistema), lpr (odnosi se na podsistem za štampanje), mail (odnosi se na podsistem za elektronsku poštu), news (odnosi se na podsistem za vesti), sysloguser (odnosi se na interne poruke), uucp (odnosi se na komunikacioni podsistem Unix to unix) i od local0 do local7 (za lokalnu upotrebu).

Format svakog reda u okviru konfiguracionog fajla syslog.conf je :
izvor_poruke.prioritet{;izvor_poruke.prioritet}{TAB}{putanja do log fajla}

Vrednosti prioriteta moguće su sledeće :

- **debug, info** - ovde spadaju poruke informacionog karakter (ne zahtevaju dodatne akcije od strane administratora);
- **notice** - ovde spadaju poruke sa većim značajem i nisu u pitanju greške (ne zahtevaju hitno reagovanje ali ih treba pratiti);
- **warning** - ne predstavljaju greške, ali ukazuju da greška može da nastane ukoliko se određena akcija ne preduzme (na primer zauzeće fajl sistema je prešlo 90%);
- **error i critial** – ovde spadaju poruke koje se odnose na greške i kritične greške;
- Windows – ovde spadaju poruke koje zahtevaju hitnu intervenciju administratora (na primer prekih mrežne konekcije);
- **emmerg** – ovde spadaju poruke o greškama koje mogu dovesti do prestanka rada celog sistema (osim preduzimanja administratorskih intervencija obaveštava se i tehničko osoblje).

Na primer, ukoliko u konfiguracionom fajlu stoji *.info;mail.none, znači da će sistem logovati sve osim onoga što stoji uz none, što u ovom slučaju znači da se ne loguju informacije o mailu.

Tu se nalaze sledeće važne putanje do log fajlova :

- **/var/log/messages -** pokazuje globalne sistemske informacije. Takođe, od značaja za bezbednost ovde se mogu pronaći informacije o uspešnoj autentifikaciji komande sudo koja pruža sveobuhvatne audit informacije. Sudo komanda omogućava korisniku, sa sudo privilegijma, da izvrši komandu u ime root-a ili nekog drugog korisnika. Sudo konfiguracioni fajl se nalazi "/etc/sudoers". Po difoltu korišćenje sudo komande zahteva autentifikovanje korisnika sa sopstvenim pasvordom (ne root pasvordom). Nakon uspešne autentifikacije, ažuriraju se vremenski pečati i korisnik može koristiti sudo komandu bez pasvorda u kratkom periodu (5 minuta po difoltu) odnosno onoliko koliko se definiše u konfiguracionom "/etc/sudoers" fajlu.
- **/var/log/secure -** pokazuje informacije o proveri identiteta upućenih na mrežne servise operativnog sistema kao i informacije o korisniku koji je koristio komandu "su" (eng. substitute user) kako bi na najjednostavniji način promenio vlasništvo trenutne (ulogovane) sesije u root ili nekog drugog korisnika[373]. Takođe, ovde se mogu pronaći dragocene informacije kako o korisnicima koji su izvršili "sudo" komande tako i nazivi samih komandi. Treba napomenuti da je sa stanovišta bezbednosti jako dobro uvesti praksu da se od administratora zahteva korišćenje sudo-

[372] U zavisnosti od Linux distribucije i verzije /etc/syslog.conf je kod RedHat-a 5 dok je kod RedHat-a 6, CentOS-a, Debian-a i njegovih derivata kao što su Ubuntu i Kubuntu sistem konfiguracija sistema za logovanje nalazi se u /etc/rsyslog.conf

[373] Treba reći da se korišćenjem komande "su" na više-korisničkim sistemima osvaruje veća bezbednost kada je u pitanju upravljanje sistemom od strane administratora. U praksi to znači da postoji mnogo manji potencijal za slučajne ili zlonamerne štete jer se administrator na sistem može prijaviti kao običan korisnik (koji ima ograničene sistemske privilegije) i obavljati rutinske poslove koje ne zahtevaju root privilegije. U slučaju kada je potrebno korišćenje root privilegoja sa komandom "su" može se prebaciti na root nalog.

a pre upotrebe određene komande, jer se time omogućava i proaktivna zaštita od neprikladnih i neovlašćenih aktivnosti. To znači da treba SUDO konfiguracioni fajl, adekvatno podesiti, kako i sami administratori ne bi zaobišli odgovornost i primenjen sistem za analizu logova (kao na primer definisanje određenih komandi i šelova koje smeju da koriste).

- **/var/log/maillog -** pokazuje informacije koje se odnose na mail server;
- **/var/log/cron/ -** pokazuje informacije o stanju raspoređenih poslova (eng. scheduled task);
- **/var/log/spooler -** pokazuje događaje koji se odnose na servise UUCP ili NNTP;
- **/var/log/boot.log -** prikazuje inormacije koje se prikazuju na ekranu pri podizanju Sistema.

Informacije od dragocenog značaja koje forenzičar može pronaći se mogu podeliti u nekoliko grupa :

a. **uspešna korisnička logovanja** - mogu se pronaći u log fajlovima pod nazivima "Accepted password", "Accepted publickey", "session opened";
b. **neuspešna korisnička logovanja** - mogu se pronaći u log fajlovima pod nazivima "authentication failure", "failed password";
c. **odjajvaljivanje korisnika sa sistema** - može se pronaći pod nazivom "session closed";
d. **izmena korisničkog naloga ili brisanje** - može se pronaći u log fajlovima pod nazivima "password changed", "new user", "delete user";
e. **upotreba SUDO komandi** - može se pronaći u log fajlovima pod nazivima "sudo: … COMMAND=…","FAILED su";
f. **otkazivanje servisa** - može se pronaći pod nazivima „service failed" ili „service failure".

Svi prethodno opisani fajlovi koji mogu sadržati pomenute dragocene podatke za forenzičku istragu potrebno je prebaciti alatkom "netcat" ili "cryptcat" na forenzičku radnu stanicu za dalju analizu. Ovi fajlovi su veoma značajni kako forenzičaru tako i administratoru sistema za kontrolu bezbednosti.

Treba znati da se generisani syslog log sastoji od 5 polja (datum, vreme, ime računara, proces koji je inicirao događaj sa ID procesa i poruka). Na osnovu ispitivanja ovih fajlova moguće je ustanoviti određene incidentne/protivpravne aktivnosti (upad u sistem preko određenih exploita nad ranjivim servisima, neovlašćeno korišćenje tuđeg naloga, Dos napadi). S obzirom da ovi logovi mogu sadržati dragocene dokaze i sami mogu biti meta napada. Na primer DoS napadom moguće je onesposobiti syslog server tako da se hard disk prepuni logovima (100% zauzeća), tako da više ne može vršiti funkciju logovanja.

Jedan od načina na koji administrator može zaštititi syslog server jeste kroz njegovo izdvajanje na posebnu privatnu mrežu u okviru postojeće mreže, kreiranje firewall-a sa dozvolama za pristup serveru, samo onih računarskih sistema koje je potrebno pratiti kao i izdvajanja log fajlova na posebne fajl sisteme odnosno particije. Dodatno je potrebno postaviti okidače (eng. triggers) nad logovima sa automatskim slanjem e-mail-a administratoru, u slučaju da je ispunjen trigger kriterijum. Jedan takav alat jeste Swatch[374].

Takođe, za povećanje proaktivne zaštite u cilju praćenja izvršenih komandi na sistemu preporučljivo je pokretanje "**Accton"** servisa. Razlog je taj, što će nakon upada na sistem, zlonamerni napadač pokušati da ukloni dokaze izvršenja komandi i to uglavnom brisanjem bash_history fajla. Međutim, moguće je uključiti na sistemu proces praćenja svih izvršenih komandi, čime se omogućava uvid u svaku izvršenu komandu uključujući njen uticaj na CPU i na memoriju. Time će se omogućiti praćenje svih izvršenih komandi na računaru kao i

[374] Dostupno na http://sourceforge.net/projects/swatch/

vreme izvršenja od strane korisnika. Potrebno je instalirati paket **Psacct** koji sadrži nekoliko alata za praćenje aktivnosti i to su :
ac - daje prikaz o tome koliko vremena su korisnici na sistemu logovani,
lastcomm - prikazuje informacije o prethodno izvršenim komandama podrazumeva se da je accton omogućen kao servis,
acct - uključuje ili isključuje servis za praćenje komandi (acct servis na Debianu i Ubuntu sistemima se startuje automatski po difoltu, dok je kod Red Hata, Fedore i Centos sistema, potrebno ručno pokrenuti servis),
sa - sumira informacije o prethodno izvršenim komandama i podrazmeva se da je omogućen accton servis.

3.2.17 Postojani podaci od značaja na Linux-u – TCP Wrappers

TCP Wrappers predstavlja program koji se obavija oko TCP-a i ima ulogu poboljšanja zaštite. Bez TCP Wrapper-a, povezivanje na određeni port izvodio bi se bez ikakve zaštite tako što bi inetd pronalazio port i odgovarajući servis bi se pokrenuo. Koncept sa TCP Wrapper-om podrazumeva da se prilikom uspostavljanja veze sa portom poziva poseban program (tcpd) koji može da izvrši određene provere pre pozivanja pravog „daemon-a“. Wrapper na sistemu može da kontroliše pristup TCP i UDP servisima. Provere koje TCP Wrapper obavlja, a koje forenzičaru mogu biti od pomoći prilikom ispitivanja zlonamernih aktivnosti su sledeće :

- vrši logovanje svih zahteva uz pomoć syslog-a (što može pomoći forenzičaru da se vidi sa kojim je portom uspostavljena veza na sistemu).
- izvršava „double reverse DNS lookup“ za proveru izvorne adrese.
- vrši proveru zahteva u odnosu na /etc/hosts.allow i /etc/hosts.deny fajlove i ukoliko zahtev prođe, dozvoljava se pristup (forenzičaru može pomoći prilikom ispitivanja zlonamernog napada na system kao i pri uspostavljanju veće zaštite na sistemu).

Treba naglasiti da je za dobru zaštitu sistema (bilo da je reč organizaciji ili kućnim računarima) važan stav u kome je sve zabranjeno osim onog što je eksplicitno dozvoljeno. To znači da bi u fajlu /etc/hosts.deny bio zabranjen sav saobraćaj dok bi u /etc/hosts.allow eksplicitno bio dozvoljen onaj potreban. Na primer izvod iz loga /var/log/messages na RED HAT Enterprise Linux sistemu :

- *Oct 23 22:15:35 toledo sshd{14558}: ROOT LOGIN REFUSED FROM xxx.xxx.15.133* , može pružiti mnogo korisnih informacija kao što su vreme i datum pokušaja prijavljivanja na sistem ime računarskog sistema (domaćina) , servis (ssh) i korisnički nalog sa kojim je pokušana prijava i ip adresa sa koje je pokušana prijava.

Drugi primer u kome je snimljeno uspešno povezivanje na servis :

- *Sep 16 21:36:29 toledo in.tftpd{614}: connect from xxx.xxx.15.133*

Ovaj zapis iz /var/log/messages ukazuje da je računar sa IP adresom xxx.xxx.15.133 povezan na TFTP servis ispitivanog računara. Na osnovu ovih logova forenzičar može utvrditi korelaciju između dobijanja pristupa računarskom sistemu i pristupu određenim fajlovima na njemu.

3.2.18 Postojani podaci od značaja na Linux-u - Korisnički nalozi

Spisak korisnika koji postoje na sistemu nalazi se u /etc/passwd fajlu. Forenzičkim ispitivanjem može se utvrditi koji je nalog kompromitovan na sistemu, odnosno pridodat za kompromitovanje sistema.
Izgled /etc/passwd fajla na sistemu :

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
vanja:x:1000:1000:vanja korac,,,:/home/vanja:/bin/bash

Forenzičar treba da obrati pažnju na korisnike sa ID userom i grupom '"0"
i mestom za njihov home. Ukoliko postoji korisnik u fajlu /etc/passwd:
sumnjivi_korisnik:x:0:0:vanja korac,,,:/:/bin/bash **,** to znači da sumnjivi_korisnik ima root privilegije na sistemu što je administratoru znak za uzbunu, a digitalnom forenzičaru dragoceni podatak za dalji tok istrage.

3.2.19 Postojani podaci od značaja na Linux-u - Korisnički fajl sa istorijom izvršenih komandi

Korisnički fajlovi sa istorijom izvršenih komandi, vrlo su značajni forenzički podaci, jer mogu pružiti dragocene dokaze o načinu kompromitovanja, kako samog sistema, tako i drugih sistema, drugim rečima daju podatke o upotrebljenoj hakerskoj metodologiji. Za bash šel, istorija izvršenih komandi se nalazi u u fajlu *.bash_history*. Forenzičar može pronaći postojeće .bash_history fajlove na sledeći način :
#find / -type f -name .bash_history

3.2.20 Postojani podaci od značaja na Linux-u - Fajlovi sa SUID, SGID, Sticky bitovi i prava nad fajlovima

Prava pristupa fajlovima i folderima na Linux sistemu definisana su setom dozvola. Ove dozvole ukazuju programu o pravima pristupa korisnika ili grupe određenom folderu ili fajlu. Ovim setom definisano je da li program, proces ili korisnik mogu pristupiti određenom fajlu ili folderu. Postoje tri tipa pristupanja fajlu odnosno folderu: "r" (odnosi se na čitanje fajla ili izlistavanje direktorijuma), "w" (odnosi se na upisivanje u fajl odnosno direktorijum), "x" (odnosi se na izvršavanje fajla, odnosno prolaza kroz direktorijum), za tri različite grupe u, g, o (korisnik odnosno vlasnik fajla eng. user "u", grupa eng .group "g" i ostali eng. other "o").

Pored pomenutih standardnih prava pristupa fajlovima i folderima (prava čitanja eng. read, pravo upisa eng. write, pravo izvršenja eng. execute) na Linux sistemima, mogu postojati i specijalna prava pristupa. Ona se određuju posebnim bitovima : **SUID bit**, **SGID bit** i **Sticky bit**.

Kada se izvršni fajl pokrene, on radi u vlasništvu korisnika koji je inicirao izvršenje. To znači da, ukoliko je korisnik "test" pokrenuo komandu "ls", odgovarajući proces će se pokrenuti u vlasništvu korisnika "test". **SUID bit** (Set User ID bit), izmenjuje ovo ponašanje na sledeći način. Ukoliko je **SUID bit** postavljen na određeni program (izvršni fajl) to znači da će se taj program pokrenuti u ime vlasništva fajla bez obzira na to ko fajl pokreće. Na primer, ukoliko je korisnik "test" pokrenuo program "demo" čiji je vlasnik korisnik root, program će se pokrenuti u ime korisnika "root" (pod uslovom da je podešen **SUID bit**). Sam ovaj koncept jeste koristan u administraciji kako bi se dozvolilo određenim aplikacijama odnosno skriptama koji su pod root vlasništvom da mogu biti izvršene od strane korisnika. Ovaj koncept podrazumeva izvršenje na ovakav način, samo nad skriptama čije je izvršenje u potpunosti poznato. To znači da, iako je korisniku dozvoljeno da izvrši ove skripte odnosno programe kao root, korisnici mogu da sa njima urade **JEDINO** ono za šta su ovi programi, odnosno skripte dizajnirani da urade. Na primer, ukoliko je skripta dizajnirana tako da se vrši bekapovanje, odnosno kopiranje 10 fajlova sa jednog mesta na drugo, korisnik bi imao samo pravo da izvrši ovaj scenario, a ne i da izvrši bilo kakvu promenu nad skriptom (jer nema pravo upisa). Ovo je odlična ideja koja omogućava korisnicima da izvedu važne bekape koristeći skriptu koja ima samo određenu namenu podešenu sa **SUID** odnosno **SGID** bitom. Međutim, ovo može predstavljati i potencijalni bezbednosni rizik. S obzirom da se skripta sa **SUID bit**-om izvršava u ime root-a postoji opasnost od zlopotrebe. Maliciozni korisnik može proslediti određene parametre toj skripti i zloupotrebiti, što može dovesti do činjenja velike štete na sistemu. Preporuka je, da se broj fajlova sa suid privilegijama na sistemu svedu na minimum, da administratori budu svesni koji su to fajlovi i da oni budu dobro čuvani.

SGID bit može da se podešava i na fajlovima i na folderima ali sa različitim značenjem. Ukoliko se **SGID bit** upotrebljava nad fajlovima, ti fajlovi se izvršavaju u ime vlasnika grupe pokrenutog fajla bez obzira ko je izvršio pokretanje fajla. **SGID bit** setovan na direktorijumu koristi se za kreiranje zajedničkih direktorijuma u okviru rada na zajedničkom projektu. Na primer, više korisnika jednog projekta rade zajedno i svi pripadaju grupi "**projekat**". Pretpostavimo da se zajednički folder zove "**projekatIII400**". Zahtev je da se u toku trajanja projekta moraju deliti međusobno fajlovi i svi moraju imati uvid u sve kreirane fajlove. Ovo se može jednostavno uraditi obezbeđivanjem dozvola za čitanje na nivou grupe. Međutim, problem nastaje prilikom kreiranja fajla, jer će on pripadati primarnoj grupi korisnika koji je kreirao fajl. To znači da, kada različiti korisnici budu kreirali njihove fajlove u folderu "**projekatIII400**" ovi fajlovi neće imati vlasništvo grupe "**projekat**". Da bi se ovaj problem prevazišao folder "**projekatIII400**" se setuje sa vlasništvom grupe "projekat" i podešava mu se specijalno pravo pristupa odnosno **SGID bit**. To zapravo znači da, kada korisnici u ovom folderu budu kreirali fajlove i foldere svi oni će pripadati grupi "**projekat**".

Sticky bit se odnosi samo na direktorijume. Ukoliko korisnik želi da kreira ili obriše fajl odnosno direktorijum u nekom direktorijumu, za to mu je potrebno pravo upisa nad tim direktorijumom. Na primer, privremeni direktorijum /tmp predstavlja direktorijum za privremeno smeštanje fajlova i direktorijumu. Da bi svi korisnici u njemu mogli da kreiraju i brišu privremene fajlove on mora da bude podešen tako da dopušta sva prava (čitanje, upis, izvršenje) na sva tri nivoa (vlasnik, grupa, ostali). Međutim, javlja se problem ukoliko svi korisnici imaju pravo upisa nad /tmp direktorijumu, to znači da oni mogu i izbrisati bilo koji fajl u tom direktorijumu, a ne samo svoj. Problem se upravo rešava podešavanjem specijalnog prava **Sticky bit**-a na direktorijumu (na primer /tmp), čime se omogućava da svako može da kreira fajl odnosno direktorijum u njemu, ali korisnik može obrisati samo onaj fajl koji je u njegovom vlasništvu. Fajlovi koji nisu u vlasništvu korisnika, korisnik ne može obrisati.

Prema tome, otkrivanje svih izvršnih fajlova na sistemu koji mogu biti pokrenuti u ime drugog korisnika, naročito onih sa root privilegijama, su kritični za bezbednost sistema i

vrlo važni kada je forenzička istraga u pitanju. Digitalni forenzičar može pronaći upravo one fajlove koji su zloupotrebljeni na sistemu od strane malicioznog korisnika.
Dozvole nad fajlovima, kao što je rečeno, koriste se za kontrolu pristupa resursima. Prava pristupa definišu se sa 4 oktalne cifre. Odnos bitova svake oktalne cifre i prava pristupa može se predstaviti na sledeći način :

Prava pristupa:		Brojčana vrednost
SUID, r	=	4
SGID, w	=	2
Sticky, x	=	1

Prve tri oktalne cifre se odnose na specijalna prava pristupa (SUID, SGID, Sticky), a ostale se odnose na prava pristupa određenih kategorija korisnika (vlasnik-korisnik, grupa, ostali). Na primer :

rwxr--r-- = 744
rwsr-xr-x = 4755 (SUID bit setovan)
rwxr-sr-x = 2755 (SGID bit setovan)
rwxrwxrwt = 1777 (Sticky bit setovan)

Pravilnim podešavanjem prava pristupa, moguće je ograničiti pristup određenim informacijama. Ukoliko prava nisu ispravno podešena, svako ko pristupi sistemu moći će da radi šta hoće na njemu.

U nastavku biće prikazani načini pronalaženja fajlova koji imaju podešena specijalna prava pristupa i oni koji mogu biti od značaja za digitalnog forenzičara.

Pronalaženje svih fajlova pod root vlasništvom sa podešenim SUID bit-om:
#find / -user root -perm -4000 -print
Pronalaženje svih fajlova pod root vlasništvom sa podešenim SGID bit-om
#find / -group root -perm -2000 -print
Pronalaženje svih fajlova pod root vlasništvom sa podešenim Sticky bit-om
#find / -group root -perm -1000 -print
Pronalaženje svih fajlova sa podešenim SUID i SGID bit-om
#find / -type f \(-perm +4000 -o -perm +2000 \) -exec ls -l {} \; 2>/dev/null ili
 # find / -perm +6000 -type f -exec ls -ld {} \;
Pronalaženje svih fajlova bez vlasništva (mogući iskopirani maliciozni programi):
#find / -nouser -print
Pronalaženje svih fajlova bez grupe (mogući iskopirani maliciozni programi):
#find / -nogroup -print
Pronalaženje svih simboličkih linkova na sistemu i mesta na koja ukazuju :
#find / -type l -ls

Sve navedene komande imaju za cilj pronalaženja nvih fajlova koji mogu biti predmet detaljne forenzičke i bezbednosne analize. Iz navedenog proizilazi, da bi ključne informacije bile pravilno zaštićene veoma je važno pravilno razumeti upotrebu, kako dozvola nad datotekama, tako i specijalnih prava pristupa.

3.2.21 Postojani podaci od značaja na Linux-u - Sumnjivi fajlovi

Ukoliko se forenzičko ispitivanje radi samo "uživo", sumnjive fajlove moguće je prebaciti na forenzičku radnu stanicu koristeći alat netcat :
Na forenzičkoj radnoj stanici pokreće se :
#cryptcat -v -l -p 9898 > ime_sumnjivog_fajla
Na ispitivanom računaru pokreće se :
#cat ime_sumnjivog_fajla | cryptcat IP_adresa_Forenzickog_racunara 9898

U slučaju da se radi o kompromitovanom kernelu potrebno je uraditi i forenzičku duplikaciju da bi forenzičar bio siguran da alate koje bude upotrebio neće biti kompromitovani. Treba naglasiti određenu specifičnost kod Linuxa u odnosu na Windows kada je reč o izvršnim fajlovima. U Windows operativnom sistemu izvšni fajl je zaključan i ne može biti obrisan dok se izvršava u memoriji, što predstavlja benefit za forenzičku istragu. Sa druge strane kada je u pitanu Linux, nakon pokretanja malicioznog fajla (na primer spomenutog pipe programa koji služi za redirekciju portova) moguće je obrisati binarni fajl. To za istragu znači sledeće, ako se računar isključi (eng. shutdown) izgubljen je fajl koji se nalazio u memoriji i nema više mogućnosti za njegovu kasniju analizu. Ono što forenzičaru može pomoći da se to ne bi desilo je folder "**/proc**". Ovaj folder se zapravo ne nalazi na hard disku već u memoriji i njegov sadržaj upućuje na startovne procese i druge informacije o sistemu [149]. Folderi imenovani brojevima ukazuju na ID startovanog procesa u memoriji. Ovaj podatak može biti dragocen ukoliko je forenzičar ustanovio o kom malicioznom procesu se radi. U tom folderu nalazi se i podfolder "**fd**" koji sadrži sve otvorene fajlove koji se odnose na taj maliciozni proces. Na primer, zlonamerni korisnk je upotrebio alat sniffer za prikupljanje šifara na sistemu, alat je startovao proces sa ID 666. To znači da će forenzičar moći da dobije dokaze u folderu "**/proc/666**" i u folderu "**/proc/666/fd**", gde će naći reference koje ukazuju na fajlove otvarane od strane samog alata sniffera, tako i fajla u kome su se smeštali prikupljani pasvordi.

Treba napomenuti da ono na šta forenzički odgovor "uživo" ne može dati adekvatne rezultate, ali može dati dobru predstavu o onom šta se desilo, dodatne analize moguće je uraditi sa mrežnom forenzikom, a kasnije forenzičkom duplikacijom, post-mortem forenzikom (analiza fajlova : slika, audio video fajlova, arhiva i dokumenta) što izlazi iz okvira ovog rada.

Cilj ovog rada je da se kroz forenzički odgovor "uživo", ukaže na one elemente koji mogu ugroziti bezbednost sistema ili omogućiti njegovu ranjivost. Takođe ovaj rad ima za cilj da kroz prikaz ranjivosti difoltno instaliranih Windows i Linux sistema (koji je prikazan u poglavlju 4.3), ukaže na potencijalne bezbednosne pretnje i preporuče adekvatne mere zaštite, realizujući time preventivnu zaštitu. Zaštita sistema, zapravo, obuhvata prevenciju sa detekcijom i odgovorom na incidentnu/ protivpranu aktivnost. Prevencija podrazumeva kontrolu pristupa, enkripciju i fajervole, dok odgovor na incident podrazumeva detekciju upada i rukovanje protivpravnim aktivnostima od strane forenzičara. Dakle, ovaj rad opisuje mesto gde se dodiruje forenzički odgovor i zaštita operativnog sistema i rezultati iz ovog rada mogu da smanje potrebno vreme za zaštitu, jer vreme zaštite obuhvata vreme detektovanja i vreme odgovora.

3.3 SOFTVERSKI FORENZIČKI ALATI ZA INICIJALNI ODGOVOR I ALATI ZA OPORAVAK PODATAKA I PARTICIJA

3.3.1 Alati inicijalnog odgovora za Windows sisteme

Tabela 9. Forenzički alati za inicijalni odgovor na Windows sistemima

Ime alata	Namena	Izvor
date i time	Prikazuje datum i vreme na sistemu	Implementirano u Windows OS

cmd.exe	Komandno okruženje za Windows operativne sisteme NT/2000/2003//2008/XP/Vista/7.	Implementirano u Windows OS.
psloggedon	Alat koji prikazuje sve povezane korisnike na sistem (lokalne i one koji koriste deljene resurse).	Dolazi u sklopu pstools-a i dostupno je na: http://technet.microsoft.com/en-us/sysinternals/bb896649.
logonsessions	Alat koji prikazuje detalje u vezi sa postojećim sesijama, tip autentifikacije, aktivne procese i tip logovanja korisnika na system.	Dostupno na: http://technet.microsoft.com/en-us/sysinternals/bb896769.aspx
net session	Prikazuje ime udaljenog korisnika koji koristi deljene resurse i IP adresu. Da bi komanda radila mora se koristiti kao korisnik sa administratorskim pravima.	Implementirano u Windows OS.
net accounts	Daje prikaz postavki naloga.	Implementirano u Operativni system.
net file	Daje prikaz otvorenih fajlova od strane udaljenih korinsika.	Implementirano u Operativni system.
net share	Daje prikaz lokalno deljenih resursa dostupnih na mreži.	Implementirano u Operativni system.
net start	Prikazuje spisak servisa i njihove statuse	Implementirano u Operativni system.
net use	Prikazuje udaljene deljene resurse sa kojima je sistem trenutno povezan.	Implementirano u Operativni system.
net user	Daje spisak svih korisničkih naloga.	Implementirano u Operativni system.
net view	Daje prikaz računara u lokalnom domenu.	Implementirano u Operativni system.
Route print	Daje prikaz ruting tabele na lokalnom sistemu.	Implementirano u Operativni system.
netusers	Prikazuje detalje vezane za poslednje vreme logovanja korisnika na sistem.	Dostupno je na : http://www.systemtools.com/cgi-bin/download.pl?NetUsers
rasusers	Prikazuje listu korisnika na domenu ili lokalno na server koji imaju privilegije udaljenog pristupa preko Routing and Remote Access-a na server.	Sastvani je deo Resource Kit utility-a za servere Windows NT, 2000, 2003, 2008.
netstat -anr	Izlistava sve aktivne portove TCP i UDP (koji su u režimu slušanja) i trenutne konekcije sa tim portovima.	Implementirano u Operativni system.
fport	Izlistava sve otvorene TCP/IP I UDP i mapira ih prema aplikaciji koja je vlasnik tog porta. Služi za brzo identifikovanje nepoznatih otvorenih portova i aplikaciju koja je povezana sa tim portom.	Kompatibilna je sa Windows NT/2000/XP http://www.mcafee.com/us/downloads/free-tools/fport.aspx
Pslist	Izlistava i daje detaljan opis svih startovanih procesa na sistema.	Dolazi u sklopu pstools-a : http://technet.microsoft.com/en-us/sysinternals/bb896649
ListDLLs	Izlistava sve DLL biblioteke koje su učitane u procese u sistemu. Alat omogućava listanje svih dll biblioteka u svim procesima, samo u određenom procesu ili lista procese	http://technet.microsoft.com/en-us/sysinternals/bb896656

	sa određenom dll bibliotekom.	
nbtstat -c	Svakom računaru, koji je konfigurisan sa Netbios-om, dodeljuje se jedinstveno ime sa kojim komunicira sa ostalim računarima u mreži. Daje informacije o statistici NetBt protokola, lokalnu i udaljenu tabelu sa NetBios imenima i keširana Netbios imena koja traju samo određeni period npr. 10 minuta. Te informacije pripadaju nestabilnim (eng. volatile) podacima. Tako da ovim alatom možemo prikupiti informacije iz keša koje mogu pokazati konekcije koje su postojale na ispitivanoj mašini. Sa parametrom -c prikazuje trenutni NetBIOS keš koji sadrži imena udaljenih računara i IP adrese.	Implementirano u Windows Operativni system.
arp -a	Mapira MAC adrese u IP adrese sistema sa kojima ima komunikaciju.	Implementirano u Windows Operativni system.
at	Daje prikaz odloženih komandi ili operacija na sistemu koje treba da se izvrše.	Implementirano u Operativni system.
kill	Prekida process.	Sastvani je deo Resource Kit utility-a za servere Windows NT, 2000, 2003, 2008.
md5sum.exe	Kreira MD5 heš vrednost za određeni fajl.	Win9x/ME/NT/2000/XP/Vista/7 http://www.pc-tools.net/win32/md5sums/
sha256sum.rexe	Kreira SHA256 heš vrednost za određeni fajl.	http://www.labtestproject.com/files/win/sha256sum/sha256sum.exe
rmtshare	Može prikazati i kreirati deljene foldere na udaljenom računaru.	Sastvani je deo Resource Kit utility-a za servere NT, 2000, 2003, 2008 ali nije kompatibilan sa njihovim x64 bitnim verzijama.
nc.exe	Netcat Obezbeđuju kanal za komunikaciju između dva sistema.	http://netcat.sourceforge.net/, http://www.downloadnetcat.com/, http://nmap.org/ncat/
cryptcat	Obezbeđuje šifrovan kanala za komunikaciju između dva Sistema.	http://sourceforge.net/projects/cryptcat/files/
PsLogList	Iščitava sadržaj iz event loga.	Dolazi u sklopu pstools-a : http://technet.microsoft.com/en-us/sysinternals/bb896649
ipconfig	Prikazuje konfiguracione informacije postojećih interfejsa na sistemu.	Implementirano u Operativni system.

PsInfo	Prikazuje informacije o lokalnom sistemu.	Dolazi u sklopu pstools-a : http://technet.microsoft.com/en-us/sysinternals/bb896649
PsFile	Prikazuje fajlove koji su otvoreni sa udaljenog sistema.	Dolazi u sklopu pstools-a : http://technet.microsoft.com/en-us/sysinternals/bb896649
PsService	Prikazuje status konfiguraciju i zavisnost od nekog servisa (procesa) i omogućava kontrolu servisa (startovanje, stopiranje, pauziranje, ponovno pokretanje i restartovanje).	Dolazi u sklopu pstools-a : http://technet.microsoft.com/en-us/sysinternals/bb896649
Volume_dump.exe	Alatka za prikupljanje informacija o drajvovima na sistemu i prikazuje USN journals informacije.	Dolazi u sklopu Forensic Acquisition Utilities (FAU) paketa dostupnog na: http://gmgsystemsinc.com/fau/03ddecb5-8262-4022-aaff-6559424ff8fc/fau-1.3.0.2390a.zip
dd.exe	Linux alatka prilagođena za Windows čiji je autor George Garner. Svrha ovog programa jeste konverzija i kopiranje fajlova (kopira zadati ulazni fajl u određeni izlazni fajl uz moguće konverzije).	Dolazi u sklopu Forensic Acquisition Utilities (FAU) paketa dostupnog na: http://gmgsystemsinc.com/fau/03ddecb5-8262-4022-aaff-6559424ff8fc/fau-1.3.0.2390a.zip
ntlast	Prikazuje informacije iz bezbednosnih logova na sistemu	Dostupno na http://www.mcafee.com/us/downloads/free-tools/ntlast.aspx
auditpol	Ovaj alat može da prikazuje i vrši izmenu trenutnih sistemskih i korisničkih bezbednosnih postavki.	Sastavni je deo Resource Kit utility-a za servere NT, 2000, 2003, 2008 ali nije kompatibilan sa njihovim x64 bitnim verzijama.
doskey	Prikazuje listu izvršenih komandi na sistemu u okviru cmd.exe šela.	Implementirano u Operativni system.
uptime	Prikazuje vreme neprekidnog rada računarskog sistema.	http://support.microsoft.com/kb/232243
Pwdump6	Dump heš vrednosti iz SAM baze sa ciljem oporavka šifri.	http://www.foofus.net/~fizzgig/pwdump/
dumpel	Dump logova na NT i Win 2000.	Sastvani je deo Resource Kit utility-a za servere Windows NT, 2000.

3.3.1 Windows Alati Za oporavak podataka

Forenzički alati za oporavak podataka omogućavaju forenzičarima pristup obrisanim informacijama ukoliko one nisu prepisane drugim informacijama. Ukoliko su prepisane još uvek je moguć njihov oporavak, ali sa specijalizovanom labaratorijskom opremom [88]. Ovi alati za oporavak podataka su generalno limitirani jer se oslanjaju na fajlove koji imaju netaknuta zaglavlja. Kada se prikupljaju podaci iz slek prostora koji sadrži fragmente fajlova, ti fragmeti mogu biti oporavljeni, ali retko mogu biti rekonstruisani u kompletne fajlove. Kada mali fajl prepisuje veliki fajl, moguće je oporaviti veći deo velikog fajla iz slek prostora. Takođe, lakše je oporaviti tekstualne podatke, jer se lakše mogu prepoznati i uočiti prilikom oporavka.

Najznačajnije forenzičke alatke sa kojima je moguć proces oporavka podataka na Windows operativnim sistemima prikazani su u tabeli 10. i biće opisani u nastavku rada.

Tabela 10. Forenzički alati za oporavak podataka na Windows operativnim sistemima

Ime alata	Podržana verzija Microsoft Windows OS[375]
Undelete	Windows server 2008, Windows server 2003**,** Windows 8, Windows 7, Window Vista, Windows XP (ne podržava Windows Vista Business i Vista Enterprise)
Active@ UNDELETE	Windows XP, Windows Vista, Windows 7, Windows 8, Windows server 2003, Windows server 2008.
Active@ UNERASER	Windows 8, Windows 7, Windows Vista, Windows, XP, Windows 95, Windows 98, Windows Me, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows NT 4.0 Workstation, Windows NT 4.0 Server, MS-DOS / PC-DOS.
BadCopy pro	Windows 9x, Windows Me, Windows 2000, Windows NT, Windows XP, Windows 2003, Windows Vista, Windows 7.
DiskInternals Uneraser	Windows 2000, Windows XP, Windows 2003, Windows 2008 Server, Windows Vista, Windows 7, Windows 8.
Edata Unerase	Windows 7, Windows Vista, Windows ME, Windows NT, Windows 2000, Windows XP, Windows 2003
Easy-Undelete	Windows 95OSR2, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista
File Recover	Windows XP SP3, Windows Vista, Windows 7, Windows 8
File-saver	Windows 95, Windows 98, Windows NT, Windows 2000, Windows ME, Windows 2003, Windows XP, Windows Vista and Windows 7
File scavenger	Windows 8, Windows 7, Windows Vista, Server 2012, Windows 2008, Windows 2003, Windows 2000, Windows NT, Windows XP
Handy recovery	Windows 9x, Windows Me, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 7
Mycroft	Windows 95, Windows 98, Windows ME, Windows XP, Windows 2000, Windows NT
PC INSPECTOR File Recovery	Windows 95, Windows 98, Windows ME, Windows NT, Windows 2000, Windows XP
Recover my files	Windows 2003, Windows XP, Windows

[375] Do kraja pisanja rada moguće je proširenje kompatibilnosti od strane proizvođača programa za navedene programe kako za verziju Windows-a tako i za tip (32-bini ili 64-bitni).

	Vista, Windows 7, Windows 8
Recover4all Professional	Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000, Windows ME, Windows 98, Windows 2008, Windows 2003 Server
Search and recover	Windows 8, Windows 7, Windows Vista, Windows XP, Windows 2000
WinUndelete	Windows 98, Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Windows 7, Windows 8

Undelete[376] - U stanju je da oporavi podatke koji se ne mogu izvući iz korpe za otpatke (eng. Recycle bin). Tipovi podataka koji se mogu oporaviti koristeći undelete alat su : deljeni podaci (eng. shard files), prethodne verzije Microsoft office fajlova, veliki fajlovi koji nisu mogli da uđu u korpu za otpatke, određeni fajlovi koji se kreiraju i brišu od strane aplikacija i fajlovi izbrisani korišćenjem komandne linije. Podržava sledeće operativne sisteme (32 bitne i 64 bitne): Windows server 2008, Windows server 2003**,** Windows 8, Windows 7, Window Vista, Windows XP. Ne podržava Windows Vista Business i Vista Enterprise.

Active@ UNDELETE[377]**-** U stanju je da oporavi podatke koji su obrisani iz korpe za otpatke, formatirane podatke sa hard diska, floppy diska, sa basic i dynamic Volume-a, sa hardverskog i softverskog RAID niza (RAID0 i RAID5). Podržava kompresovane, kriptovane, i fragmentirane fajlove. Pored hard diskova program ima podršku iz za oporavak podataka sa prenosnih uređaja kao što su CompactFlash, Secure Digital, SmartMedia, Sony memory stick, Zip drajv i USB drajv. Moguće je oporaviti obrisane podatke sa sledećih fajl sistema FAT12, FAT16, FAT32, NTFS, NTFS5 i EFS. Podržava sledeće operativne sisteme (32 bitne i 64 bitne) Windows XP, Vista, Windows 7, Windows 8, Windows server 2003, Windows server 2008

Active@ UNERASER[378] **-** U stanju je da oporavi podatke (fajlove i foldere) koji su obrisani na FAT12, FAT16, FAT32, NTFS fajl sistemu. Moguće je oporaviti fajlove sa obrisanih ili formatiranih particija. Podržava kompresovane, kriptovane, i fragmentirane fajlove. Nije neophodno instaliranje na sistem već se može pokrenuti i sa USB prenosnog drajva i ima podršku za DOS sisteme. Podržava sledeće operativne sisteme: Windows 8, Windows 7, Windows Vista, Windows, XP, Windows 95, Windows 98, Windows Me, Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows NT 4.0 Workstation, Windows NT 4.0 Server, MS-DOS / PC-DOS.

BadCopy pro[379]- Ova alatka služi za oporavak izgubljenih i oštećenih podataka sa floppy drajva, CD-R, CD-RW, DVD-ROM, DVD+/-R/W, Digial Media, zip drajva i diskova. Ne upisuje podatake na originalan disk, već snima oporavljene informacije u zadati direktorijum. U stanju je da oporavi podatke iz sesija sa višesesijskih CD-a i DVD-a. Podržava sledeće operativne sisteme Microsoft Windows 9x/Me/2000/NT/XP/2003/Vista/7.

DiskInternals Uneraser[380] - Ovaj alat služi za oporavak obrisanih fajlova (dokumenti, fotografije, mp3 i zip), foldera i oštećenih diskova. Uspeva oporaviti i izgubljene fajlove koji su posledica virusnog napada ili zlonamernog korisničkog ponašanja. Od uređaja podržava SD, microSD, Compact Flash, SONY Memory Stick, xD and MMC. USB flash drives. Od fajl sistema podržava NTFS, exFAT, FAT12/16/32, Ext2, Ext3, Ext4, Reiser, Reiser4, UFS i

[376] http://www.condusiv.com/home-use/undelete/home-edition/?SID=8&rid=106504, 23.04.2012
[377] http://www.active-undelete.com/ , 24.02.2013.
[378] http://www.uneraser.com/
[379] http://www.jufsoft.com/badcopy/
[380] http://www.diskinternals.com/uneraser/

skrivene NTFS FAT12/16/32, kao i kompresovan NTFS i NTFS5 i šifrovan NTFS5. Prepoznaje lokalizovana imena sa podrškom za duge nazive u FAT12, FAT16 i FAT32. Podržava sledeće operativne sisteme Microsoft Windows 2000, XP, 2003, 2008 Server, Vista, Windows 7, 8.

Edata Unerase[381] - Ovaj alat služi za oporavak izbrisanih fajlova, fajlova koji su izbrisani iz korpe za otpatke kao i izgubljenih podataka nakon formatiranja hard diska, nakon virusnih infekcija, neplaniranog gašenje računara ili nakon otkaza programa. Ima dva metoda pretrage. Brzo skeniranje fajl sistema koji traži samo obrisane fajlove i kompletno skeniranje koji pretražuje obrisanje i izgubljene fajlove. Od uređaja podržava hard diskove, floppy drajvove, Memory sticks, USB flash drajvove, Zip drajvove, Compact Flash kartice, SmartMedia kartice. Od fajl sistema podržava FAT12/16/32 and NTFS. Podržava sledeće operativne sisteme Microsoft Windows 7/Vista/ME/NT/2000/XP/2003.

Easy-Undelete[382] - Ovaj alat može oporaviti nestale fajlove i foldere na NTFS, FAT32, FAT16 i FAT12 fajl sistemima i može prikazati izgled slike (Jpeg, PNG, TIFF, GIF, BMP, ICO, TGA, PCX, WBMP, PNM) ili binarnog fajla pre oporavka (heksadecimalni prikaz). Podržava hard diskove, memorijske kartice, USB flash drajvove, Zip drajvove. Pokreće se bez instaliranja. Podržava sledeće operativne sisteme Microsoft Windows 95OSR2, 98, ME, NT, 2000, XP, 2003 and Vista.

File Recover[383] - Ovaj alat može oporaviti obrisane fajlove, fajlove koji su nestali prilikom pražnjenja korpe za otpatke, kao i oporavak fajlove nakon akcija brisanja koja zaobilaze korpu za otpatke (SHIFT+DELETE, brisanje iz komandnog okruženja, brisanje prevelikih fajlova i korišćenje programa za brisanje koji zaobilaze korpu za otpatke). Ukoliko je fajl parcijalno prepisan, ovaj program će pokušati rekonstrukciju preostalog sadržaja. Moguće je korišćenje batch moda (oporavak više fajlova odjednom) prilikom oporavka podataka. Podržava hard diskove, floppy drajvove, memorijske kartice, USB flash drajvove, Zip drajvove. Podržava FAT16, FAT32, ExFAT i NTFS fajl sisteme. Podržava sledeće operativne sisteme Microsoft Windows XP SP3 (samo 32bit verziju), Microsoft Windows Vista (32bit i 64bit verzije), Microsoft Windows 7 Microsoft Windows 8 (32bit i 64bit verzije).

File-saver [384] - Ovaj alat služi za oporavak fajlova obrisanih od strane nekog malicioznog programa ili onih koji su ispražnjeni iz korpe za otpatke. Poseduje mogućnost provere uspešnosti oporavka izbrisanih fajlova. Ima podršku za oporavak neograničenog broja fajlova. Podržava hard diskove, floppy diskove i kartice digitalnih kamera. Podržava FAT16, FAT32, ExFAT i NTFS fajl sisteme. Od operativnih sistema podržava Microsoft Windows 95, Windows 98, Windows NT, Windows 2000, Windows ME, Windows 2003, Windows XP, Windows Vista and Windows 7.

File scavenger[385] - Ovaj alat služi za oporavak digitalnih fotografija sa većine medija. Takođe moguće je da oporavi fotografije koje su oštećene ili uništene od strane virusa ili slučajnim brisanjem iz Windows explorera, korpe za otpatke, iz komandnog okruženja. Ima podršku za kompresovane diskove, osnovnem i dinamičke diskove. Moguće je čak oporavati formatirane drajvove, oštećene raid nizove, oštećene particije (preko funkcije Defunct Volume search) i oporavak podataka sa oštećenih diskova koji sadrže loše sektore ili oštećene particije. Program je moguće pokrenuti sa floppy diska ili usb prenosnog drajva ili ga instalirati na sistem. Od operativnih sistema podržava Microsoft Windows 8, 7, Vista, Server 2012/2008/2003/2000, NT i XP (32- and 64-bit).

[381] http://www.octanesoft.com/data_recovery.html, 24.04.2012
[382] http://www.easy-undelete.com/, 24.04.2012
[383] http://www.pctools.com/file-recover/, 24.04.2012
[384] http://www.recovery-magic.com/undelete/affiliate.aspx, 24.04.2012
[385] http://www.quetek.com/prod02.htm, 24.04.2012

Handy recovery[386] - Ovaj alat omogućava oporavak fajlova sa hard diskova i floppy diskova kao i slika sa medija CompactFlash, SmartMedia, Multimedia, Secure Digital. Program može oporaviti fajlove koji su obrisani, oštećeni malicioznim programom, padom sistema, programskom greškom i može oporaviti podatke nakon formatiranja particije. Oporavlja podatke izbrisane iz korpe za otpatke kao i kompresovane i šifrovane na NTFS-u. Pretraživanje izbrisanih fajlova je slično kao kod Windows Explorera. Moguće je snimanje fajlova na druge diskove uz oporavak čitavih stabla foldera. Od fajl sistema podržava FAT12/16/32/64(ExFAT), NTFS/NTFS 5, EFS, HFS/HFS+. Od operativnih sistema podržava Microsoft Windows 9x/Me/NT/2000/XP/2003/Vista/Win7.

Mycroft[387] - Ovaj alat je vrlo brz i efikasan pretraživač koji može biti jako koristan digitalnom forenzičaru. Ova alatka pomaže digitalnom forenzičaru da izvrši brzu pretragu za određenim pojmovima nakon zaplene hard diska. Ono što je značajno istaći jeste da pre započinjanja same pretrage ovaj program zaključava hard disk da bi sprečio bilo kakve promene informacija na ispitivanom hard disku. Prema dostupnim podacima brzina pretrage iznosi 5MB/sec [56].

PC INSPECTOR File Recovery[388] - Ova alatka može biti od koristi u slučaju oštećenja boot sektora, obrisanih fajlova ili particija. Od particija podržava FAT 12/16/32 i NTFS. Moguće je oporavak podataka sa originalnim vremenom i vremenskim pečatom. Moguć je oporavak fajlova na mrežne drajvove. U stanju je da oporavi podatke koji su bez hedera. Od operativnih sistema podržava WINDOWS 95/98/ME/NT/2000/XP.

R-Undelete[389] - Ovaj alat može oporaviti fajlove sa bilo kog validnog logičkog diska vidljivog od strane Operativnog sistema. Može oporaviti fajlove sa oštećenih ili izbrisanih particije. Oporavlja podatke koji su brisani bez slanja u korpu za otpatke, koji su izbrisani iz korpe za otpatke, koji su obrisani od strane malicioznog programa ili nakon naglog isključenja OS (nestanak struje). Podržava kreiranje image-a, što je korisno u slučaju da hard disk sadrži bad sektore koji narastaju. Može oporaviti podatke sa sledećih fajl sistema : FAT (FAT12, FAT16, FAT32, exFAT), NTFS, NTFS5. Od operativnih sistema podržava Windows 2000 /XP /2003 /Vista /2008 /Win7 /Win8.

Recover my files[390] - Pomoću ove alatke moguće je oporaviti obrisane podatke koji su ispražnjeni iz korpe za otpatke, podatke koji su formatirani ili oštećeni na hard disku usled aktivnosti malicioznih programa ili nakon iznenadnog isključenja računara. Moguće je oporaviti dokumenta fotografije, video i muzičke fajlove i emal-ove. Podržava hard diskove, memorijske kartice, USB flash drajvove, Zip drajvove, floppy diskove i druge prenosne medije. Može oporaviti podatke sa sledećih fajl sistema : FAT (FAT12, FAT16, FAT32), NTFS, NTFS5. Od operativnih sistema podržava Windows 2003/XP/Vista/Windows 7/Windows 8.

Recover4all Professional[391] - Ova alatka može oporaviti podatke slučajno obrisane na Windows sistemu bez obzira da li su podaci izbrisani iz korpe za otpatke ili su obrisani direktno. Da bi se sprečilo prepisivanje fajlova, ova alatka ne zahteva instalaciju i može biti pokrenuta direktno sa floppy diska USB diska ili flash drajva. Ima podršku za oporavak svih tipova dokumenata, slika, muzičkih i video fajlova. Podržava NTFS i FAT fajl sisteme kompresovane drajvove i fajlove, sve RAID nivoe kao i GPT[392]. Ima podršku za duža imena. Od uređaja podržava hard diskove, prenosne diskove, Zip drajvove, floppy diskove, memorijske kartice (CompactFlash, SmartMedia, SecureDigital, Memory Stick). Od operativnih sistema podržava Windows 8/7/Vista/XP/2000/ME/98/2008 and 2003 Server.

---

[386] http://www.handyrecovery.com/, 24.04.2012

[387] http://www.dibsusa.com/, 24.04.2012

[388] http://www.pcinspector.de/default.htm?po=1&language=1, 24.04.2012

[389] http://www.r-undelete.com/, 24.04.2012

[390] http://www.recovermyfiles.com/, 24.04.2012b

[391] http://www.recover4all.com/, 24.04.2012

[392]GUID Partition Table, više o GPT može se naći na Microsoftovom sajtu
http://msdn.microsoft.com/en-us/library/Windows/hardware/gg463525.aspx , pristupljeno 04.03.2012.

Search and recover[393] - Ova alatka omogućuje istraživaču da brzo oporavi obrisane podatke, foldere, muzičke i video fajlove, slike, programe, Web strane, e-mail poruke u Microsoft Outlook i Outlook express klijentima, Netscape mail, Thunderbird i Eudora. Poseduje proširenu podršku za oporavak Outlook podataka (oporavak obrisanih task-ova, kontakata, beležnica (eng. notes), i dnevnika). Omogućuje snimanje oporavljenih podataka direktno na CD ili DVD. Da bi sprečio gubitak podataka, ovaj alat može se pokrenuti sa CD-a. Moguće je oporaviti podatke sa hard diskova, memorijskih kartica, flash drajvova, CD-a, DVD-a. Od operativnih sistema podržava Windows8/7/Vista/XP/2000 (32-bit i 64-bit)

WinUndelete[394] - Ova alatka omogućava oporavak podataka sa hard diskova, floppy diskova, Zip drajvova, Jaz diskova, prenosnih diskova, memorijskih kartica. Može oporaviti podatke nakon pražnjenja korpe za otpatke kao i one podatke koji nisu ni prosledjivani korpi za otpatke (obrisani iz DOS komandnog okruženja, SHIFT+DEL), podatke obrisanje od strane malicioznih programa. Podržava FAT12/16/32, NTFS i NTFS 5. Može prikazati slike, običan tekst (eng. plain text) i Microsoft dokumente pre oporavka. Od operativnih sistema podržava Windows® 98/2000/2003/2008/XP/Vista/7/8 (32-bit & 64-bit)

3.3.2 Linux alati za inicijalni odgovor

Tabela 11. Forenzički alati za inicijalni odgovor na Linux sistemima

Ime alata	Namena	Izvor
nc	Netcat obezbeđuju kanal za komunikaciju između dva sistema.	http://netcat.sourceforge.net/
dd, dcfldd	Svrha ovog programa jeste konverzija i kopiranje fajlova (kopira zadati ulazni fajl u određeni izlazni fajl uz moguće konverzije).	DD implementiran u system, a poboljšana verzija dostupna na: http://dcfldd.sourceforge.net/
date	Prikazuje datum i vreme na sistemu.	Implementirano u system.
cat	Služi sa prikaz i povezivanje fajlova.	Implementirano u system.
pcat	Može dati prikaz svih procesa koji se nalaze u memoriji.	Sastavni je deo TCT kompleta alata dostupnog na : http://www.porcupine.org/forensics/tct.html
netstat	Daje prikaz trenutno aktivnih mrežnih konekcija.	Implementirano u system.
netstat -nr	Daje prikaz kernel IP ruting tabele.	Implementirano u system.
arp	Daje prikaz ARP keša na sistemu..	Implementirano u system.
route	Takođe daje prikaz IP ruting tabele	Implementirano u system.
route -Cn	Daje prikaz Ruting keša.	Implementirano u system.
dmesg	Daje informacije o hardveru na sistemu koje dobija od strane ring bafera jezgra.	Implementirano u system.
ls	Izlistava sadržaj direktorijuma.	Implementirano u sistem
fdisk -l /dev/???	Fdisk je alatka koja služi za rad sa particijama na Linux. Pokrenuta sa svičem -l i određenim uređajem daje informacije o particijama.	Implementirano u system.
script	Pomoću ove komande moguće je dokumentovanje pokrenutih komandi.	Implementirano u system.
ps -auxwww	Izlistava sve startovane procese prema pripadajućem korisniku.	Implementirano u system.
memdump	Pomoću ove alatke moguće je uraditi dump memorije.	Dostupan TCT sajtu: http://www.porcupine.org/forensics/tct.html
df	Daje prikaz montiranih uređaja, tačku montiranja, veličinu, rasapoloživ kapacitet i zauzeće uređaja.	Implementirano u system.
showmount	Daje prikaz NFS deljenih resursa na server.	Implementirano u system.

[393] http://www.iolo.com/search-and-recover/, 24.04.2012
[394] http://www.winundelete.com/, 24.04.2012

3.3.2 Linux alati za oporavak podataka

E2undel[395] - Ova alatka može se primeniti na Linux operativnom sistemu sa ext2 fajl sistemom. Sastoji se od biblioteke koja može oporaviti obrisane fajlove prema imenu. Na sistemu potrebna su samo prava čitanja. Nakon oporavka podataka treba proveriti tri dela fajla : sadržaj fajla, metadata podatke o fajlu (datum i vreme kreiranja, vlasništvo i prava,), i ime fajla. Ne podržava ext3, ReiserFS, XFS i JFS.

R-Linux[396] - Ova alatka može se primeniti na Linux operativnom sistemu sa ext2, ext3, ext4 fajl sistemom sa kernelom 2.6 i iznad. Ova alatka prepoznaje lokalna imena i može sačuvati oporavljene podatke na disku koji je vidljiv od strane operativnog sistema. Jednostavan je za upotrebu, oporavlja podatke sa diska koji ima loše sektore[397], podatke koji su obrisani od strane malicioznog programa, nestali podaci usled krahiranja sistema ili iznenadnog isključenja. Ova alatka može pomoći ukoliko je došlo do promene ili oštećenja particije na sistemu tako što će pokušati pronaći prethodnu particiju i oporaviti podatke koji se na njoj nalaze.

Stellar Phoenix Linux Data Recovery[398] - Ova alatka može oporaviti izgubljene ili nepristupačne podatke sa Linux fajl sistema EXT4, EXT3, EXT2, i Windows FAT12, FAT16, FAT32 fajl sistema. Može oporavljati fajlove, direktorijume i particije kao posledica slučajnog formatiranja, gubitka particije, oštećenja fajlova ili delovanje malicioznog programa. Poseduje automatizovani čarobnjak koji istraživača vodi kroz tri koraka : procena, analiza i oporavak. Ova alatka poseduje samo funkcije čitanja. Oporavljeni podaci mogu da se smeštaju na prenosne uređaje.

3.3.3 Oporavak obrisanih Windows i Linux particija

Oporavak obrisanih particija jeste proces procene i izvlačanje obrisanih particija. Ovaj proces je jako važan kada je reč o oporavljanju podataka. Oporavljanje može da podrazumeva oporavljanje particija koje su obrisane slučajno, od strane virusa, usled otkazivanja programa, ili čak sabotaže. U nastavku će biti prikazani programi koji služe za oporavak particija.

Acronis Recovery expert[399] - Ova alatka je sastavni deo paketa Acronis Disk Director Suite koji služi za kompletnu zaštitu korisničkih podataka omogućujući oporavak obrisanih ili izgubljenih particija. Takođe štiti sistem o d hardverskih i programskih grešaka i malicioznih napada. Može raditi nezavisno tako što se pokreće sa butabilnog CD-a ili diskete omogućujući oporavak particija čak i ako sistem ne može da se bootuje. Podržava sledeće fajl sisteme FAT16, FAT32 ,NTFS , Ext2, Ext3, ReiserFS3, Linux SWAP. Od operativnih sistema podržava (x86 i x64) Windows 7, Windows Vista, Windows XP.

Active@ Disk image[400] - Uz pomoć ove alatke moguće je uraditi bekap i oporavak kako celog hard diska tako i pojedinačnih FAT, NTFS particija. Ono što izdvaja ovaj alat jeste mogućnost pregleda fajlova i foldera unutar napravaljenog imidža pre oporavka podataka. Može se pokrenuti sa Dos diskete ili CD-roma, DVD-a ili USB flash . Daje prikaz kompletnog HDD-a, particija i informacije o imidžu diska. Mogućnost kreiranja kompresovanog i nekompresovanog raw imidža fizičkog hard diska (sector by sector). Od

[395] http://e2undel.sourceforge.net/
[396] http://www.r-tt.com/free_Linux_recovery/
[397] U ovom slučaju pravio bi se imidž celog hard diska i fajlovi bi se dalje procesirali kroz napravljeni imidž.
[398] http://www.stellarinfo.com/Linux-data-recovery.htm
[399] http://www.acronis.com/homecomputing/products/diskdirector/#requirements
[400] http://www.disk-image.com/

fajl sistema podržava FAT12, FAT16, FAT32, NTFS i HTFS5. Od operativnih sistema podržava Windows 8 / 7 / Vista / Server 2003 / Server 2008 / XP /Small Business Server 2011.

Active@ Partition Recovery[401] - Uz pomoć ove alatke moguće je oporaviti obrisanu particiju (kako primarnu tako i proširenu) samo u slučaju da njena lokacija nije prepisana. Može kreirati bekape MBR, tabele Particija i Volume boot sektore. Može pomoći pri oporavku nesistemskih particija. Takođe, ima mogućnost automatskog korigovanja BOOT.INI fajla i boot sektora da bi sačuvao bootabilnost sistema. Ova alatka može popraviti MBR i održati integritet particije. Podržava diskove veće od 2TB. Od fajl sistema podržava FAT12,FAT16,FAT32,exFAT, NTFS, Apple HFS+, FreeBSD Unix UFS i Linux ExtFs.
Od operativnih sistema podržava (x86 i x64) Windows 2000/XP/Server 2003/2008/Vista/Windows 7/ Windows 8.

DiskInternals Partition recovery[402] - Ova alatka namenjena je za oporavak podataka i particija. Ne zahteva posebne veštine jer program dolazi sa vodičem korak po korak (eng. wizard step-by-step). Oporavlja podatke sa oštećenih, obrisanih i reformatiranih particija. Ovaj program skenira svaki sektor na disku. Takođe u stanju je da oporavi podatke sa virtuelnih diskova VMware[403] (uključujući imidže koji su smešteni na udaljenom ESX serveru), Oracle VirtualBox[404], Microsoft VirtualPC[405], and Parallels[406], bez potrebe instalacije virtuelne mašine. Oporavljene podatke program može narezati na CD ili DVD ili exportovati putem FTP-a. Od fajl sistema podržava FAT12, FAT16, FAT32, VFAT, NTFS, NTFS4, NTFS5, Ext2, Ext3. Od operativnih sistema podržava Microsoft Windows 95, 98, ME, NT, 2000, XP, 2003 Server, Vista, Windows 7 i 2008 Server.

GetDataBack[407] - Ova alatka može oporaviti izgubljene podatke, obrisane, oštećene, formatirane ili reformatirane. Takođe, može oporaviti oštećene particije na hard disku, oštećen boot sektor kao i oporavak FAT/MFT[408]. Podržava Unicode[409] što omogućava oporavak fajlova sa imenima enkodovanih sa nestandardnim setom karaktera (kao na primer japanski, kineski , korejski, ruski i grčki set karaktera). Ima podršku za sve FAT i NTFS fajl sisteme. Od operativnih sistema podržava Windows 95, 98, ME, NT, 2000, XP, 2003, Vista, Windows 7, or Windows 8.

Testdisk[410] - Ova alatka može oporaviti izgubljene particije i omogućiti povratak butabilnosti diska kada on postane nebutabilan kao posledica neke programske neispravnosti, aktivnosti zlonamernog programa ili ljudske namera ili greške. Može oporaviti MFT, boot sektore kao i FAT tabelu. Od fajl sistema podržava FAT12/FAT16/FAT32, exFAT, NTFS, ext2/ext3/ext4. Primena ove alatke u različitim digitalno forenzičkim ispitivanjima imidža prikazana je na sajtu CGIsecurity[411]. Od operativnih sistema podržava DOS, Windows 95, Windows 98, Windows (NT4, 2000, XP, 2003, Vista, 2008, Windows 7 (x86 & x64), Linux, FreeBSD, NetBSD, OpenBSD, SunOS i MacOS X.

---

[401] http://www.partition-recovery.com/
[402] http://www.diskinternals.com/partition-recovery/
[403] http://www.vmware.com/
[404] https://www.virtualbox.org/
[405] http://www.microsoft.com/Windows/virtual-pc/
[406] http://www.parallels.com/
[407] http://www.runtime.org/data-recovery-software.htm
[408] MFT (eng. Master File Table) predstavlja mesto gde se nalaze informacije o svim fajlovima i direktorijumima u okviru NTFS fajl sistema. Sadrži listu zapisa sa informacijama za pronalaženje podataka na disku kao i njihova vremena i datume kreiranja, poslednjih izmena i poslednjih pristupa.
[409] Preporuka je da se oporavak podataka vrši na minimum Windows XP sistemu, jer Windows 98 i Windos ME ne podržavaju u potpunosti Unicode.
[410] http://www.cgsecurity.org/wiki/TestDisk
[411] http://www.cgsecurity.org/wiki/TestDisk_and_PhotoRec_in_various_digital_forensics_testcase#Digital_Forensics_Tool_Testing_Images

Svi navedeni programi koji se bave oporavkom podataka osim što doprinose prikupljanju dragocenih informacija za forenzičku istragu predstavljaju i veoma važan element u strategiji zaštite samih podataka.

3.4 DIGITALNO FORENZIČKI KOMPLETI ALATA ZA WINDOWS I LINUX SISTEME

U današnje vreme forenzički programi se najčešće koriste za prikupljanje dokaza, kako u krivičnim postupcima, tako i u korporativnim istragama, jer sa jedne strane umanjuju rizike koji mogu nastati sa ispitivanjem medija u njegovom prirodnom okruženju, a sa druge pružaju mogućnost brzog pretraživanja i pregledanja. Pomenuti rizici podrazumevaju izmenu kritičnih metadata podataka kao što su datumski i vremenski pečati pristupanim ili obrisanim fajlovima prilikom forenzičke analaize. Zato mnogi forenzički alata obezbeđuju zaštitu integriteta nad prikupljenim dokazima pomoću heširanja (CRC, MD5, SHA1) da bi se osiguralo da su dokazi koji se iznose pred sudom ostali nepromenjeni nakon prikupljanja. To znači da pravosudni organi prilikom sprovođenja zakona u velikoj meri zavise i od forenzičkih programa kojima se vrši prikupljanje, analiza i očuvanje kritičnih dokaza. Zato je od krucijalne važnosti da se upotrebljavaju samo provereni i bezbedni forenzički alati. Postoji veliki broj radova koji se bave problemima i slabostima koji se odnose na forenziče alate, a značajni su sledeći : Tim Newsham, Chris Palmer i Alex Stamos sa radom "Breaking Forensics Software: Weaknesses in Critical Evidence Collection" [142], Chris Ridder sa radom "Evidentiary Implications of Potential Security Weaknesses in Forensic Software" [162] i Ryan Harris sa radom „Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem"[78].

Digitalno forenzički kompleti alata predstavljaju skup alata koji mogu realizovati više elemenata forenzičkog procesa. To znači da kompletom mogu biti obuhvaćeni procesi pravljenja forenzičkih kopija dokaza i njihova verifikacija, oporavak izbrisanih ili izgubljenih particija ili podataka, dešifrovanje zaštićenih fajlova, analiza podataka, dokumentovanje pronađenih dokaza i kreiranje izveštaja. Postoji preko 150 različitih automatizovanih alata[412] koji se koriste prilikom istrage visokotehnološkog kriminala [162].

Sa aspekta platforme na kojoj rade mogu se podeliti na komplete alata koji rade pod Windows ili Linux operativnim sistemom. Sa aspekta koda kompleti se mogu podeliti na one sa otvorenim kodom i na one koji se licenciraju.U komplete koji rade na Windows operativnom sistemu spadaju : Accessdata FTK, Guidance Encase forensic, Ilook investigator, X-way forensic. U komplete koji rade pod Linux operativnim sistemima spadaju The Sleuth kit, Autopsy, Penguin Sleuth, The Coroner's Toolkit (TCT), Helix. Najvažniji forenzički kompleti biće navedeni u tabeli 12. i biće opisani u nastavku rada.

Tabela 12. Forenzički kompleti alata

Naziv forenzičkog alata	Web sajt	Okvirna cena
ENCASE forensic	http://www.guidancesoftware.com	4000$
ILOOK Investigator	http://www.perlustro.com/	2200$
The Sleuth kit, Autopsy	http://www.sleuthkit.org/	Open Source - besplatan

[412] Videti na http://www.cftt.nist.gov/project_overview.htm . National Institute of Standards and Technology ima program koji se bavi upravo ispitivanjem forenzičkih alata na slabosti.

forensic browser		
AccessData Forensic Toolkit (FTK)	http://www.accessdata.com/	5500$
Penguin Sleuth	http://www.penguinsleuth.org/	Open Source - besplatan
The Coroner's Toolkit (TCT)	http://www.porcupine.org/forensics/tct.html#features	Open Source - besplatan
Helix Live CD	http://www.e-fense.com/helix	Starije verzije su besplatne ali nemaj podršku
Knoppix-STD 0.1	http://s-t-d.org/index.html	Open Source - besplatan
LiveWire Investigator	http://www.wetstonetech.com/cgi-bin/shop.cgi?view,14	9000$
The ProDiscover Family	http://www.techpathways.com	8000$
X-ways Forensics	http://www.x-ways.net/forensics/index-m.html	1500$

3.4.1 ENCASE forensic[413]

Ovaj set alata ujedno predstavlja industrijski standard i kompletno rešenje za digitalnu računarsku istragu baš kao i AccessData FTK. Sa ovim alatom moguće je sprovesti efikasno prikupljanje podataka na forenzički ispravan način tako da se proces može ponoviti i odbraniti pred sudom. Omogućava istraživačima prikupljanje podataka sa velikog broja uređaja, otkrivanje potencijalnih dokaza, kao i izrade detaljnih izveštaja o svojim nalazima održavajući pritom integritet nad dokazima. Dostupne su različite verzije ovog alata koje mogu biti namenjane za privatan sektor ili za pravosuđe (Law enforcement) u zavisnosti od potreba i načina upotrebe.

Kada je reč o prikupljanju podataka, može prikupljati podatke sa servera, radnih stanica i tableta iz RAM memorije ili sa diskova, čuvajući lako izmenjive podatka bilo gde na mreži bez ometanja poslovanja. Podrazumeva sigurnu istragu i analizu prikupljenih podataka preko LAN/WAN mreže sa centralne forenzičke lokacije (na primer kod Enterprise Encase rešenja). Od tipova podataka obuhvata dokumente, slike, Internet artefakte, Web istoriju i keš, rekonstruisanje HTML stranica, chat sesije, kompresovane fajlove, bekap fajlove, log i eventlog fajlove, šifrovane fajlove, fajlove sa RAID-a nizova kao i elektronsku poštu. Podržani formati elektronske pošte su Mbox (Unix), Netscape, AOL (ver 6,7,8,9), Yahoo, MSN Hotmail, Microsoft Outlook i Microsoft Outlook express [20].

Kreira bit-by-bit sliku. Proizveden binarni duplikat identičan je originalu i verifikuje se generisanim heš vrednostima. U stanju je da oporavlja podatke i particije, detektuje obrisane fajlove, vrši analizu potpisa fajlova (eng. file signature) i heš vrednosti, pa čak i iz kompresovanih fajlova i sa nealociranog prostora. Digitalni istgraživači mogu pregledati rezultate nakon što se podaci prikupe. Kada je jednom slika (eng. image) kreirana (podržava VMWARE, DD, Safeback v2), istraživači mogu pretraživati i analizirati više drajvova odjednom. U okviru Encase alata implementirana je NSLR (eng. The National Software Reference Library)[414] bioblioteka sa heš vrednostima poznatih fajlova čime se značajno smanjuje vreme i količina podataka potrebnih za analizu. Prisutna je podrška za prikaz više od 100 fajlova u njihovoj prirodnoj formi, ugrađena je podrška za pregled Registry baze, integrisan je prikazivač za fotografije, a rezultati pregleda mogu da se vide na vremenskoj osi, odnosno kalendaru. Sa bezbednosne tačke gledišta vrši auditing računara u slučaju

[413] https://www.guidancesoftware.com/products/Pages/encase-forensic/overview.aspx
[414] http://www.nsrl.nist.gov/

kompromitovanja napadom zero-day[415] (eng. zero-day attack), a takođe prepoznaje rootkit programe koji se odnose na Windows kernel i sanira njihove posledice.

Poseduje mogućnost programiranja skripti, za ovu alatku, upotrebom Enscript programskog jezika što forenzičarima može pomoći da automatizuje specifične vrste pretraživanja i analize. EnCase uspešno zaobilazi BitLocker zaštitu postavljenu u Vista operativnom sistemu kao i starije PGP zaštite [186]. Generisani izveštaji sadrže listu svih fajlova i foldera, detaljnu listu posećenih URL adresa sa datumima i vremenima pristupa. Takođe pruža detaljne informacije o hard disku kao i detalje o prikupljanju podataka. Za autenfikaciju svih novijih EnCase verzija upotrebljava se USB dongle drive, koji predstavlja ključ sa kojim se program otključava.

3.4.2 ILOOK Investigator[416]

Ilook spada među prve Law enforcement komplete alata u svetu koji se bavi digitalnom forenzikom na Windows sistemima. Do verzije 8 ovaj komplet je bio isključivo namenjen pravosudnim organima kao i vojsci, ali od verzije IX ovaj alat je dostupan i kao komercijalan proizvod. Poseduje sopstveni alat za kreiranje forenzičke kopije ne samo za Intel sisteme, već podržava 18 različitih procesora. U funkciji analize poseduje napredne tehnike pretrage i pregleda slike diska sa kompromitovanog računara. Može da vrši pretraživanje slike diska dobijenih drugim programima za pravljenje forenzičke kopije (bit po bit kopije) kao na primer, Encase imidž fajlove, Safeback imidž fajlove, ISO imidž fajlove, VMware virtuelne disk fajlove. Ima mogućnost kreiranja heš za imidž fajlove CRC32, MD5, SHA1. Podržava veliki broj fajl sistema kao na primer : FAT 12/16/32/32x, VFAT, NTFS 4/5, NTFS 4/5 Compressed, HFS, HFS+, Ext2, Ext3, ReiserFS 1/2/3, SysV-AFS, SysV-EAFS, SysV-HTFS, Novell NWFS, Novell NWFS Compressed, VMDK (VMWare Drive Mount disk), Microsoft Virtual PC disk, CDFS, ISO 9660, ISO 9660, i UDF. Podržava puno UNICODE pretraživanje. Poseduje pretraživanje u različitim modovima (standardna, indeksirana i bulk pretraga). Može vršiti analizu potpisanih fajlova (eng. file signature) i heš vrednosti (podržava CRC32, MD5, SHA1). Poseduje funkciju heš deduplikacije (u slučaju učitavanja više slika odjednom) koja uklanja duplirane fajlove čime se može značajno ubrzati pretraživanje. Može se implementirati i Hashkeeper 417 kreirana od strane U.S. National Drug Intelligence Center (NDIC) 418 ili NIST NSRL [419], baza čime bi se vreme za pretraživanje smanjilo eliminišući poznate fajlove.

Poseduje i granularno izvlačenje fajlova sa kojim možemo da izdvojimo odgovarajući deo fajl sistema za pretragu. Takođe poseduje mogućnost oporavka oštećenih i izbrisanih fajlova kao i Orphaned FAT direktorijuma. Ima ugrađen hex editor sa mogućnošću pretraživanja. Takođe, događaje iz Event viewer-a može prikazati na vizuelnoj mapi prema tipu događaja na vremenskoj osi.

Podržani formati za rekonstrukciju elektronske pošte i attachmenta su MBox, mbx, PST, OST, EML, EMLX, DBX, AOL, Lotus NOTES. Poseduje naprednu tehniku oporavka elektronske pošte iz MS Outlook-a. Takođe, može uraditi i rekonstrukciju Internet keša. Poseduje pretržaivač registarske baze sa pronalaženjem skrivenih registarskih ključeva. Poseduje mogućnost programiranja skripti za ovu alatku (moguće je razviti sopstvenu .NET aplikaciju koja može da se integriše u ILOOK). Od novina prisutna je funkcija analize fajlova

[415] Zero-day napad predstavlja napad određenim programom (zero-day exploit) koji iskorišćava ranjivost računarskog programa (servisa) koja nije prepoznata od strane programera. Zero-day exploit predstavlja program koji koristi sigurnosni propust da bi se izvršio napad.

[416] http://www.perlustro.com/

[417] Hashkeeper predstavlja veliku bazu podataka u Ms Access formatu koja sadrži 69 miliona potpisanih fajlova. Ova baza u sebi sadrži heš vrednosti bezbednih i zlonamernih fajlova čime mogu da se prepoznaju šifrovani programi, fajlovi sa zabranjenim pornografskim sadržajima i programe koji služe za prikrivanje zlonamernih aktivnosti (eng. staganonography programs).

[418] http://www.justice.gov/archive/ndic/

[419] http://www.nsrl.nist.gov/

koja detektuje slike i filmove zabranjenog sadržaja na osnovu prepoznavanja ljudskih formi. Takođe može detektovati i šiframa zaštićene fajlove. Sa bezbednosne tačke gledišta poseduje mogućnost detekovanja malicioznih programa kao štu su Virusi i Trojanci.

ILOOK generiše detaljne izveštaje, bilo da se radi o slučaju ili o dokazima. Počev od verzije 7 ILOOK kalsifikuje dokaze prema Virtuelnim kategirijama. Dokazi iz Virtuelne kategorije mogu biti dodeljeni različitim izveštajima prema tipu i snimljeni u 7 različitih formata (PDF, HTML, MHT, RTF, Excel, TEXT, CSV) ili poslati mailom.

3.4.3 The Sleuth kit, Autopsy forensic browser[420]

The Sleuth kit (TSK) i Autopsy forensic browser predstavljaju Linux orijentisane komplete alata za forenzička istraživanja čiji je autor Brian Carrier. TSK i Autopsy su otvorenog koda i rade na Unix platformi. TSK sadrži kolekciju Linux alata namenjenih komandnom okruženju za forenzičku analizu, dok Autopsy predstavlja grafički interfejs nad tim alatima za forenzičku analizu iz komandnog okruženja (koji pripadaju TSK). Sa ovim alatima moguće je istraživati fajl sisteme kao i logičke diskove (eng. volume). Ovi alati mogu služiti za analizu Windows i Linux fajl sistema. Mogu da analiziraju raw (dd), expert witness (encase) i AFF fajl sisteme i slike diskova podržavajući NTFS, FAT, UFS1/2, ext 2/3 i ISO 9660 fajl sisteme (čak iako operativni sistem na ispitivanom računaru ne podržava fajl sisteme). TSK takođe može oporaviti slak prostor na disku. Autopsy je HTML orijentisan tako, da se njemu može prići sa bilo koje plaftorme uz pomoć HTML pretraživača. Interfejs kod Autopsy je u formi fajl menadžera i pokazuje detalje o obrisanim fajlovima i strukturi fajl sistema.

TSK sadrži 20 komandnih alata organizovanih u grupe. Grupe obuhvataju alate za disk, alate za volume, fajl sistem alate i alate za pretragu. Alati za fajl sisteme su organizovani u kategorije [25]. U nastavku slede kategorije alata koji su deo ovog kompleta opisane prema Brian Carrier-u[421] :

- **alati koji se odnose na fajl sistem** - ovi alati procesiraju generalne informacije o fajl sistemu kao na primer raspored blokova, veličinu i boot blokove, labele. Jedna takva alatka jeste fstat.
- **alati koji se odnose na nazive datoteka** - ovi alati procesiraju strukturu imena fajlova koji su locirani u direktorijumu višeg reda (eng. parent direcotory). U ove alate spada ffind koji pronalazi dodeljena i neraspoređena imena datoteka na koja se ukazuju određen metadata strukture i alatka fls koja izlistava dodeljena i obrisana imena datoteka u direktorijumu.
- **alati koji se odnose na metadata strukture** - ovi alati procesiraju metadata strukture koje sadrže detalje o fajlovima. Primeri ovih struktura su zapisi direktorijuma u FAT, MFT zapisi u NTFS i inodi u Ext i UFS fajl sistemima. U ove alate spadaju icat (prikazuje sadržaj blokova dodeljenih određenom inodu), ifind (može da se ustanovi koji inod sadrži određeni blok), ils (izlistava metadata strukture i njihov sadržaj u formatu gde je razgraničenje "vertical bar" odnosno "|"), istat (prikazuje statistiku i detalje o određenoj metadata strukturi, na primer o broju inoda, u lako razumljivim formatu). Kao cilj upotrebe ovih alata jeste da se dobije kopija fajla bez upotrebe API komandi (CreateFile, CopyFile i druge) koje Rootkit može da onemogući u smislu skrivanja ili sprečavanja pristupa fajlu [113].
- **alati koji se odnose na jedinice podataka** (eng. data unit) - ovi alati procesiraju jedinice podataka prema mestu gde je uskladišten sadržaj fajla. Na primer, klasteri u

[420] http://www.sleuthkit.org/

[421] Svaka alatka ima dva dela u svom imenu. Prvi deo ukazuje na grupu a drugi deo identifikuje funkciju. Na primer alat fls, spada u kategoriju fajl („f“) sa funkcijom izlistavanja („list“) [166].

FAT i NTFS fajl sistemu i blokovi u ext i UFS sistemima. U ove alate spadaju dcat (izvlači sadržaj određene jedinice na primer bloka podata), dls (izlistava sadržaj obrisanog bloka na disku i može izvući nealociran prostor fajl sistema), dstat (prikazuje statistiku o bloku podataka u lako razumljivom formatu), dcalc (izračunava gde podaci iz slike nealociranog prostora, dobijenih alatom dls, nalaze na originalnoj slici)

- **alat za upravljanje medijuma "mmls"**- ova alatka procesira sliku diska i analizira strukturu particija. Moguće je pronaći skrivene podatke između particija. Daje se prikaz rasporeda diska uključujući i nealociran prostor. Izlaz ove alatke identifikuje tip particije i dužinu, što olakšava postupak upotrebe dd da se izvuče particija. Izlaz je sortiran na osnovu početnog sektora pa je lako identifikovati praznine u rasporedu.
- **imidž fajl alatke** - ovi alati prikazuju detalje koji se odnose na imidž fajl. Alatka img_stat prikazuje detalje o formatu imidž fajla, dok img_cat prikazuje raw sadržaj imidž fajla.

TSK kao i Autopsy kompleti sadrže dodatne korisne alate, kao na primer mactime. Mactime na osnovu rezultata dobijenih alatim "fls" i "ils" može kreirati vremensku osu o aktivnostima kako raspoređenih tako i nealociranih fajlovima (vreme pristupa izmene i promene) [6]. Alat Hfind (koristi binarni algoritam za traženje md5 heš vrednosti u već pomenutima bazama NIST NSRL i HashKeeper[422]) i može skratiti vreme potrebno za analizu fajlova eliminišući poznate dobre fajlove, a identifikujući loše, na osnovu poređenja sa bazom.

Ovi forenzički kompleti pokrivaju post-mortem analizu i u tom slučaju moraju se pokrenuti iz pouzdanog i proverenog okruženja (na primer forenzička laboratorija) i analiza "uživo" i u tom slučaju ovi kompleti se pokreću sa cd-a u nepouzdanom okruženju (što se radi u slučajevima odgovora na incident kada je on potvrđen). Nakon što se incident potvrdio, istražitelj može da sprovede post-mortem analizu. Takođe ovi alati poseduju dobre tehnike pretraživanja potencijalnih dokaza sa UNICODE podrškom. Moguće je: prikazivanje fajlova i direktorijuma uključujući i imena obrisanih fajlova, pretraživanje sadržaja fajla u raw ili hex formatu izvlačeći ASCII string. Kada su nepoznati fajlovi u pitanju forenzičar može vršiti njihovo poređenje u heš bazama (NIST NSRL ili HashKeeper) da bi se potvrdilo da li se radi o poznatim dobrim ili malicioznom fajlovima. Sortiranje fajlova se radi prema njihovim internim potpisima. Ujedno se vrši i upoređenje ekstenzija fajla sa tipom fajla da bi se identifikovali fajlovi sa promenjenim ekstenzijama (gde je bio cilj da se fajl sakrije).

3.4.4 AccessData Forensic Toolkit (FTK) and Ultimate Toolkit (UTK)[423]

Ovaj digitalni forenzički komplet alata koristi se od strane pravosuđa, vladinih agencija, i korporacija širom sveta. Dizajniran za detaljno pronalaženje i ispitivanje računarskih dokaza prilikom digitalne forenzičke istrage visokotehnološkog kriminala. Sa ovim kompletom moguće je izvršiti prikupljanje, oporavak fajlova, indeksiranje podataka kao i oporavak podataka na najnižem nivou (eng. data carving). Sadrži moćne alate za pretraživanje, filtriranje fajlova i njihovu analizu. FTK je prepoznat i kao vodeći forenzički alat kada je u pitanju analiza elektronske pošte. FTK uključuje, FTK imager (program sa kojim se prave forenzička kopija ispitivanog hard diska i forenzičke slike), KFF heš biblioteka, prikazivač registarske baze (eng. Registry viewer[424]) kao i 50-100 klijentskih

[422] U 2012 godini NDIC je ostao bez finansiranja i zatvorio je svoja vrata 16.juna 2012. pa je dostupnost i budućnost Hashkeep-era neizvesna. Izvor http://www.whiteoutpress.com/articles/q22012/after-19-years-of-waste-nat-drug-intel-center-closes/

[423] http://www.accessdata.com/solutions/digital-forensics/ftk

[424] Accessdata Registry viewer omogućava pristup zaštićenom "Storage sistem provider" ključu koji sadrži šifre elektronske pošte, Internet šifre i podešavanja. Takođe, pravi izveštaj sa dragocenim podacima iz registarskih ključeva koji su od interesa za istragu.

DNA (DNA ili Distributed Network Attack[425]) licenci[426] za oporavak šifara. Može praviti forenzičke slike, čitati slike dobijenih drugim alatima (ka na primer ENcase). Može prikupiti zaključane sistemske fajlove (SAM/System/NTuser). Sa svojom optimizovanom dtsearch funkcijom izuzetno brzo sprovodi indeksiranje i pretraživanje nad velikim skupovima podataka. Koristi MD5 i SHA-1 haširanje za verifikaciju fajlova. Slike odnosno imidži diskova napravljenih sa programom FTK Imager (ne odnosi se na FTK Imager Lite) sud priznaje kao valjani dokaz. Takođe, AccessData FTK podržava veliki broj postojećih formata za pravljenje forenzičkih kopija. To znači da on može otvoriti i imidže kreirane sa EnCase alatom, SMART alatom i drugih alata. pa čak i .vmdk fajlove koji predstavljaju slike radnih memorija sa virtualnih mašina.

Ultimate Toolkit uključuje kompletan FTK, alat za oporavak šifara (PRTK - Password Recovery toolkit), prikazivač registarske baze, Wipedrive pro, Microsoft NT login access utility kao i Novel utility. Sadrži komponente za oporavak izgubljenih ili zaboravljenih šifara. Postoji mogućnost analiziranja celog hard diska u potrazi za šifrovanim i zaštićenim podacima. Poseduje module za analizu i dešifrovanje registarskih podataka, kao i module za čišćenje hard diska. Da bi se ovi proizvodi mogli koristiti, neophodna je upotreba USB security key (koji se još naziva i dongle) baš kao i kod pomenutog Encase alata. Za svoje proizvode kompanija nudi trening kao i korišćenje demo verzije koji može biti skinut sa zvaničnog sajta kompanije.

3.4.5 Penguin Sleuth[427]

Ovaj komplet alata je u stvari bootabilna Linux distribucija zasnovana na Knopix sistemu prilagođena forenzičaru. Uključuje različite komplete alata kao što su TCT (The Coroner's Toolkit), Autopsy i TST (The Sleuth Kit) kao i alate za skeniranje virusa i skeniranje sistema na ranjivost (eng. penetration test). Može se koristiti iz komandnog ili iz grafičkog okruženja. Omogućeno je pregledanje uživo (eng. live privew) kompromitovanog računara bez izmene nad dokazima kada je u pitanju EXT2, FAT32 i NTFS4. Ernest Baca je uradio proveru studije (eng. validation) o korišćenju Knoppix distribucije za pregled "uživo" na računaru sa EXT3 ili reiserfs instaliranim particijama gde je zaključeno da se kao posledica javlja promena MD5 heš vrednosti particije[428]. Takođe, treba skrenuti pažnju da se posebno bude oprezan prilikom ispitivanja kompromitovanog Linux računara. Razlog leži u tome što će Knoppix pokušati da koristi swap prostor, a on može sadržati potencijalne dokaze koji u tom slučaju mogu biti izmenjeni. Forenzički alati koji se mogu naći u ovom kompletu su sledeći :

- **Sleuth Kit** - forenzički alati komandnog okruženja;
- **Autopsy** - grafički deo Sleuth kit;
- **Dcfldd** - unapređena verzija DD Imaging alata sa ugrađenim heširanjem;
- **Foremost**[429] - alat komandnog okruženja za oporavak podataka
- **Air** (Automated Image and Restore) - grafički interfejs za (dd ili dc3dd[430]) za kreiranje forenzičkih slika;
- **Md5deep**[431] - program za MD5 heširanje;
- **Netcat** - obezbeđuju kanal za komunikaciju između dva sistema;

[425] DNA predstavlja novi pristup u procesu oporavka šifrom zaštićenih fajlova. U prošlosti se za oporavak koristila snaga jedne mašne dok se sa novim DNA pristupom koristi snaga svih za to licenciranih mašina na mreži.

[426] Broj licenci može da varira u zavisnosti od FTK paketa koji se kupuje.

[427] http://penguinsleuth.org/

[428] http://www.penguinsleuth.org/Linuxforensics/pensleuth.html

[429] Dostupno na http://foremost.sourceforge.net/

[430] Unapređena dd verziija od strane Jesse Kornblum iz DoD Cyber Crime centra omogućava heširanje sa algoritmima MD5, SHA-1, SHA-256, and SHA-512.

[431] Dostupno na http://md5deep.sourceforge.net/

- **Cryptcat** - obezbeđuje šifrovanje kanala za komunikaciju između dva sistema.

NTFS alati kompleta PSK:
- **Qtparted** - grafički alat za particionisanje;
- **Regviewer** - alatka za prikaz Windows registarske baze.

Bezbednosni alati kompleta PSK:
- **Etherape** - grafička alatka za nadgledanje mrežnog saobraćaja;
- **Clamv** - antivirusni skener;
- **Nikto2**[432] - bezbednosni skener za web server;
- **Snort**[433] - alatka komandnog okruženja za detekciju upada u mrežu (da difotlnim pravilima);
- **John the Ripper** - password cracker komandnog okruženja;
- **Rkhunter**[434] - alatka komandnog okruženja koja pretražuje znakove prisustva rootkit programa;
- **Ethereal** - alatka za analizu saobraćaja na mreži;
- **FWBuilder** - grafički Firewall program;
- **Nessus** - grafički skener ranjivosti sistema;
- **Chkrootkit** [435] - alatka komandnog okurženja koja pretražuje znakove prisustva rootkit programa.

3.4.6 The Coroner's Toolkit (TCT)[436]

Primarno je razvijen za UNIX sisteme od strane Dan Farmer and Wietse Venema, ali može izvesti prikupljanje podataka i analizu i na diskovima koji nisu pod Unix fajl sistemom. Alati koji su sastavni deo TCT kompleta su :

– **grave-robber** - ova alatka služi za prikupljanje podataka;
– **alati pisani u C-u** o kojima je bilo reči u prethodnim kompletima (ils, icat, pcat, mactime);
–**unrm& lazarus** - ovi alati služe oporavak obrisanih fajlova;
–**findkeytool** - alatka koja služi za oporavak šifarskih ključeva iz pokrenutog procesa ili fajla.

3.4.7 Helix Live CD[437]

Starije verzije Helixa predstavljaju prilagođenu Knoppix live Linux distribuciju za forenzičku istragu, dok su novije bazirane na Ubuntu live distribuciji. Forenzičar podiže Linux okruženje koje podrazumeva prilagođen Linux kernel, detektovanje hardvera kao i prisustvo mnogih forenzičkih programa i programa za odgovor na incidentnu aktivnost. Nema uticaja na računar koji se ispituje što predstavlja forenzički ispravan pristup. Neće uraditi automatski (eng. mount) priključak swap prostor kao što neće priključiti ni bilo koji konektovan uređaj na ispitivani sistem. Karakteristika ovog kompleta jeste ta što sadrži spoj Windows funkcionalnosti koja se ogleda prilikom prikupljanja lako izmenjivih podataka uživo sa Windows sistema (program se pokreće kao standardna Windows aplikacija) i Linux

[432] Dostupno na http://www.cirt.net/nikto2
[433] Dostupno na www.snort.org
[434] http://rkhunter.sourceforge.net/
[435] http://www.chkrootkit.org/download.htm
[436] http://www.porcupine.org/forensics/tct.html
[437] http://www.e-fense.com/products.php

funkcionalnosti sopstvenog butabilnog operativnog sistema koji se koristi u sveobuhvatnoj post-mortem analizi. Najvažniji alati koji su deo Helix kompleta su sledeći :
Alati odgovora na incident :
- **WFT, WTF2** (Windows Forensics Toolchest)[438] - Ova alatka čiji je autor Monty McDougal dizajnirana je da omogući ponovljiv automatizovan proces forenzičkog odgovora uživo, odgovora na incident i procenu bezbednosti na Windows sistemima na osnovu prikupljenih bezbednosno relevantnih informacija sa sistema [123]. Generiše izveštaj u HTML formatu.
- **IRCR2** (Incident Response Collection Report)[439] - Ova alatka čiji je autor John McLeod je skripta koja omogućava prikupljanje i analizu forenzičkih podataka na Windows operativnom sistemu. Slična je alatu TCT (Farmer i Vanema) i orijentisana je više prikupljanju nego analizi, jer je ideja da se ovako prikupljeni podaci, nakon incidentne radnje, pošalju digitalnom forenzičaru na dodatne analize.
- **FRU** (First Responder Utility) - Ova alatka čuji je autor Harlan Carvey omogućava forenzičarima da izbegnu nepraktičnost netcata[440] kada je u pitanju prikupljanje podataka uživo sa ispitivanog sistema. Sastoji se iz dve komponente, serverske i klijentske. Za funkcionisanje na Windows sistemima potrebni su određeni dll-ovi, jer je kod originalne skripte pisan u perlu i potom kompajliran za Windows okruženje.
- **Nigilant32** - Ova alatka razvijena je od strane Matthew Shannon iz Agilant Risk Managemet, omogućava forenzičaru da pregleda hard disk, da napravi sliku memorije i da uradi snimak stanja (eng. snapshot), trenutno pokrenutih procesa i otvorenih portova na sistemu. Ima veoma mali uticaj na sistem i zauzima manje od 1mb memorije kad se učita. Podržava Windows 2000, XP i 2003.
- **FRED** (First Responder's Evidence Disk) - Ova alatka čiji je autor Jesse Kornblum predstavlja skriptu za odgovor na incident slična je alatki IRCR. Orijentisana je ka prikupljanju lako izmenjivih podataka na Windows operativnom sistemu bez modifikovanja ispitivanog sistema. Ova alatka od Helix verzije 2 nije prisutna u kompletu.
- **SecReport** (Security Reports) - Ova alatka služi za prikupljanje bezbednosnih informacija na ispitivanom sistemu. Takođe, pomoću nje moguće je vršiti poređenja rezultata dva sistema ili istog Sistema, ali sa različitim vremenima. Poseduje grafičko okruženje. Informacije koje prikuplja su sledeće : hard diskovi, procesor, ostali uređaji, podešavanja page fajl setovanja, otvoreni portovi, instalirane zakrpe, programi, servisi, konfiguracija event loga, mrežna konfiguracija, bebednosna (eng. audit) konfiguracija.
- **Prikazivači različitih namena** - U ovom kompletu mogu se naći prikazivači, messenger šifara, šifara za korišćenje elektronske pošte, mrežne šifre, zaštićenog područja, registarske baze, istorije IE, IE šifre, Outlook PST šifre, kolačiće IE i Mozille, polja prekrivena asterisk znacima "******".
- **Pouzdano komandno okruženje** - omogućava komandni šel koji je pouzdan i proveren za vršenje forenzičkog prikupljanja podataka.
- **MD5 Generator** - generiše MD5 heš za prikupljene podatake.
- **Pc inspector File Recovery**[441] - Ova alatka kompanije Convar služi za oporavak podataka sa FAT 12/16/32 i NTFS-a. Automatski pronalazi particije čak i ako je boot sektor kod FAT particije (ne odnosi se na NTFS) obrisan ili oštećen. Oporavlja podatke se originalnim vremenskim i datumskim pečatima. Omogućeno je i snimanje oporavljenih podataka na mrežni disk. Podržava sledeće formate podataka : arj , avi , bmp , cdr , doc , dxf , dbf , xls , exe gif , hlp , html , htm , jpg , lzh , mid , mov , mp3 pdf , png , rtf , tar , tif , wav , zip. Od operativnih sistema zvanično podržava Windows 95/NT/98/Me/2000/XP.

[438] Dostupno na http://www.foolmoon.net/security/wft/index.html
[439] Dostupno na http://ircr.sourceforge.net/
[440] Alatka netcat u većini slučajeva funkcioniše odlično, međutim kada naraste broj komandi koje treba primeniti (tako na primer može doći do grešaka prilikom kucanja) postaje nepraktičan.
[441] Dostupno na http://www.convar.de/ , pristupano 16.04.2013

- Windows Systernals Rootkit Revealer[442] - Autori ove alatke su Bryce Cogswell i Mark Russinovich. Poseduje naprednu tehniku pretraživanja rootkit-a na sistemu (bilo da je reč o korisničkom ili kernel modu rootkit-a). Najnovija verzija nije komandno orijentisana. Podržava Windsows XP (32-bit) i Windows server 20003 (32-bit).

3.4.8 Knoppix-STD 0.1[443]

Ovaj komplet alata predstavlja kolekciju više stotina bezbednosnih alatki otvorenog koda. Spada u live Linux distribucije što znači da se pokreće sa boot-abilnog diska u memoriji bez promene operativnog sistema na računaru. Upotrebljava se za oporavak podataka u post-mortem analizi ili nad zaključanim računarima. Ovaj komplet alata pruža i mogućnost izvođenja procene ranjivosti sistema kao i penetraciono testiranje (simulacija napada na sistem sa ciljem procene sigurnosti računarskog sistema ili mreže).
Značajni forenzički alati koji dolaze u sklopu ove distribucije su sledeći :

- **sleuthkit** : komplet o kome je već bilo reči.
- **autopsy** : komplet o kome je već bilo reči.
- **biew** : binarni prikazivač.
- **bsed** : binarni editor.
- **dcfldd** : US DoD Computer Forensics Lab verzija dd.
- **fenris :** alat za debagovanje koda, dekompajliranje.
- **fatback** : oporavak FAT.
- **foremost** : oporavak specifičnih tipova fajlova sa slike diska.
- **ftimes** : system baseline tool (be proactive).
- **galleta** : oporavak kolačića iz Internet Explorer-a.
- **mac-robber** : TCT's graverobber pisan u C jeziku.
- **md5deep** : izvršenje md5 heširanja nad vise fajlova/direktorijuma.
- **memfetch** : prikupljanje dump-a memorije.
- **pasco** : pretraživanje IE index.dat fajla.
- **photorec** : prikupljanje fajlova sa digitalnih kamera
- **readdbx** : konvertovanje Outlook Express .dbx fajlova u mbox format.
- **readoe** : konvertovanje celog Outlook Express direktorijuma u mbox format.
- **rifiuti** : pretraživač Windows Recycle Bin INFO2 fajlova.
- **secure_delete** : bezbedno brisanje fajlova, swap prostora memorije…
- **testdisk** : testiranje i oporavak nestalih particija.

ids – alati za detektovanje upada na sistem

- **snort 2.1.0**: IDS.
- **ACID** : Web interfejs za snort.
- **barnyard** : brzo procesiranje snort logova.
- **oinkmaster** : ažuriranje snort definicija.
- **bro** : mrežni IDS.
- **prelude** : mrežni i lokalni IDS.
- **logsnorter** : praćenje logova.
- **swatch** : praćenje bilo kakvog fajla.
- **sha1sum** : generisanje i verifikacija SHA1 heša.

[442] Dostupno na http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx , pristupano 16.04.2013
[443] http://s-t-d.org/

- **md5sum** :generisanje i verifikacija MD5 heša.

alati za procenu ranjivosti na sistemu

- **amap 4.5** : mapira startovane programe na udaljenom računaru.
- **chkrootkit 0.43** : pretraživanje pristustva na rootkit.
- **clamAV** : antivirusni skener.
- **hydra** : brute force alatka.
- **nbtscan** : skeniranje SMB mreže.
- **nessus 2.0.9** : alatka za skeniranje ranjivosti na sistemu.
- **nikto** : skener WEB-a na ranjivosti.
- **screamingCobra** : skener WEB-a na ranjivosti.

3.4.9 LiveWire Investigator[444]

Predstavlja sveobuhvatan komplet alata za digitalnu forenziku. Poseduje veliki broj opcija, kako za prikupljanje podataka, tako i za njihovu analizu. Pogodan je za forenziku "uživo", u stanju je da prikuplja podatke uključujući i stanje "running state" dok system nastavlja da radi. Poseduje automatsko logovanje i kreiranje izveštaja za sve pokrenute istražne aktivnosti. Prikuplja i snima trenutno aktivno stanje sistema "running state" i poseduje mogućnost kreiranja slike fizičke memorije. Uživo može da pregleda registarsku bazu. Prikuplja ključne informacije o startovanim programima, procesima, mrežnim konekcijma, prenešenim podacima. U stanju je da mapira mreže, procenjuje ranjivosti na sistemu, prikuplja dokaze direktno sa ispitivanog računara, kao i da vrši skeniranje na maliciozne programe. Od operativnih sistema podržava Windows NT4, 2000 pro, XP, 2003 server, Vista.

3.4.10 The ProDiscover Family[445]

Prodiscover Family predstavlja sveobuhvatan komplet za digitalnu forenziku i podrazumeva dva paketa alata : Prodiscover forensic paket i Prodiscover incident response paket. Namenjen je pravosudnim organima.

Prodiscover forensic paket služi za prikupljanje, analizu, upravljanje i kreiranje izveštaja o digitalnim dokazima. Prilikom prikupljanja za analizu podataka kreira se bitstream slika originalnog diska uključujući i skriveni prostor HPA (eng. Host protected area)[446]. Moguća je pretraga fajlova, metadata podataka kao i celog diska uključujući slek prostora i HPA. Može čitati slike raw (.dd) formata i Encase formata. Podržava sve verzije Windows operativnih sistema sa podrškom za fajl sisteme FAT 12/16/32/exFAT , NTFS, SUN Solaris UFS, Linux Ext 2/3/4, i Mac OSX HFS+, uključujući dinamičke diskove i programski RAID. Moguća je upotreba Proscript-a, i Perla-a da se omogući automatizovanje procesa istrage.

Prodiscover incident response paket pretvara Prodiscover forensic u klijent server aplikaciju koja omogućava pregled diska, prikupljanje slike diska i analizu preko TCP/IP mreže. Pored navedenih funkcionalnosti sadrži i dodatne napredne alate za odgovor na sajber napade. U stanju je da brzo identifikuje upade na sistem bez gašenja sistema. Dozvoljava

[444] https://www.wetstonetech.com/faq_livewire.html
[445] http://www.techpathways.com/webhelp/whnjs.htm
[446] HPA predstavlja deo hard diska skriven od operativnog sistema, BIOS-a a samim tim i od korisnika [67]. Uglavnom se koristi od strane proizvđača računara da bi se tu smestili podaci sa održavanje ili oporavak sistema. Naravno, zlonamerni korisnici tu oblast mogu da iskoriste za skrivanje podataka. Za proveru postojanja HPA na disku moguće je koristiti i Brian Carrirer-vu Sleuth kit alatku disk_stat.

forenzičaru da prikupi sadržaj fizičke memorije sa "živog" sistema. Takođe, odlikuje se posedovanjem najmodernijeg sistema za verifikaciju podataka.

Omogućena je potpuna indeksirana pretraga, mountovanje „uživo“, kreiranje slika svega na ispitivanom Windows sistemu uključujući Volume shadow copy. Može obavljati neograničen broj istovremenih kreiranja slika sistema. Uz pomoć ovog seta alata moguće je utvrditi, da li je sistem kompromitovan i omogućava prikupljanje potrebnih dokaza da se to i dokaže. Istraživanje može obuhvatati kreiranje slike fizičkog diska ili memorije.
Ovaj komplet u stanju je da pronađe sve podatke koji se nalaze na ispitivanom disku u forenzički ispravnom maniru, čak i one koji se nalaze u HPA (eng. host-protected area) oblasti diska bez izmene podataka realizujući analizu skrivenih podataka [193]. Za obezbeđenje integriteta kreiraju se heš potpisi (MD5, SHA-1, SHA-256) za sve fajlove i moguće je njihovo poređenje sa određenom bazom poznatih fajlova. Ima funkciju izvlačenja EXIF[447] informacija iz JPEG fajlova. Prodiscover incident response zahteva instaliranje serverskog apleta (PDServer program) na ispitivanom računaru da bi se realizovao postupak prikupljanja podataka, što ga čini prihvatljivim, više korporativnom okruženju, nego za istrage pravosudnih organa.

3.4.11 X-ways Forensics[448]

X-Ways Forensics predstavlja forenzičko radno okruženje za digitalnu istragu računarskih sistema. Podržava Windows XP/2003/Vista/2008/7*, 32 Bit/64 Bit. Podržava veliki broj opštih kao i specifičnih funkcija za forenzičku ostragu. Podržava kloniranje diskova i pravljenje slike originalnog diska bez izmene podataka. Od fajl sistema podržava FAT12, FAT16, FAT32, exFAT, TFAT, NTFS, Ext2, Ext3, Ext4, Next3 [449] , HFS, HFS+/HFSJ/HFSX, ReiserFS, Reiser4, XFS, UFS1, UFS2, CDFS/ISO9660/Joliet, UDF, GPT, Windows dinamičke diskove i LVM2.. Može čitati slike formata raw (.dd), ISO, VHD i VMDK i encase (.E01). Obezbeđuje kompletan pristup diskovima, RAID-u i slikama većim od 2TB. Ima funkciju pregledanja i dumpa fizičke memorije za operativne sisteme Windows 2000, XP, Vista, 2003 Server, 2008 Server, Windows 7, a može prikupiti i virtuelnu memoriju startovanih procesa. Poseduje različite tehnike oporavljanja podataka koji obezbeđuju brzinu. Ova altka vrši prikupljanje podataka iz slek prostora, slobodnog prostora . Kreira katalog fajlova i direktorijuma za sve medije. Izračunava hep vrednosti za sve fajlova sa dostupnim algoritmima CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD[450]. Ima podršku da importuje NSRL RDS 2.x, HashKeeper, i ILook heš za potrebe deduplikacije poznatih fajlova i pronalaženja onih malicioznih. Poseduje odlično simultano fizičko i logičko pretraživanje kao i zaštitu od upisivanja da bi se obezbedio integritet podataka. Raspolaže sa funkcijom analize elektronske pošte prikupljene iz sledećih formata : Outlook (PST, OST), Exchange EDB, Outlook Express (DBX), AOL PFC, Mozilla (including Thunderbird), generic mailbox (mbox, Unix), MSG, EML Vrši automatsku detekciju zaštićenih MS Office i pdf fajlova kao i detekciju slika u njima sa funkcijom Skin color detection koja služi za ubrzavanje pronalaženja tragova dečije pornografije. Takođe ovaj komplet poseduje i veliki broj prikazivača različitih namena : prikazivač Registry baze (za sve Windows verzije) sa generisanjem registarskog izveštaja, prikazivač even logova (.evt, .evtx), shortcut fajlava (.lng), Windows prefetch fajlova, raspoređenih zadataka (.job), wtmp/utmp/btmp logova, Outlok imenika, Firefox istoriju, Firefox download, Chrome

[447] Exchangeable image file format (Exif) predstavlja standard koji opisuje format slike, zvuka, snimljenih digitalnim kamerama. Ovaj standard obuhvata se metadata podacima, kao na primer datum i vreme, opis, copyright informacije, tip kamere i njena podešenost i dodatni podaci.
[448] http://www.x-ways.net/forensics/
[449] http://www.ctera.com/products/technology/next3-file-system
[450] http://homes.esat.kuleuven.be/~bosselae/ripemd160.html

istoriju, Chrome arhiviranu istoriju, podatke o Chrome logovanjima, Safar cache, Skype bazu podataka sa kontaktima i prenešenim fajlovima. Izvlačenje metadata podataka iz velikog broja različitih tipova podataka kao što su : MS Office, OpenOffice, StarOffice, HTML, MDI, PDF, RTF, WRI, AOL PFC, ASF, WMV, WMA, MOV, AVI, WAV, MP4, 3GP, M4V, M4A, JPEG, BMP, THM, TIFF, GIF, PNG, GZ, ZIP, PF, IE cookies, DMP memory dumps, hiberfil.sys, PNF, SHD & SPL printer spool, tracking.log, .mdb MS Access database, manifest.mbdx/.mbdb iPhone backup. Ima mogućnost detektovanja HPA prostora na disku. Ima mogućnost dekompresovanja kompletnog hiberfil.sys fajla. Takođe, nakon prikupljenih podataka i pronađenih dokaza alatka izrađuje detaljan izveštaj o nalazima.

X-ways winhex[451] - ova forenzička alatka (znatno jefitinija) digitalnom forenzičaru može koristiti kao hex editor, disk editor ili RAM editor zajedno sa ostalim funkcijama programa kao što su spajanja, odvajanja, kombinovanja i procene fajlova. Takođe, ovaj program poseduje funkciju brzog pretraživanja i funkciju zamene, šablon za uređivanje, enkripciju, funkciju izmene fajlova, mehanizam za pravljenje rezervnih kopija, mogućnost pravljenja slike diska, kloniranje diska i štampanje. Od strane disk editora podržani su flopy diskovi, hard diskovi cd i dvd drajvovi. Podržava kreiranje heš vrednosti za veliku količinu fajlova (CRC32, MD4, ed2k, MD5, SHA-1, SHA-256, RipeMD. Ova alatka služi za prikupljanje i analizu dokaza, jer pored mogućnosti za kopiranje i verifikaciju dokaza, sadrži i HEX editor koji omogućava analizu podataka.

3.5 TRENDOVI U RAZVOJU ODGOVORA NA PROTIVPRAVNE AKTIVNOSTI

Kada je reč o zlonamernom iskorišćavanju (eng. exploit) računarskog sistema podrazumeva se dobijanje pristupa na iskorišćenom sistemu, većih prava na sistemu i uskraćivanje servisa na kompromitovanom sistemu. Sve tri pomenute zlonamerne aktivnosti su korisne za malicionznog korisnika (napadača) i zavise od tipa napada koji se želi postići. U praksi postoje slučajevi gde se ove aktivnosti kombinuju jedna sa drugom, kao na primer kada napadač kompromituje korisnički nalog da bi imao pristup sistemu. Međutim, pošto nema „administratorske“ privilegije ne može doći do osetljivih informacija niti instalirati zlonamerne programe, u tom slučaju napadač bi izvršio i drugi napad tj. zlonamernu aktivnost koja za cilj ima dobijanje adminisratorskih privilegija da bi dobio pristup osetljivim informacijama i instalirao zlonamerne programe.

Na osnovu velikog broja izveštaja vodećih kompanija koje se bave bezbednošću na Internetu može se ustanoviti da se kompromitovanje računarskih sistema izvodi sve više na sofisticiranije načine (brisanje podataka, šifrovanje podataka, manipulacije sa vremenom i datumima, manipulacija sa meta podacima i upotreba antiforenzičkih programa). Korišćenje nebezbednih mreža može da ima za posledicu kompromitovanje računarskih sistema koji ih koriste[452]. Treba istaći da je veliki broj napada realizovan na osnovu iniciranja od strane samih korisnika, primeri su fišing napadi, korišćenje malicioznih sajtova i metode socijalnog inženjeringa. Fokus na zaštitu od napada treba usmeriti na aktivnosti zaštite pre nastupanja protivpravne aktivnosti (priprema za protipravne aktivnosti) kao i edukovanja što većeg broja krajnjih korisnika po pitanju bezbednog korišćenja računarskih sistema i načinima zaštite. Na primer, zaštitu od napada socijalnog ineženjeringa treba usmeriti na edukaciju službenika u organizaciji. To znači da ukoliko se sumnja u identitet određene osobe (na primer poziv telefonom) toj osobi postaviti niz specifičnih pitanja koja će da otklone sumnje u identitet ili

[451] http://www.x-ways.net/winhex/, 23.04.2012

[452] Najveći broj napada u mreži se realizuje preko layer 2 napada i putem DNS napada. U layer 2 napade spada VLAN hoping, napadi na MAC adrese, DHCP napadi, ARP napadi, napadi obmane a u DNS napade spada DNS hijacking, hijacking HTTP sesije.

da otkriju zlonameran pokušaj. U praksi se pokazalo da se određeni napadači dobro pripremaju za napad tipa socijalnog inženjeringa proučavajući organizaciju. Tako da ukoliko postoji i mala sumnja treba obavestiti i pretpostavljenog, radi dodatnih provera. Korisnici računarskih sistema, takođe treba da vode računa i o tome da kada unose svoje šifre na računarske sisteme nemaju nikoga iza sebe koji može gledati unos šifre. Takođe, treba zabraniti čuvanje šifri (ili njen nagoveštaj) na papirićima pored računara. Da bi se zaštitili od napada pogađanja korisničkih šifri, nikada ne upotrebljavati datume rođenja, porodična ili imena bliskih osoba, imena kućnih ljubimaca, za šifre. Upotreba šifri iz rečnika takođe može biti kompromitovana „dictionary" napadom. Ukoliko se koristi neka reč iz rečnika zbog veće zaštite nju je bolje modifikovati, kao na primer reč „projektant" modifikovati u „pr0j3kt4nt" ili upotrebljavati određene fraze kao na primer „kolikojesati?21h". Napadi na korisničke šifre mogu biti izvedeni i sa tzv. brute-force napadom, a zaštita od njih jeste korišćenje dugačke šifre, upotreba različitih znakova, brojeva, velikih i malih slova. Ukoliko napadaču treba dosta vremena da pogodi šifru, vrlo je verovatno da će odustati. Korišćenje fraza za šifre je dobra opcija za njenu bezbednost. Zaštita od već pomenutih fišing napada je u praksi veoma jednostavna. Ukoliko se od korisnika traže lični podaci da se ostave na određeni Web sajt obavezno pogledati URL adresu. Na primer, pretpostavljate da treba da se nalazite na Yahoo.com sajtu, a URL adresa pokazuje YAHOOHOHO.com to znači da ste na lažnom sajtu. Kada ste na pravom Yahoo.com sajtu URL adresa može samo da bude Yahoo.com, sve ostalo je lažno.

Takođe, da bi se protivpravne aktivnosti mogle suzbijati na pravi način, potrebno je vršiti usklađivanje sa međunarodnim propisima i standardima kao i primena istih.

Mnogi stručnjaci smatraju da je ideja IPS superiornija od detekcije upada IDS. Ipak, Foster i Wislon napominju da sve dok su napadači, odnosno upadi i dalje uspešni potreba za detektovanjem upada je više nego očigledna [64]. Osim toga da bi se sprečavalo ponavljanje upadanja ili napada na sisteme, neophodna je računarska forenzika koja bi utvrdila najpre zašto je došlo do napada ili upada i na koji način. Dakle, računarska forenzika predstavlja i integralni deo zaštite od upadanja na računarski sistem.

To znači da se uspešna zaštita u okviru organizacije može ostvariti kroz postojanje kadrova koji se bave upravljanjem incidentom i upravljanjem rizikom uz obavezno postojanje zaposlenog digitalnog forenzičara. To za posledicu ima smanjenje vremena potrebnog za zaštitu[453]. Takvim sistemom se upravlja kroz postojanje oranizacionih, upravnih i tehničkih mera.

Prava zaštita podrazumeva prevenciju (prava pristupa, kriptografska zaštita i fajervoli) zajedno sa detekcijom (detektovanje incidenta sa digitalnim forenzičarem, odnosno protivpravne aktivnosti) i reakcijom odnosno odgovorom na incidentnu radnju .

Većina organizacija reaguju samo na bezbednosne pretnje i uglavnom te reakcije dolaze nakon što je šteta već učinjena. Ključ infomacione bezbednosti leži upravo u proaktivnom pristupu bezbednosnim pretnjama, što podrazumeva uklanjanje bezbednosnih ranjivosti, pre nego što one budu iskorišćene od strane potencijalnog napadača.

Phillip G. Bradford i Ning Hu u svom radu „A Layered Approach to Insider Threat Detection and Proactive Forensics" su predstavili mogućnost upotrebe peroaktivne forenzike u otkrivanju insajderskih napada uz pomoć sistema za online praćenje korisničkih aktivnosti koje se odnose na otkrivanje potencijalnih zloupotreba računarskih sistema [18].

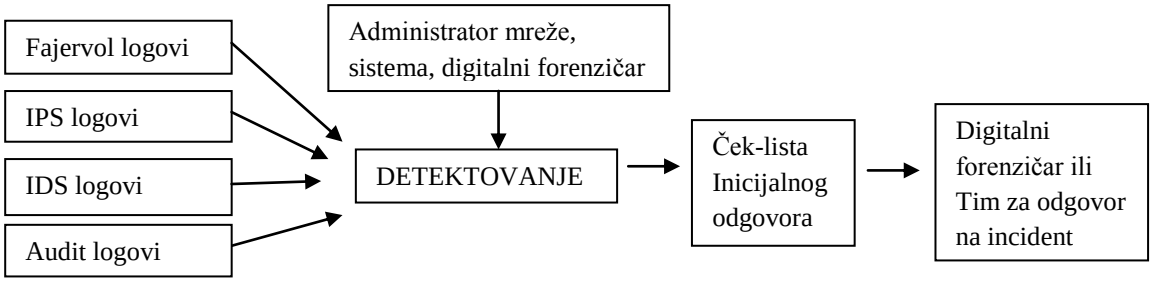
[453] Vreme zaštite = vreme detekovanja + vreme odgovora

3.5.1 Detektovanje incidentnih odnosno protivpravnih aktivnosti

Detekcija upada prema NIST-u (eng. The National Institute of Standards and Technology)[454], definiše se kao proces praćenja i analize događaja koji se javljaju u računarskom sistemu ili na mreži sa ciljem prepoznavanja znakova upada koji se definišu kao pokušaji da se kompromituju poverljivost, integritet, raspoloživost ili da se zaobiđu mehanizmi zaštite računarskih sistema ili mreže[455]. Alati kojima se detektuju ugrožavanje bezbednosti sistema mogu upozoriti administratore (sistema i mreže) mnogo brže nego da se njihova identifikacija vrši manuelno. Sistem za detekciju upada (eng. intrusion detection system - IDS) predstavlja program koji automatizuje proces detekcije upada. Sistem za prevenciju upada (eng. Intrusion prevention system (IPS) ima sve mogućnosti sistema za detekciju upada i može pokušati da zaustavi mogući incident [167]. Ukoliko se onemoguće preventivne funkcije IPS-a on će funkcionisati kao IDS. Za razliku od manuelne provere administratori će na upozorenja koje alati budu generisali, brzo odreagovati i proveriti sumnjive aktivnosti. IDS sistemi su veoma važne kompomente bezbednosti, ali oslanjajući se samo na njih to neće biti garant kompletne bezbednosti na sistemima i mreži. Potrebno je dakle, da se stalno pretražuju znakovi bezbednosnih incidenata koji se mogu prepoznati u vidu :

-sumnjivih stavki u logovima,
-upozorenja od strane IDS,
-upozorenja od strane IPS,
-prisustva neobjašnjivih korisničkih naloga na sistemu ili mreži,
-prisustva sumnjivih fajlova sa nepoznatim ekstenzijama na sistemu,
-neobjašnjivog modifikovanja foldera i fajlova,
-prisustva neuobičajenih servisa,
-otvorenih nestandardnih portova,
-nepredvidivog ponašanja sistema,
-velike količine primljenih paketa (u odnosu na očekivane)
-nedostupnosti drajvovima na sistemu.

Pomenuti znakovi su najosnovniji indikatori potencijalnog ugrožavanja sistema koji se moraju proveravati, a opširiniji spisak indikatora biće izložen u sledećem poglavlju 3.5.2.



Slika 74. Prikaz detektovanja incidentne radnje

Mora se istaći da se rana detekcija upada može detektovati kroz pregledanje, kako pomenutih sistemskih logova, tako i sigurnosnih logova za praćenje aktivnosti (slika 74.). Koji sve procesi mogu biti praćeni zavisi od Auditing konfiguracije na samom sistemu. Audit log može sadržati sledeće informacije :

-specijalne operacije kao na primer promene šifre;

[454] http://www.nist.gov/index.html
[455] Baiju Shah, How to Choose Intrusion Detection Solution, Version 1.2e, SANS Institute InfoSec Reading Room 2001, dostupno na http://www.sans.org/reading_room/whitepapers/detection/choose-intrusion-detection-solution_334.pdf , 25.03.2012

-administrativne aktivnosti na sistemu;
-kreiranje i brisanje objekata u sistemu;
-prijavljivanje na sistem i odjavljivanje;
-da li je događaj bio uspešan ili nije i kada se dogodio;
-čitanje i otvaranje fajlova;
-upis ili izmena fajla;
-ime korisnika koji je inicirao aktivnost.

U zavisnosti od potrebnog nivoa bezbednosti podešava se i nivo Auditinga. Potrebno je naći dobar balans između potrebnog nivoa bezbednosti i performansi računara sa mogućnostima procesiranja dobijenih informacija. Auditing log može da se napuni velikom količinom nepotrebnih informacija, pa se može pojaviti problem da se izdvoje i pronađu bitne informacije i podaci.

Sistemi za detekciju upada IDS (eng. intrusion detection system) mogu biti i uređaji ili programi koje detektuje neovlašćeno korišćenje ili napad na računar ili na mrežu [141]. Mogu biti mrežno ili računarski orijentisani i kombinovani[456]. Upadi se mogu posmatrati kao pokušaji kompromitivanja integriteta, poverljivosti (tajnosti), i dostupnosti informacija odnosno podataka kroz zaobilaženje bezbednosnih mehanizama informaciono komunikacionih sistema.

Prema tome, detekcija može da se radi ručno putem pregledanja log fajlova, automatski ili kombinovano. Iako IDS uređaji po difoltu nisu dizajnirani za forenzičku upotrebu, logovi koje ovi uređaji generišu prema Bill Allen-u mogu biti ključ za uspešnu forenzičku istragu pod sledećim uslovima [5]:

- Moraju da sadrže dovoljno detalja da identifikuju datum vreme, tip upada, moguće izvore i dr.;
- Moraju se čuvati na bezbednom mestu, a ne na računaru koji može biti kompromitovan.
- Mora biti zaštićen od kompromitovanja, pre za vreme i i posle nastalog forenzički relevantnog događaja.
- Mora da generiše precizan izveštaj o svim dokazima koji ukazuju na upad.
- mora biti koordinisan da pokaže sve aktivnosti preduzete od strane zlonamernog napadača na sistemu.

Upozorenje na incident može doći od strane IPS-a, IDS-a, krajnjih korisnika, tehničke podrške, sistem administratora i drugih sistema za zaštitu.

Sistemi za detektovanje upada (IPS i IDS) na računarske sisteme, u stvari pokušavaju da definišu i detektuju abnormalna ponašanja i aktivnosti koje nisu u skladu sa normalnim aktivnostima. Korišćenjem ovakvih sistema pruža mogućnost rane detekcije pokušaja upada na računar ili u mrežu.

Ovaj sistem omogućava proveru različitih tipova aktivnosti kao na primer: detektovanje upada ili pokušaja upada na sistem, detektovanje zamaskiranog napadača (eng. masquerading) detektovanje pokušaja testiranja upada (eng. penetrating) od strane legitimnih korisnika na sistemu, detektovanje odliva informacija (eng. leakage) od strane legitimnih korisnika na sistemu, detekcija trojanskih konja, virusa i napade odbijanja servisa. Profesor Robert Kaufman ističe četiri glavne metode na kojima treba da se bazira sistem za detekciju upada [91][92]:

[456] Računarski orijentisani IDS procesira kontrolne podataka kao i log datoteke i može da utiče na perfomanse računarskog sistema. Na primer, računarski orijentisani IDS će uhvatiti zlonamerne korisnike koji su se ulogovali direktno na sistem, ali će propustiti mrežne aktivnosti. Mrežno orijentisani IDS procesira podatke na mrežnom segmentu, iako je lako primenjiv susreće se sa mnogobrojnim problemima (kao na primer lažni alarm,i zahteva se postojanje velikog broja senzora). Na primer, mrežno orijentisan IDS propustiće zlonamerne aktivnosti pojedinca na ulogovanom računaru, ali će primetiti napade usmerene na više računara. Kombinovani IDS koristi najbolje iz prethodna dva sistema.

- Profilisanjem korisnika - Podrazumeva kreiranje profila za svakog korisnika prema njegovim najčešće sprovođenim akcijama. Taj profil će predstavljati korisnički identitet odnosno obrazac ponašanja koji se posmatra i uspostalja nakon određenog vremenskog perioda. Na primer, svaki korisnik ima običaj da, koristi samo određene komande, pristupa istim fajlovima, prijavljuje se u određeno vreme sa određenim učestalostima, i izvršava iste programe[457]. Iz navedenog, proističe da će se korisnički profil kreirati na osnovu ovih aktivnosti i mora se održavati učestalim ažuriranjima (maskirani napadač neće moži da odgovara profilu pa će napad biti primećen).
- Profilisanjem napadača - Podrazumeva kreiranje napadačkog profila odnosno definisanje aktivnosti koje će napadač preduzeti, ukoliko ostvari neovlašćeni pristup. Tehnika profilisanja počinioca zlonamernih aktivnosti bazira se na analizi prirode dela i načina učenjenog dela. Analiziraju se antropološke, biološke, psihološke, demografske i lične karakteristike potencijalnih počinilaca i upoređuju se sa prethodnim, sadašnjim i naknadnim osobinama načina izvršenja dela. Ove informacije se kombiniju sa drugim relevantnim podacima i fizičkim dokazima i upoređuju sa karakteristikama poznatih tipova ličnosti i mentalnih abnormalnosti. Na osnovu svega toga pravi se opis potencijalnog počinioca[458] [55]. Na primer, ukoliko je napadač ostvario neovlašćeni pristup na sistem najčešće korišćena akcija je proveravanje trenutno prijavljenih korisnika na sistem i istraživanje fajlova direktorijuma i aktivnih servisa. Takođe, profilisanjem treba obuhvatiti i insajderske aktivnosti koje se odnose na sticanje pristupa, od strane legitimnih korisnika na sistemu, datotekama za koje nisu ovlašćeni. Problem kod ovog profilisanja je taj što je teško definisati sve moguće profile bezbednosnih incidenata, a ponekad su aktivnosti novog korisnika koji se upoznaje sa sistemom vrlo slične sa aktivnostima zlonamernog napadača.
- Analizom potpisa (eng. signature analysis) - Kao što svaki pojedinac ima jedinstveni pisani potpis koji se može koristiti u svrhu identifikacije, pojedinci takođe imaju i potpis kucanja "eng. typing signature". Vreme koje je potrebno da se otkucaju određeni parovi ili trojke slova može se meriti, a kolekcija tih digrafa ili trigrafa zajedno formiraju jedinstvene kolekcije na osnovu kojih se pojedinac može profilisati sa ciljem identifikacije. Naravno ova tehnika zahteva specijalnu opremu i na nju se ne može u potpunosti osloniti kao na jedini faktor pri kontroli pristupa baš kao što to navode Bergadano, Gunetti, Picardi [17].
- Otisak napada (eng. attack signature)[459] - Podrazumeva se prepoznavanje konkretnih aktivnosti ili akcija kao pokazatelja napada na sistem. Na primer, pokušaj da se iskoriste ranjivosti na sistemu (bezbednosne rupe eng. security hole) korišćenjem exploit programa. Na primer, najčešći tipova ranjivosti koji se zloupotrebljavaju su pogrešna konfiguracija sistema ili servisa (eng. misconfiguration), podrazumevana konfiguracija sistema ili servisa (eng. default configuration), ranjivosti na prepunjavanje bafera servisa ili aplikacije (eng. buffer overflow), ranjivost na sql inekciju servisa (eng. sql injection), XSS ranjivost servisa (eng. cross-site scripting)[460]. Koliko rizika i slabosti podrazumevana konfiguracija donosi sa sobom biće prikazano u posebnom poglavlju koje će se baviti analizom ranjivosti Operativnih sistema i servisa instaliranih sa podrazumevanim parametrima. Kao problem može da se istakne činjenica da svi metodi napada ne mogu biti poznati, tako da se novi otisci napada konstantno kreiraju, pa je sistem za detekciju upada potrebno često ažurirati (eng. update).

[457] Tipovi aktivnosti koji mogu da se snimaju uključuju iskorišćenost CPU i I/O, vreme uspostavljanja konekcije i dužina trajanja i broj uspostavljanjih konekcija, lokacija korišćenja, korišćene komande, upotreba maila, upotreba kompajlera i editora, pristup i izmena fajlova i foldera, greške i mrežne aktivnosti.

[458] Mirjana Drakulić, Ratimir Drakulić, Cyber kriminal, Prezentacija, Fon 2011, dostupno na http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDMQFjAA&url=http%3A%2F%2Fposlis.fon.bg.ac.rs%2Findex.php%3Foption%3Dcom_docman%26task%3Ddoc_download%26gid%3D295%26Itemid%3D14&ei=QjttUfLgIsnkswawmoDIDg&usg=AFQjCNGqrlDyeh9PUTyZ42pif5r8eyS11Q&bvm=bv.45175338,d.Yms&cad=rja

[459] Kaufman J. Robert, Intrusion Detection and Incident Response IS 3523 course,UTSA Spring 2012, dostupno na http://faculty.business.utsa.edu/rkaufman/IDLsn4.ppt, 24.03.2012

[460] Napadi tipa Cross site scripting (XSS) nastaju kada zlonamerni napadač na WEB sajt unosi takve maliciozne podatke da aplikacija izvršava nešto što nije predviđeno. U praksi ranjivosti na XSS su se prepoznale u određenim funkcijama WEB sajta kao na primer pretraživač na sajtu, forme za logovanja, polja za komentare.

Kada se primenjuju pomenuti sistemi za praćenje aktivnosti (eng. monitoring) postavlja se pitanje očuvanja privatnosti od strane pojedinca. Ukoliko se monitoring primenjuje, organizacija je u obavezi da obavesti pojedinca da su njihove aktivnosti predmet monitoringa. Na primer, računarski sistemi vladinih organizacija u Sjedinjenim Američkim Državama poseduju banere upozorenja. Koordinacioni centar CERT (CA-92:19)[461] dobio je informacije (koje je CERT dalje preporučio) od Američkog odeljenja za pravosuđe (eng. USA DOJ) po pitanju praćenja otkucaja na tastaturi (eng. monitor keystrokes) kao metod zaštite računarskih sistema od neovlašćenog pristupa da se korisnik mora eksplicitno upozoriti u formi upozoravajućeg banera.
Prema forenzičkoj praksi ukoliko je napadač ostvario neovlašćeni pristup na sistemu uz ostvarivanje root odnosno admin privilegija na njemu, prepoznate su sledeće aktivnosti koje mogu da izazovu mnogo štete:

- dodavanje sebe tj. zlonamernog korisnika za budući pristup sistemu,
- dodavanje kompromitovanog sistema u botnet kolekciju za korišćenje u napadu na druge sisteme,
- korišćenje kompromitovanog sistema kao proxy servera za kompromitovanje drugih sistema,
- instaliranje rootkit alata za lakši povratak na sistem uz dobijanje kompletne kontrole nad sistemom,
- permanentna krađa informacija,
- upotreba sistema za skladištenje zabranjenog materijala,
- onesposobljvanje sistema ili uništavanje svih informacija na njemu.

Benefiti detekcije upada u sistem su višestruki : markiraju se napadi koji nisu sprečeni drugim sredstvima, sprečavanje daljeg širenja štete na računarskim sistemima ili u mreži nakon nastanka incidentne radnje (na primer, nakon upada hakera na server), dokumentuju se postojeće pretnje, poboljšava se kvalitet i kontrola administracije i dizajna bezbednosti odnosno mehanizma za detektovanje incidentne radnje koja aktivira odgovor na incident. Sve pomenuto ima za cilj kreiranje bezbednijeg funkcionisanja mreže i operacija na računarima. Poseban značaj detekcije upada, ističe se u digitalnoj forenzici čiji rezultati sa jedne strane utiču na poboljšanje bezbednosti u informacionim sistemima, a na drugoj strani ti rezultati pomažu u procesuiranju incidentnih odnosno protivpravnih aktivnosti. Bitno je istaći da se vreme zaštite izračunava na osnovu vremena potrebnog za detekciju i vremena reakcije na incidentnu odnosno protivpravnu aktivnost.

3.5.2 Indikatori incidentnih odnosno protivpravnih aktivnosti

Za samu istragu veoma je važna inicijalna procena digitalnog istraživača koji mora da sagleda sve simptome incidentne aktivnosti, da bi se dobio odgovor na pitanje, da li je u pitanju sistemski problem ili incidentna, odnosno protivpravna aktivnost. To za rezultat podrazumeva potvrđivanje da li se radi o incidentu, identifikovanje incidente i prijavljivanje incidentne radnje, odnosno protivpravne aktivnosti. U daljem tekstu biće izneti neki od potencijalnih indikatora incidentne, odnosno protivpravne aktivnosti koji se u praksi dešavaju:

- neobjašnjivo visoka iskorišćenost opreme (računarskih stanica, serverskih stanica, mrežnih resurasa, storidža),
- pojava upozorenja/alarma od strane sistema za detekciju napada IDS, firewalli ili network trap dna sistemu može registrovati napad od spolja ili izunutra,

[461] http://cpsr.org/prevsite/cpsr/privacy/computer_security/cert_keystroke_monitoring.txt/

- veliki broj neuspešnih logovanja na sistem,
- neobjašnjiva upozorenja ili alarmi firewall-a na operativnom sistemu,
- logovanje putem skrivenih ili difoltnih korisničkih naloga (na primer guest),
- registrovana neuobičajeno velika aktivnost na mreži ili na sistemu tokom neradnih sati,
- izmenjeni datumi na fajlovima,
- izmenjeni korisnički profil za logovanje,
- neobjašnjivo zaključavanje korisničkih naloga,
- izmenjena korisnička lozinka bez znanja korisnika,
- pronađeno je postojanje novih SUID i SGID programa,
- mrežni senzori detektuju neuobičajeno visoki nivo mrežne aktivnosti,
- prisustvo novih naloga na sistemu koji nisu kreirani od strane sistem administratora,
- postojanje nepoznatih datoteka ili izvršnih fajlova,
- neobjašnjivi oštećeni fajlovi ili servisi,
- neobjašnjive promene u fajlovima ili dozvolama za pristup direktorijuma,
- neobjašnjive promena privilegija,
- neobjašnjivi gubici osetljivih i kritičnih podataka,
- izmene web stranica na web serveru,
- postojanje hakerskih alata na sistemu (na primer exploiti, snifferi),
- izbrisani ili prazni log fajlovi,
- performanse računara drastično smanjene,
- obaranje računarskog sistema (nemogućnost bootovanja, iznenadna restartovanja računara, zamrzavanje, iznenadno isključivanje),
- detektovanje otvorenih backdoor portova na sistemu,
- neobičan način korišćenja programa, kao na primer kompajliranje programa na korisničkom nalogu koji ne pripada nalogu programerskog profila,
- konstantno onemogućavanje normalnog rada antivirusnog programa,
- nemogućnost instaliranja novih aplikacija,
- aplikacije koje su najčešće korišćene nisu funkcionalne,
- nepravilan rad task menadžera (nemogućnost pokretanja task menadžera),
- nemogućnost normalnog izvršavanje registry editora (pri pokretanju se zamrzava ili se zatvara),
- otvaranjem Internet pretraživača vrši se redirekcija na nepoznate sajtove,
- izmena ili dodavanje sistemskih programa bez znanja administratora,
- prisustvo novog aliasa instaliranog na e-mail sistemu,
- prisustvo zabranjenog pornografskog sadržaja,
- nestanak/krađa računara ili mrežne opreme.

3.5.3 Odluke koje se odnose na rešavanje incidentne odnosno protivpravne aktivnosti

Pre nego što se donese konkretno rešenje kao odgovor na incidentnu, odnosno protivpravnu aktivnost moraju se uzeti u obzir sve okolnosti i okruženje u kome se ona desila. Ukoliko se incidentna, odnosno protvipravna aktivnost desila u nekoj organzaciji, bitno je ustanoviti njene prioritete. To može da podrazumeva i utvrđivanje i primenu određenih aktivnosti prema značajnosti, kao na primer vraćanje operativnog sistema u operativno stanje, obezbeđivanje integriteta podataka, procena efekta incidenta odnosno protivpravne aktivnosti, prikupljanje dokaza. Potrebno je detaljno razmotriti prirodu incidenta odnosno protipravne aktinosti, da bi se razumelo na koji način se desila incidentna, odnosno protivpravna aktivnost i primeniti odgovarajuće zaštitne mere nad pogođenim računarskim sistemom. Takođe, utvrditi da li postoje skriveni ili sistemski uzroci incidentne odnosno protipravne

akivnosti (kao na primer, nedostaci standarda, nepoštovanje standarda, nepoštovanje procedura itd.). Potrebno je predvideti i oporavak kako kompromitovanog računara tako i onog koji je bio pod uticajem protivpravne aktivnosti. To za posledicu može imati upotrebu starijih verzija podataka, ranije stanje operativnog sistema (eng. restore point), ili programa koji obezbeđuju normalnu operativnost sistema. Neophodno je definisati odgovarajuće primene ispravki (eng. patch) nad operativnim sistemima ili programima sa ciljem onemogućavanja ranjivosti nad računarskim sistemima i odrediti odgovorna lica. Treba napomenuti, da se sve vrste ispravki moraju prethodno testirati, pre nego što se upotrebe na produkcionim sistemima. Osobe određene za ispravljanje sistemskih problema, takođe moraju da kontrolišu i prate napredak neophodnih ispravki.

Takođe, vrši se potvrđivanje o tome da li su primenjena zaštitna sredstva i kontramere bile efikasne, odnosno vrši se provera da li se nad svim kompromitovanim računarskim sistemima izvršila pravilna primena zaštitnih mera. Kada se incidentna odnosno protivpravna aktivnost konstatuje u organizaciji (čak, iako je odgovor na incident bio efikasan) potrebno će biti ažuriranje svoje bezbednosne politike kako bi se smanjio rizik od budućih incidenata odnosno protivpravnih aktivnost i neophodnih procedura koje će budući odgovor učiniti još efikasnijim. S obzirom da dogovorena adekvatna rešenja, kada je u pitanju protivpravna aktvnost, skoro uvek zahtevaju više resursa nego što je raspoloživo, treba uzeti u razmatranje i realizaciju proaktivne zaštite na operativnom sistemu.

Na donošenje rešenja takođe utiče i način na koji izvršena incidentna odnosno protivpravna aktivnost. Ukoliko je sistem kompromitovan, zlonamerni napadač može prići računarskom sistemu ili mreži preko kompromitovanih servisa (eng. vulnerable services), preko zadnjih vrata (eng. backdoors) ili putem važećih kredencijala (eng.credentials). Ukoliko se protivpravna aktivnost realizovala na osnovu ranjivosti servisa, rešenja će da obuhvataju i razmatranje mrežnih protivmera, vršenje skeniranja ranjivosti operativnog sistema i instaliranje zakrpa (eng. patches) i ispravki (eng. fixes). Ukoliko se protivpravna aktivnost realizovala na osnovu zadnjih vrata, rešenje će obuhvatiti i razmatranje mrežnih protivmera, detaljna provera računarskog sistema, vršenje skeniranja ranjivosti operativnog sistema i instaliranje zakrpa (eng. patches) i ispravki (eng. fixes). Ukoliko se protivpravna aktivnost realizovala na osnovu važećih kredencijala rešenjem će se zahtevati izmena svih šifara na sistemu kao i primena nove autentifikacione šeme.

3.5.4 Forenzički odgovor na incidentnu/protivpravnu aktivnost

Odgovor na incidentnu/protivpravnu aktivnost može da postoji samo ako se ona uspešno bude detektovala. Prilikom prvog odgovora (forenzičkog ili tima u okviru kompanije[462]) na incidentnu/protivpravnu aktivnost, potrebno je doneti odluku o tome da li da se kompromitovani računar isključi ili da ostane uključen. Ovo je vrlo osetljiva odluka, jer nestabilni podaci (eng. volatile data) prilikom isključivanja računara mogu biti izgubljeni, jer se nalaze u memoriji računara, stanjima mrežnih konekcija i stanjima startovanih procesa [196]. Takođe, gašenje sistema može, ne samo da utiče i na mogućnost izvođenja imidžinga, već može da promeni podatke koji se nalaze u operativnom sisemu. Većina sistema se može isključiti na dva načina :

[462] Postoje različiti tipovi timova za odgovor na incidentnu, odnosno protipravnu aktivnosti (eng. computer security incident response team ili skraćeno CSIRT). Na primer, postoje interni CSIRT timovi u okviru samih organizacija kao što su banke, korporacije, univerziteti i vladine organizacije. Zatim, postoje nacionalni CSIRT timovi koji pružaju usluge na nivou cele države, kao na primer Japanski CSIRT tim (eng. Japan computer emergencz response team coordination center ili skraćeno JPCERT/CC). U svetu postoje i centri za analizu sintetizovanih podataka (prikupljenih podataka) koji određuju trendove i modeluju incidentne aktivnosti da bi se predvidele buduće aktivnosti i pružila rana upozorenja. Takođe, postoje i CSIRT provajderi koji nude svoje usluge odgovora na incidentnu, odnosno protipravnu aktivnost na zahtev klijenata.

- **Regularan shutdown** - Podrazumeva uklanjanje operativnih aktivnosti sa sistema(zatvaranje otvorenih fajlova, brisanje privremenih fajlova, mogućnost brisanja swap fajla). Takođe, shutdown može inicirati i uklanjanje malicioznog materijala (uklanjanje rootkita koji je bio u memoriji ili trojanski konj može da ukloni dokaze o malicioznim aktivnostima). Izvođenje shutdown operacije je moguće sa korisničkim nalogom koji ima dovoljno privilegija.
- **Isključenjem napojnog kabla iz struje** (ili vađenje baterije iz lap topa ili drugog prenosnog uređaja) - Ovim postupkom moguće je sačuvati swap fajlove, privremene fajlove i ostale informacije koje mogu biti izmenjene ili obrisane regularnim shutdown-om. Mana ovog postupka, jeste da naglim gubitkom struje fajlovi (najčešće su to otvoreni fajlovi ili fajlovi kojima je prustupljeno) na nekim Operativnim sistemima mogu da se oštete. Za neke korisničke uređaje kao što su PDA ili mobilni telefoni, uklanjanje baterije može za posledicu da ima gubitak podataka [96].

To znači da forenzičar prilikom donošenja odluke o isključivanju računarskog sistema mora dobro poznavati karakteristike ispitivanog Operativnog sistema kao i vrstu podataka koje treba da sačuva.

Ukoliko prvi odgovor vrši forenzički tim, vrlo je važno da se obezbedi zaštićena komunikacija između članova. U praksi se dalje vrše intervjui sa odgovarajućim osobljem, da bi se dobile relevantne informacije o incidentnoj/protivpravnoj aktivnosti. Bitno je da se na osumnjičenom računaru, na forenzički prihvatljiv način, pregledaju svi mogući izvori informacija uključujući fajervole, uređaje za nadgledanje mreže, svičeve i rutere. Svi računarski sistemi u mreži kao i mrežni uređaji su sumnjivi dok se ne sazna stvarna razmera incidenta. Cilj ove faze je da se prikupi što više informacija da se utvrdi, da li se incidentna radnja zaista desila i ako se desila u kolikoj meri će se to odraziti na poslovanje organizacije, odnosno da li spada u protivpravnu aktivnost nakon čeka bi otpočela zvanična istraga. Ukoliko je incidentna radnja učinjena, vrši se procena obima incidentne radnje, izdvajaju se neophodni resursi i definiše se neophodan nivo stručnosti, potreban za odgovor na nju. Na primer, u praksi koraci koji se ovde primenjuju su sledeći :

- ograničava se obim i intezitet incidentne radnje,
- proveravaju se integriteti računara na mreži,
- proveravaju se integriteti svih mrežnih uređaja na mreži,
- proveravaju se integriteti svih fajlova i direktorijuma na sistemu (cheksum),
- porede se sistemski fajlovi sa onima iz bekapa ili iz inicijalnih distribucija,
- uklanjanjaju se pojedinci koji predstavljaju potencijalne pretnje,
- isključuju se osumnjičeni ili ciljani računari sa mreže ili mrežnog uređaja,
- izbegava se logovanje na kompromitovani računar kao administrator (Windows OS), odnosno kao root korisnik (Linux OS),
- vrši se promena šifara na svim računarima koji nisu kompromitovani, ali koji se nalaze u istoj mreži kao i kompromitovan računar.

Na osnovu konsultovanja obimne literature koraci odgovora na incident mogu se grupisati na sledeći način :

- **Otkrivanje i prijava incidentne aktivnosti** - Za forenzičku istragu značajno je otkrio problem (korisnik, vlasnik programa, vlasnik sistema...).
- **Potvrda da se radi o incidentu ili protivpravnoj aktivnosti** - Za forenzičku istragu značajno je da li se radi o korisničkim, programskim sistemskim incidentima (greškama) ili protivpravnoj aktivnosti.
- **Pokretanje istrage** (korporacijske ili javne) - U zavisnosti od tipa maliciozne aktivnosti (DDOS napad, neovlašćeni pristup ili izmena podataka, neovlašćeno mrežno ispitivanje (eng. network probing), upotreba zlonamernih programa).
- **Oporavak kompromitovanih resursa** - Ukoliko je potrebno oporavak ugroženih sistema.

- **Izveštaj i preporuke za buduću zaštitu** - Identifikovanje slabosti u mreži i na sistemima i preporuke za poboljšanje bezbednosti.

Navedeni koraci dokumentuju se putem ček-liste Inicijalnog odgovora (primer ček-liste dat je u prilogu 1 ovog rada). Izuzetno je bitno da se vodi računa da se ne ugrozi digitalno mesto zločina. Fokus treba da bude usmeren na sledeće kritične detalje : trenutni datum i vreme, ko izveštava o incidentnoj aktivnosti, tip incidentne aktivnosti, kada se ona desila, koji je program odnosno uređaj obuhvaćen incidentnom aktivnošću, kao i kontakti osoba iz organzacije koji su obuhvaćeni digitalnom istragom.

Ukoliko je faza pripreme (više o tome bilo je reči u poglavlju 2.2.8 Model "Odgovor na incident") za incidentnu/protivpravnu aktivnost dobro realizovana, ova faza će biti u mogućnosti da smanji vremenski okvir, od detektovanja incidentne aktivnosti, do potvrde da li se radi o incidentnoj ili protivpravnoj aktivnosti (i u tom slučaju se pokreće zvanična istraga), kao i da se tačno i brzo odredi obim incidenta. Ova pripremna faza obezbeđuje obuku i opremu za lica koja će biti uključena u istragu incidenta [70].

Potrebno je istaći da čak i najspremnije (po pitanju bezbednosti) organizacije mogu biti suočene sa protivpravnim aktivnostima, kao što su dela prevare, krađe, upada u računarske sisteme, finansijske prevare, krađa intelektualne svojine, DDOS napadi, podmetanje malicioznih programa i drugih protivpravni aktivnosti.

Na primer, incidenti koji se dešavaju u okviru orgranizacije, uglavnom se odnose na sledeće probleme :

- gubitak ili curenje osetljivih (poverljivih) podataka,
- neprihvatljivo korišćenje računarskih resursa od strane zaposlenih,
- širenje malicioznih programa (na primer virusi, crvi, špijunski programi),
- računarski upadi od spolja,
- napadi tipa odbijanja servisa (na primer DOS, DDOS),
- manipulacija dokazima,
- prekid radnog odnosa sa zaposlenim koji je na ključnoj poziciji u IKT sistemu predstavlja vrlo ozbiljan sigurnosni problem,
- istraga nad drugim zaposlenim licima u IKT sistemu.

U odgovoru na incidentnu aktivnost u zavisnosti od obima i tipa incidenta i veličine organizacija učestvuje veliki broj lica. Tu se pre svega misli na korporacijiski tim za odgovor na incident (kod velikih kompanija) ili digitalnog forenzičara (kod manjih kompanija), vlasnika ili programera aplikacije, stručnjaka za bezbednosnost informacija, administratora sistema, administratora zaštitinih barijera, mrežnog administratora. Takođe, (u zavisnosti od tipa incidenta) mogu da učestvuju lica iz različitih oblasti, kao na primer, menadžeri poslovnih organizacija, advokati i tužioci kao predstavnici prava, nadležni državni organi, kadar tehničke podrške i krajnji korisnici odnosno vlasnici sistema. I zato je jako važno da se osoblje koje radi kao tehnička podrška, edukuje da razume na koji način napadači napadaju računarske sisteme i kako da uoče napade putem nadzora mrežnih aktivnosti.

Dakle, forenzički odgovor na incidentnu radnju/protivpravnu aktivnost podrazumeva ispunjavanje velikog broja različitih ciljeva kao što su :

- koordinisan odgovor na incident svih timova koji rade na istrazi,
- oporavak servisa na bezbedan način,
- dobijanje odgovora na pitanje da li se incident dogodio ili ne i da li je reč o protivpravnoj aktivnosti,
- prikupljanje preciznih informacija o incidentnim aktivnostima,
- procenjuje se obim i troškovi incidenta/protivprane aktivnosti,
- izvođenje oporavka podataka ili informacija nakon izazvane štete ili gubitka,
- uspostavljanje kontrole za pronalaženje i pravilno rukovanje digitalnim dokazima,

- identifikovanje izvora napada i motivacije (da li je tip zlonamerne aktivnosti poznat javnosti),
- poštovanje prava na privatnost utvrđenim zakonom,
- svođenje na minimum ometanja tekućeg poslovanja u mrežnom okruženju,
- omogućavanje sudskog postupka ili disciplinskog postupka (u okviru kompanije postupak protiv učinioca),
- obezbeđivanje tačnih i pravovremenih izveštaja sa preporukama,
- minimiziranje izloženosti tj. ugroženost vlasničkih podataka,
- zaštita imovine i ugleda organizacije,
- edukacija višeg menadžmenta u cilju boljeg sagledavanja i razumevanja bezbednosti,
- pomoć za brže detektovanje i/ili sprečavanje incidentnih/protivpravnih aktivnosti u budućnosti (učenjem kroz iskustva, izmenama politike i procedura u samim organizacijama).

3.5.5 Politika bezbednosti

Formulisanje sveobuhvatne i efikasne politike bezbednosti predstavlja, ideal bezbednosti računarskih sistema i mreža. Ona treba da bude prilagođena jedinstvenim karakteristikama organizacije uz obezbeđenje prihvatljive privatnosti zaposlenih. Skup jasno definisanih pravila koja obuhvataju sva područja na kojima je moguće izvršiti neku vrstu napada naziva se sigurnosnom tj. bezbednosnom politikom. Sigurnosnom politikom određuju se pravila ponašanja i odgovornosti koja se odnose na informacioni sistem, sa ciljem minimiziranja štete nastale namernim ili nenamernim delovanjem [143].
Prema Shimonskom, svrha bezbednosne politike jeste da se formalno navedu ciljevi, pravila i formalne procedure uz pomoć kojih je moguće definisati opšti bezbednosni položaj i bezbednosnu arhitekturu organizacije [173]. Pored toga, Shimonski ukazuje da bezbednosna politika mora sadržati i sedam važnih funkcija [173]: a. mora biti razumljiva, b. mora biti realna, c. mora biti dosledna, d. mora biti primenjiva, e. dokumentovana, distribuirana i pravilno prezentovana, f. fleksibilna, g. periodično preispitivana. Prema Wylupskom, Champion-u i Grant-u, politika bezbednosti treba da obuhvati i procedure od strane IT koje za cilj imaju preispitivanje bezbednosti posebno onih koji utiču na produktivnost i privatnost zaposlenih [90]. Bezbednosna politika se formira perma definisanoj imovini (hardver, programi, ljudski resursi) i procenjenog rizika. Jednu dobru strategiju za definisanje imovine (eng. assets), procesa u toku i procene rizika, predložio je Danchev u radu „*Building and implementing a successful information security policy"*. Imovina i procesi u toku moraju biti definisani kako bi se osigurala njihova zaštita [49]. Potrebno je prvo ustanoviti koja se imovina štiti, a zatim se vrši procena potencijalnih rizika. Predlaže se kreiranje liste imovine prema prioritetima, na osnovu kritičnosti za organizaciju (kategorije, sistemi, procesi). Procesom analize rizika potrebno je obuhvatiti, hardver, programe i mrežu. Pod hardverom se podrazumevaju svi serveri, radne stanice, prenosivi računari, prenosivi hard diskovi i drugi prenosni uređaji koji služe za skladištenje podataka (CD, DVD, BRD, USB flash i dr.). Kada je reč o mreži koja obezbeđuje spoljni pristup (svojim zaposlenima, korisnicima ili partnerima) neophodno je razmotriti bezbednost tačke pristupa mreži organizacije, bez obzira da li je reč o dial-up ili VPN pristupu. Shodno navedenom, neophodno je ograničiti pristup specifičnim programima, servisima ili serverima uz limitirano trajanje šifre. Neažurirani programi, servisi i sistemi, mogu dovesti do ranjivosti sistema, pa je neophodno politikom definisati i period skeniranja sistema na ranjivosti kako bi one bile blagovremeno identifikovane. U praksi potencijalne bezbednosne pretnje mogu se pojaviti upotrebom nezaštićenih programa, fajl šering programa (vuze, morpheus, kaza, E-donkey, torrent, e-mule i drugi), instant čat programa, progama za zabavu i drugih besplatnih programa nepoznatog izvora. Zato je potrebno izvršiti procenu rizika, identifikovati digitalnu imovinu

(eng. assets) i definisati nivoe pristupa sa principom dovoljnih privilegija neophodnim za obavljanje potrebnih aktivnosti. Digitalna imovina može obuhvatati i informacije iz organizacije (vlasničke podatke, korisničke podatke), intelektualna vlasništva i pristup servisima kao na primer e-mail, Internet i drugi. Politikom treba obuhvatiti i kreiranje grupa i privilegija svih onih koji koriste digitalnu imovinu u okviru organizacije na osnovu pozicije u organizaciji. Cilj kreiranja grupa, jeste upravljanje pristupom informacija uz pomoć autentifikacije, autorizacije i privilegija. Autentifikcija daje odgovor na pitanje ko se prijavljuje na sistem, autorizacija daje odgovor na pitanje šta želimo, a privilegije daju odgovor na pitanje, zašto želimo (čitanje, pisanje, izvršenje) [49]. Upravljanje rizicima u okviru bezbednosne politike mora se posvetiti posebna pažnja. Prema Danchev-u rizici su podeljeni na fizičke bezbednosne pretnje (zloupotreba šifri, virusna zaštita, prenosni uređaji, upravljanje incidentom) i Internet pretnje (Web pretraživanje, e-mail, instant messaging, download programa i otvaranje fajlova). Upotreba šifri i njihova bezbednost moraju biti pažljivo razmotrene. Na osnovu velikog broja literature i primera iz prakse upotreba šifri treba da ima sledeće karakteristike :

- mora da bude jedinstvena (jedan nalog jedna šifra);
- za šifru ne upotrebaljavati porodična imena, kućne ljubimce, matični broj,
- dužina šifre ne sme biti manja od 10 karaktera,
- šifra mora sadržati osim slova i brojeve i znakove,
- promenjena šifra ne sme biti slična prethodnoj tako što joj se pridoda broj na kraju (doktorskiR2D$ ne sme postati doktorskiR2D$1),
- šifra na sistemu i na svim programima ptreba biti podešena da automatski ističe posle određenog (definisanog vremena),
- ukoliko je moguće kreirati infrastrukturu sa javnim ključevima i upotrebljavati dvofaktorske ili trofaktorske mehanizme autentifikacije.

Kada je reč o virusnoj zaštiti, Danchev sugeriše da se u bezbednosnoj politici eksplicitno definišu ponašanja zaposlenih na računarskim sistemima i na Internetu kako bi se izbeglo izlaganje virusima. Preporuka je da se fajlovi i programi nepoznatog izvora nikada ne otvaraju. Svaki fajl ili program obavezno se moraju skenirati ažuriranim antivirusnim programom, pre njegovog otvaranja, bez obzira na ekstenziju koju ima, a najmanje jednom nedeljno je neophodno izvršiti antivirusno skeniranje kompletnog sistema (sa prethodno ažuriranim antivirusnim definicijama). Privremeno onemogućavanje antivirusnog programa treba biti zabranjeno, osim u izuzetnim slučajevima, usled privremenih intervencija nadležnih IT stručnjaka.

Upotreba prenosnih uređaja (USB flash, DVD, CD, floppy, trake i dr.) mora biti kontrolisana i ograničena na sisteme u okviru ogranizacije. Politikom treba onemogućiti pristup prenosnim medijima koji nisu vlasništvo organizacije, osim u izuzetnim slučajevima kada je nephodan pristup, ali uz nadzor IT stručnjaka sa prethodnom proverom na maliciozne programe.

Proces obavljanja periodičnog sistemskog bekapa i njegova verifikacija kao i održavanje računarskih sistema, moraju biti obuhvaćeni bezbednosnom politikom.

S obzirom da svaki bezbednosni upad ima svoje specifičnosti u svojoj bezbednosnoj politici, organizacija mora da ima prethodno definisan i implementiran plan inicijalnog odgovora koji pruža uvid u načine odgovora na ranjivost. Organizacija treba da ima u pripravnosti spreman tim obučenih kadrova sa mogućnošću upotrebe forenzičkih tehnologija za praćenje zloupotrebljenog exploita ili druge zlonamerne aktivnosti. O strategiji odgovora detaljnije će biti reči u sledećem poglavlju.

Za Internet rizike (Web pretraživanje, e-mail, instant messaging, download programa i otvaranje fajlova) prema Danchevu, neophodno je politikom pažljivo odrediti prihvatljivu upotrebu svake od aktivnosti koje mogu dovesti do kompromitovanja bezbednosti. To zapravo znači da je politikom neophodno definisati kada i na koji način zaposleni mogu da

pretražuju WEB, download-uju fajlove, otvaraju fajlove, koriste e-mail i druge servise. Pomenuti bezbednosni rizici moraju biti jasno predstavljeni, a aktivnosti moraju biti praćene u slučaju neodgovarajućih ili protivpravnih aktivnosti.

Udaljeni pristup putem VPN forme ili bežičnim putem jeste dobro za produktivnost, ali bez kontrole sistemi i mreža se izlažu bezbednosnim pretnjama. Sistemi koje koriste VPN i dalje su priključeni na Internet i shodno tome neophodno je regulisati aktivnosti. To zapravo znači da sistemi koji koriste VPN, obavezno moraju biti zaštićeni fajervolom i antivirusnim programom sa redovnom ažuriranošću, jer bez njih su i sistem i mreža ranjivi na upade. Treba imati na umu da su upotrebom WI-FI tehnologije računarski sistemi mobilnih korisnika (eng. Lap top users) u bezbednosnom smislu potencijalno ranjivi i da zlonamerni napadači mogu iskorišćavanjem ranjivosti da ukradu podatke, unesu viruse i izvrše različte maliciozne aktivnosti (širenje spama, DOS napadi). Najveći broj zloupotreba WI-FI ranjivosti se dešava prilikom korišćenja javnih hotspot lokacija. Prema istraživanju Wireless Broadband Alliance (WBA)[463] u saradnji sa Informa[464] organizacijom, početkom 2011. godine registrovano je 1.3 miliona javnih hotspot-ova sa tendencijom rasta na 5.8 miliona do 2015. godine[465]. Ova statistika govori, da će izloženost bezbednosnom riziku mobilnih korisnika biti u sve većem porastu. Na osnovu iznetog opravdano je bezbednosnom politikom onemogućiti pristup mreži mobilnim uređajima koji nisu pod kontrolom organizacije, odnosno u njenom vlasništvu.

Može se reći da dobra bezbednosna politika u organizaciji zapravo predstavlja uspostavljanje balansa između, sa jedne strane potreba korisnika i rizika koje te potrebe nose, a sa druge strane između zaštite i prihvatljive privatnosti. Politika bezbednosti mora biti dostupna svim zaposlenima, u elektronskom ili papirnom obliku. Prilikom njenog distribuiranja zaposleni treba da svoju saglasnost o pridržavanju u skladu sa bezbednosnom politikom potvrde svojim potpisom. Značajnije dopune, izmene i brisanja, se prosleđuju obaveštenjima u formi e-mail-a, govornom poštom i drugim sredstvima obaveštavanja. Dodatno, politikom je potrebno jasno i precizno definisati prihvatljive aktivnosti, nedozvoljene aktivnosti i lične aktivnosti zaposlenih (odobrenih uz saglasnost odgovarajućeg hijerarhijskog nivoa). Takođe je potrebno izraditi precizne liste i procedure sprovođenja disciplinskih postupaka u slučaju kršenja bezbednosne politike. Reviziju bezbednosne politike vršiti prema definisanom vremenskom periodu. Između ostalog njen cilj jeste ispravka i eliminisanje što većeg broja ranjivosti na sistemima i mreži, nakon stečenih novih znanja iz incidentnih aktivnosti i odgovora na njih. Iz navedenog može se zaključiti da je bezbednosnom politikom potrebno definisati digitalno forenzičku istragu računarskog (sigurnosnog) incidenta i njegovo rešavanje, skupom pravila, koja omogućavaju i olakšavaju oporavak sistema posle incidenta i time smanjuju njegov uticaj i sprečavaju ponavljanje računarskog incidenta.

3.5.6 Formulisanje strategije odgovora

Strategija odgovora mora biti obuhvaćena bezbednosnom politikom. To podrazumeva uključivanje nadležnih lica, odnosno donosioce odluka u organizaciji. Izuzetno je važno razumeti karakter incidenata, što podrazumeva svesnost problema, sagledavanje potencijalnog uticaja na poslovanje, moguće počinioce i razumevanje načina, na koji se način desila protivpravna aktivnost. Da bi strategija odgovora pružila zadovoljavajuće rezultate, neophodno je njome obuhvatiti izbor osobe koja će imati odgovornost za formulisanje strategije odgovora i odgovarajuće podjedince koji će učestvovati u realizaciji uspostavljene

[463] www.wballiance.com/
[464] http://www.informa.com/
[465] Izvor : http://www.telecompaper.com/news/global-public-wi-fi-hotspots-to-hit-58-mln-in-2015--837903

strategije odgovora na protivpravnu aktivnost. Zatim, bitno je odrediti prioritete organizacije i koliki je njihov uticaj na odgovor na protivpravnu aktivnost, kao i definisati izvodljive opcije odgovora u odnosu na prioritete. Treba uzeti u obzir sledeće faktore koji direktno utiču na strategiju odgovora na protivpravnu aktivnost :

- Koliko ja ugroženost kompromitovanog sistema ?
- Koji je tip incidentne radnje u pitanju - (na primer DOS napad, krađa, distribucija nedozvoljenog sadržaja, ugrožavanje privatnosti, vandalizam) ?
- Da li će se pokretati interna ili javna istraga ?
- Kolika je osetljivost podataka ?
- Da li je protivpravna aktivnost poznata javnosti ?
- Koliki je nivo postignutog neovlašćenog pristupa od strane zlonamernog napadača ?
- Ko su počinioci - unutrašnji ili spoljašnji napadač ?
- Kolika je veština napadača ?
- Koliki je vremenski zastoj na sistemu i koliko se on može tolerisati ? Na primer, ukoliko je kompromitovan server tako da je onemogućen neki bitan servis, donosi se odluka na koji način će se server povratiti u operativno stanje, odnosno da li će se njegov oporavak realizovati on-line ili post-mortem.
- Klasifikovanje kompromitovanog računara, ispitati da li je u pitanju server ili radna stanica korisnika.
- Procena ukupnog gubitka.
- Koliki su preostali raspoloživi resursi za rešavanje protivpravne aktivnosti ?

Ovom strategijom potrebno je definisati, ko treba da bude uključen u donošenje odluka i ko treba da rukovodi i da realizuje odgovor na protivpravnu aktivnost i korake koje treba sprovesti. Organizacija može da iskoristi bezbednosne incidente i kao sredstvo za obuku i za reviziju bezbednosne politike.

3.5.7 Nedostaci forenzičkog odgovora „Uživo“ i najčešće forenzičke greške

U prethodnim poglavljima date su najznačajnije prednosti u odgovoru na incidentnu/protivpravnu aktivnost "uživo" i koji sve podaci mogu biti pronađeni na određenim mestima značajnih, kako za forenzičku istragu, tako i sa stanovišta bezbednosti. U daljem tekstu biće navedeni i nedostaci odgovora "uživo".

Odgovor "uživo " zahteva upotrebu pripremljenih alata za odgovor "uživo", ali oni nisu apsolutno nezavisni od operativnog sistema. Takođe, zahteva se postojanje decentralizovanih off-site lokacija (eng. off-site location)[466] za odgovor na protivpravnu aktivnost i sa podrazumevanom obukom lica koja će da realizuju off-site odgovor na protipravnu aktivnost. Prilikom prikupljanja uživo doći će do promene vremenskih pečata (eng. stamps) datuma i vremena prikupljanih podataka (na primer vreme pristupa fajlu).
Neophodna je interakcija za dobijanje brojeva portova, broja particija i imena log fajlova i korisničke konfiguracije. Zahteva se administratorsko logovanje na svakoj konzoli.
Nije dozvoljena forenzička duplikacija "uživo". Dobijene informacije odnosno izlazi dobijeni forenzičkim alatima, nisu uvek dobro organizovani i pregledni. Odgovor "uživo" nije moguće uvek realizovati.

Na osnovu prakse i konsultovanja obimne literature najčešće greške mogu se grupisati na sledeći način :

- Kršenje zakona (Neovlašćeno oduzimanje (zaplena), prikupljanje dokaza, upotreba nelicenciranih programa kao i posedovanje ilegalnih programa).

[466] Kada se govori o off-site lokaciji misli se na off-site zaštitu podataka što podrazumeva slanje kritičnih podataka sa glavne lokacije odnosno van glavne lokacije tj. off-site lokacije. Može da se transportuje pomoću prenosivih medija za skladištenje podataka, kao na primer magnetne trake , optički uređaji i drugi uređaji slične namene. http://en.wikipedia.org/wiki/Off-site_data_protection, 16.03.2012

- Uništavanje dokaza (kroz pokušaj oporavka podataka, patchovanje sistema ili izmenom vremenskih i datumskih pečata, nad dokazima na sistemu ili „ubijanje“ zlonamernog procesa).
- Neuspešno održavanje kompletne dokumentacije (nebeleženje preduzetih koraka na sistemu, neuspešno dokumentovanje pronađenih dokaza u forenzičkom maniru).
- Neuspešno kontrolisanje pristupu digitalnim informacijama.
- Potcenjivanje obima incidentne radnje, odnosno protivpravne aktivnosti (podcenjivanje količine dokaza koji se mogu pronaći)
- Neblagovremena i neprecizna prijava incidentne radnje odnosno protivpravne aktivnosti (neuspešna prijava preciznih informacija donosiocima odluka, na primer prijava pogrešnog vremena ili vremenske zone).
- Neuspešno ili neblagovremeno obezbeđivanje tačnih informacija (predugo čekanje na prijavu incidenta)
- Nepostojanje plana za odgovor na incidentnu radnju, odnosno protivpranu aktivnost.

Da bi se navedene forenzičke greške eliminisale ili bar smanjile na prihvatljiv nivo u okviru organizacije, neophodno je postojanje plana, kontrolisanje njegovog sprovođenja, dokumentovanje svih preduzetih forenzičkih mera i izveštavanje. Međutim, čak iako se poštuju navedena upozorenje koja je odnose na greške, istraga može da se završi bez hvatanja počinioca, suđenja i sankcionisanja baš kao što navode G. Grubor i M. Milosavljević u svom radu [132][12], a razlozi su sledeći :

- Gubljenje traga – jer je prošlo suviše vremena od incidenta i nema dokaza;
- Nekompletno logovanje, ili ga uopšte nema;
- Cena istrage je veća nego gubici nastali usled incidenta i nije rentabilno nastaviti istragu;
- Veliki prostor skrivanja počinioca (Internet), a incident se dogodio samo jedanput, sa malo ili bez imalo dokaza;
- Incident nije sasvim određen – nije jasno da li je, ili nije bezbednosni incident;
- Ne može se nedvosmisleno ukazati na počinioca;
- Nema dovoljno dokaza da se nedvosmisleno dokaže slučaj;
- Postojanje političkog ili druge vrste pritiska da se istraga zaustavi;
- Zataškavanje istrage.

4. ISPITIVANJE RANJIVOSTI NA WINDOWS I LINUX PLATFORMAMA I MERE ZAŠTITE

Ranjivosti sistema predstavljaju hardverske i programske slabosti u vidu grešaka ili loše konfiguracije koje zlonamerni korisnik može kompromitovati. Upravljanje konfiguracijom, zakrpama i bezbednošću na sistemu su od pojedinačnih disciplina evoluirali u jedan IT problem koji se danas naziva upravljanje ugroženošću [116].
Nijedan sistem nije 100% siguran i svaki ima svoje ranjivosti. Razlozi leže u činjenici, što iako nema u datom momentu na sistemu prepoznatih programskih propusta, problemi vezani za bezbednosna podešavanja na sisemu i zloupotrebu funkcija programa, uvek su prisutni. Zbog velikog broja slabosti svojstvenih bezbednosnim podešavanjima na sistemu, zajedno sa mogućnostima zloupotrebe programskih funkcija i programskim propustima, u svakom trenutku postoje desetine, ako ne i stotine ranjivosti na samo jednom računarskom sistemu.

Ove ranjivosti imaju čitav niz različitih karakteristika. Neke od njih jednostavne su za zloupotrebu (eng. exploit), dok su za druge zloupotrebe ranjivosti potrebni određeni preduslovi. Sa nekim exploitima dobijaju se admin tj. root privilegije, dok drugi mogu obezbeđivati samo pristup sistemu sa difoltnim privilegijama. Upravo je analiza ranjivosti na sistemima jako značajna sa stanovišta zaštite, da bi organizacije mogle da znaju koji su propusti prisutni na sistemima, koliko je teško napadaču da ih iskoristi i kakvu bi posledicu izazvalo da se oni iskoriste. Bezbednost na sistemima može se sagledati i kroz moto Erica Cole-a : „Prevencija je idealna, ali je detekcija obavezna.“[467][468] Dakle, kada je zaštita u pitanju kako u organizaciji tako i u kućnim sistemima, postoje dve ključne komponente : prevencija i detekcija. Većina organizacija zaštitu na svojim sistemima fokusirala je na prevenciji, ali ne i na detektovanju zlonamernih aktivnosti. Na primer, većina kompanija na svojim sistemima ima instalirane fajervol-ove koji deluju preventivno. Tu mogu da se jave dva problema. Prvi je taj da organizacija ne može da spreči kompletan saobraćaj, što na neki način otvara mogućnost za potencijalni napad. Drugi problem leži u činjenici da preventivni mehanizmi nisu prilagođeni ili nisu ispravno konfigurisani, pa samim tim pružaju minimalnu zaštitu ili nikakvu. Uspostavljanjem samo preventivne mere, nije dovoljno da se spreči svaki napad. U tom slučaju ključno je, da oraganizacija mora da uspostavi svoju odbranu na takav način da prepozna pretnju (napadača) blagovremeno, pre nego što se desi kompromitovanje sistema.

Kada se radi o protivpravnoj aktivnosti tipa upada u računarski sistem, napadač će uvek ići linijom manjeg otpora. Upravo zato je izuzetno važno, da organizacija (baš kao i vlasnici kućnih računara) razume svoje slabosti na sistemima i da se ne koncentriše samo na jednu oblast zaštite. Na primer, nikada se ne treba oslanjati samo na Antivirusni program sa ciljem detektovanja malicioznih programa, iz više razloga. Prvo malicizno programi se brzo razvijaju i sistem može sadržati maliciozni program, a da ga antivirus kao takvog ne prepoznaje, jer jos nije uvršćen u antivirusnu bazu podataka. Drugo, veliki broj malicioznih programa imaju način da onemoguće antivirusnu zaštitu na sistemu, tako da skener na maliciozne programe ništa ne prijavljuje. Takođe, veliki broj regularnih programa se koristi na nedozvoljen način u svrhu protivprane aktivnosti. Dobar primer upotrebe regularne aplikacije na nelegalan način naveden je u radu S. Baker-a., P. Green-a, T. Meyer-a, i G. Cochrane-a “*Checking Microsoft Windows® Systems for Signs of Compromise*“ : FTP server jeste regularan program (servis) koji može biti instaliran od strane zlonamernog napadača sa ciljem hostovanja i distribucije nedozvoljenog materijala, a antivirusni program ga neće

[467] http://www.sans.edu/research/security-laboratory/article/honeypots-guide
[468] http://www.computerworld.com/s/article/82515/How_to_secure_your_company?nlid=SEC2

detektovati kao nešto maliciozno (pošto izgleda kao regularna aplikacija), jer ne ispituje način na koji se program koristi [11].

Zaštita se zapravo postiže neprekidnim ciklusom otkrivanja slabosti i njenog ispravljanja. Samo ukoliko postoji jasan stav o razumevanju bezbednosti računarskih sistema u okviru organizacije (jer otkrivanjem najslabije karike, neka druga karika postaje najslabija) i plan da se bezbednosni rizici smanje, mogu se prevazići i bezbednosni problemi.

Sa stanovišta bezbednosti cilj je pronaći najslabiju kariku i zakrpiti je (eng. patching), pre nego što je iskoristi zlonamerni napadač. Upravo to i predstavlja prozor ranjivosti (eng. Window of Vulnerability) termin koji se odnosi na upravljanje ranjivostima na sistemima. Prozor ranjivosti se odnosi na vremenski period u kome je sistem ranjiv na određeni bezbednosni propust, konfiguracioni problem ili neki drugi faktor koji smanjuje bezbednost na sistemu. Prema S. Manzuiku A. Goldu i C. Gatfordu razlikujemo dva prozora ranjivosti : [116] :

1. Nepoznati prozor ranjivosti – obuhvata vreme od otkrivanja ranjivosti do momenta kada je sistem obezbeđen od te ranjivosti tj. Pečovan.
2. Poznati prozor ranjivosti - obuhvata vreme od kada je proizvođač (eng. vendor) objavio zakrpu, do momenta kada je sistem obezbeđen od ranjivosti tj. Pečovan.

Iako većina organizacija obraća pažnju na poznati prozor ranjivosti izračunavanje nepoznatog prozora ranjivosti je dragoceno za planiranje strategije za ublažavanje štete.

Krajnji cilj je da se zakrpi dovoljan broj ranjivosti na sistemu koji će odbiti zlonamernog napadača zbog neuspešnih pokušaja upadanja na sistem. Većina proizvođača programa (sistema) ili hardvera nude zakrpe preko svojih mailing listi koji se odnose na bezbednost. Na primer, Microsoft bilten lista koja se tiče bezbednosti, a preko koje se dobijaju informacije o pitanjima i problemima koji se odnose na Microsoft proizvode, zove se „Microsoft Security Bulletins“ i dostupna je na web adresi http://technet.microsoft.com/en-us/security/bulletin . Bugtraq jeste jedna od prvih bezbednosnih mailing listi. Ukoliko se problem pojavi, skoro uvek će biti postavljen na ovoj listi i dostupna je na web adresi http://seclists.org/bugtraq/ . Treba spomenuti i VulnWatch listu koja ne spada u diskusione liste, ali se bavi isključivo objavljivanjem sigurnosnih problema i dostupna je na web adresi http://seclists.org/vulnwatch.

Osim u izuzetno malom broju slučajeva, nikada se ne mogu ukloniti svi propusti na sistemu. Baš zbog toga cilj jeste da se ili ukloni i ublaži najveći broj rizika koji će odbiti napadača ili da se napadač blagovremeno otkrije i spreči šteta. Veliki broj organizacija ne preduzimaju adekvatne bezbednosne mere, sve dok im se ne desi kompromitovanje sistema, odnosno nastanak štete. Suština je ta, da ukoliko se bezbednosni problem otkrije na vreme manje će štete imati organizacija, odnosno vlasnik računara. Što je više vremena proteklo od detektovanja napada, vreme za saniranje raste, a nastala šteta je veća.

Zaštita od zlonamernih napadača zahteva stalnu pažnju i nadzor, jer većina organizacija koja je priključena na Internet neće biti u stanju da spreči svaki napad. Zato napadač koji uspeo da iskoristi određeni propust na sistemu mora da se otkrije što pre. Naveo bih primer koji pokazuje koliko je važno da osim preventivnih mera postoje i mere za detektovanje. U jednoj organizaciji koja može mnogo da izgubi ukoliko njene ponude i spiskovi sa klijentima budu dostupne u javnosti, postavilo se pitanje procene bezbednosnih rizika. Taj predlog nije naišao na odobrenje, iz razloga što kompanija nije imala nikakvih bezbednosnih povreda u poslednje tri godine. Na pitanje koliko su imali napada na sajt, odgovor je bio da napadi nisu detektovani, jer nisu ni tražili napade. Način na koji su utvrdili da su napadani jeste na osnovu korisničkih žalbi ili na osnovu ometanja servisa što je za organizaciju bilo definisano kao minimalno ometanje, pa se nije dovodilo u vezu sa povredom bezbednosti. To znači da je za organizaciju jedini način utvrđivanja povrede bezbednosti bio ukoliko dođe do prekida servisa. To dalje implicira da je napadač mogao da

upadne u računarski sistem organizacije, zatim preuzme sve osetljive fajlove i iskoristi ih sa ciljem krađe klijenata. To u organizaciji ne bi primetili, jer napad nije ugrozio njihov servis. Posle određenog perioda javio se problem sa storidžom, a pripisan je korisnicima koji kopiraju velike količine fajlova. Nakon forenzičkog ispitivanja, konstatovano je sledeće : sistem za skladištenje podataka bio je prepun hakerskih alata i raznih exploita na sistemu, pronađeni su i maliciozni programi tipa Trojanaca na čak 13 servera, progrešno konfigurisan fajervol i nedostatak nadziranja log fajlova i mrežnih aktivnosti[469]. Takođe, pronađeni su i 5 naloga sa administratorskim privilegijama ali se nije znalo kome pripadaju. Iz svega može se zaključiti da je ova organizacija ozbiljno ugrožena, a da toga nisu bili svesni. Ispravljanje ovog problema trajalo je blizu 8 meseci i koštalo je organizaciju preko 150.000 evra. Da je organizacija imala odgovarajuće procedure koje se odnose na bezbednost sistema, nakon prvog upada zlonamernog napadača u sistem, napadač bi bio uhvaćen i organizaciji bi trebalo nekoliko sati da se očisti i zakrpi svoje ranjivosti.

Ono što iz iznetog sledi je, da sistem pored zaštitnih barijera mora da ima i sistem za detektovanje upada (IDS) koji zajedno sa forenzičarem predstavlja proaktivan pristup u bezbednosti sistema. To je ono čemu teži veliki broj organizacija, ali nažalost većina organizacija ne pridaju veliki značaj IDS-u i forenzičkoj analizi, dok se ne desi veća šteta. Velike ogranizacije koriste mamce tj. hanipot-ove (eng. Honeypot) kao vid proaktivnosti na svojim nezaštićenim delovima mreže, sa ciljem proaktivnog detektovanja upada na sistem.

Treba istaći da kada je u pitanju bezbednost sistema ne postoji "srebrni metak" kao jedinstveno zaštitno rešenje. Potrebno je imati višenivoiski pristup u zaštiti [103]. Na primer, fajlervol je dobar za početak, ali nije rešenje. Tek nakon dodavanja sistema za nadziranje IDS, većeg broja fajervola, aktivnog nadziranja logova, forenzičkog nadziranja, antivirusne zaštite, zaštićenog dial-up pristupa, VPN pristupa, kriptografski zaštićene komunikacije u okviru organizacije, upotrebe jakih šifara, liste za kontrolu pristupa i upotrebne analize ranjivosti približavamo se sigurnoj mreži i sigurnim računarskim sistemima. Ovakav pristup koji ima više mehanizama zaštite i naziva se višenivoiska zaštita (eng. defense in depth). Haneypot predstavlja postavljanje ranjivog računara (sa minimumom sigurnosti) na posebnom delu mreže kao mamac koji će privući potencijalnog napadača [90]. Cilj je zapravo nadziranje malicioznih aktivnosti programa ili napadača kako bi organizacija spremno odgovorila na takve aktivnosti. U svom radu B. Spernow je opisao na koji način Microsoft upotrebljava hanipot kao proaktivni element zaštite sa ciljem otkrivanja i sprečavanja upada [181].

Svrha ovog rada je da ukaže i na to, da ne postoji način da se računarski sistemi pravilno zaštite ukoliko se ne zna protiv čega je usmerena zaštita. Samo pravilnim razumevanjem protivpravnih aktivnosti, načina na koji se napadi dešavaju, šta maliciozni korisnici (napadači) rade kako bi kompromitovali sistem, učenjem od forenzičkih događaja i analizom ranjivosti računarskih sistema i odgovornošću zaposlenih, organzacija može da sprovede zaštitu na pravi način.

Analiza ranjivost pomaže organizaciji da na pravilan način eliminiše svoje slabosti štiteći računarske sisteme od zlonamernih aktivnosti malicionznih korisnika ili napadača. Zapravo pristup zaštiti na sistemima može se uporediti sa onim što je Sun Tzu rekao u "Art of War" : "*upoznaj neprijatelja i upoznaj sebe pa možeš osvojiti bitku i bez gubitaka*." Korišćenjem istih alata koji koriste zlonamerni napadači, da bi izvršili prodor na računarski sistem ili mrežu, mogu se pronaći i zakrpiti bezbednosne rupe na sistemu, pre nego što ih napadač iskoristi baš kao što je to naveo G. Kipper u svojoj knjizi [97]. Ukoliko se proaktivna analiza ranjivosti (bezbednosno skeniranje sistema), uz dokumentavanje ranjivosti na

[469] U većini slučajeva postojanje sistema za logovanje aktivnosti na mreži predstavlja i jedini način na osnovu koga je moguće utvrditi da li je u toku kompromitovanje sistema ili je već iskompromitovan. Samo ako se zna šta se dešava na mreži moguće je pravilno se odbraniti od napada. U većini slučajeva organizacije koje ne nadziru svoje logove one rizikuju da će biti kompromitivani a time i poslovni krah.

dosledan i metodičan način, sprovodi u redovnim intervalima, organizacija će biti svesna svojih potencijalnih bezbenosnih propusta od kritičnih do onih manje važnih.

To znači da će samo dobro pripremljeni računarski sistemi koji podrazumevaju proaktivni pristup zaštite zajedno sa uspostavljenom bezbednosnom politikom (in-depth) i procedurama biti odbranjeni od napadača (ili će ga odvratiti ili će ga sprečiti ili će biti brzo detektovan), a organizacija neće pretrpeti gubitak (ili će on biti mali).

4.1 PRIMERI RANJIVOSTI

U daljem tekstu biće navedene najčešće ranjivosti sa kojima se suočavaju, kako administratori sistema, tako i forenzičari pri analizi incidentnih i protivpravnih aktivnosti. Prikazana lista nije potpuna (niti može biti), ali može poslužiti kao polazna tačka za organizacije (vlasnike računarskih sistema) koje žele da obezbede svoje mreže i računarske sisteme. Ne treba da čudi što su mnoge ranjivosti prikazane u ovom radu iste baš kao i one publikovane od strane SANS (System, Administration Networking, and Security) instituta[470] i FBI istraživanja. SANS je napravio sjajnu klasifikaciju kroz top 20 najčešćih ranjivosti koje se odnose na operativne sisteme Linux i Windows. Lista u ovom radu obuhvata većinu SANS ranjivosti uz pridodate druge ranjivosti (prepoznatih uz pomoć analize ranjivosti, koja će biti prikazane u praktičnom delu rada) koje su prisutne na računarskim sistemima. Sve ove prikazana ranjivosti moguće je otkriti na osnovu analize ranjivosti (ili testom penetracije) [88]. Neke od prepoznatih ranjivosti mogu direktno da kompromituju sistem dok uz pomoć drugih je moguće dobijanje korisnih informacija koje napadaču mogu pomoći da oraganizuje napad.

Neki od njh se odnose na većinu operativnih sistema, a neki od njih su specifični za Linux odnosno za Windows operativne sisteme. U daljem tekstu biće opisane prepoznate ranjivosti, uz predložene adekvatne protivmere, da bi se ranjivost otklonila, a sistem zaštitio.

4.1.1 Opšte ranjivosti

1. Podrazumevane (eng. default) instalacije Operativnih sistema i aplikacija (posebna pažnja u ovom radu biće posvećena upravo analizi operativnih sistema nakon difoltne instalacije Linux i Windows operativnih sistema u poglavlju 4.3), nose sa sobom velike bezbednosne rizike. Na primer, mogu se pojaviti nezaštićeni korisnički nalozi - nalozi bez šifre. Dešava se da se sistemi isporučuju sa korisničkim nalozima bez šifara ili sa poznatim fabričkim šiframa ili sa aktivnim gost (eng. guest) nalogom bez šifre. U slučaju da korisnici zaborave da postave šifru, odnosno promene podrazumevanu šifru, to daje prostora zlonamernim napadačima da lako realizuju upad u računar. Opasnost leži u činjenici da potencijalni napadač može dobiti kompletnu kontrolu nad sistemom. To znači da napadač može dobiti jednostavan pristup sistemu (preko nezaštićenog naloga, kao na primer guest) i pokrenuti neke od exploit alata na sistemu sa ciljem dobijanja pune kontrole nad sistemom. Čak i ako administrator promeni šifru difoltnog naloga, taj nalog će i dalje biti meta zlonamernog napadača koji će uz pomoć upotrebe "brute force" alata pokušati da pogodi šifru.

   Rešenje : *Na svakom računarskom sistemu obavezno promeniti root šifru (na Linuxu), odnosno preimenovati administratorski nalog i promeniti administratorsku šifru, onemogućiti guest nalog, prekontrolisati sve postojeće naloge (obrisati sve defaultne naloge) i podesiti nove šifre, pre puštanja sistema u produkciju. Savet je da*

[470] SANS lista klasifikovanih ranjivosti http://www.sans.org/top20/2005/#w5, 26.04.2012

se sa programima za proveru šifara otkriju slabe šifre na sistemu i blagovremeno ih promeniti.

2. Instalirani servisi na default Operativnom sistemu – U praksi je vrlo čest slučaj da se pri instalaciji programa ili Operativnog sistema instaliraju i startuju servisi bez znanja onog ko vrši instalaciju. Na primer, određene Linux distribucije po difoltu instaliraju servise kao na primer Sendmail, rstat, FTP koji nisu podrazumevano nužni, a koji predstavljaju potencijalnu ranjivost na sistemu. Takođe, na Windows NT sistemima difoltna instalacija ponuđena je sa servisom IIS (Internet Information Server). Fluktuacija sistem administratora u organizaciji je vrlo česta pa novi administrator sistema ne može identifikovati sve servise koji rade na sistemima, pa samim tim ne može imati uvid u njihove ranjivosti.

   Rešenje : *Analizom ranjivosti (ili pentracionim testom) moguće je otkriti servise kojih administrator nije bio svestan. Takođe, potrebno je detaljno proučiti dokumentaciju programa ili sistema koji je potrebno instalirati. Novi administrator sistema treba da utvrdi koji su servisi pokrenuti na sistemu za koji će biti odgovoran. Dodatno potrebno je periodično vršiti skeniranje servera sa port skenerima za proveru da li postoje novi servisi. Na fajervolu je potrebno blokirati sve nepotrebne portove kako bi se sprečio zlonamerni napad na servis koji je greškom pokrenut.*

3. Upotreba nezaštićene komunikacije (eng. clear text , eng. unencrypted data) : servisi na sistemu konfigurisani da prenose sve informacije u čistom tekstu predstavljaju ranjivost, kako na sistemu, tako i u mreži. To znači da se informacije koje putuju kroz mrežu prenose u nezaštićenom obliku. Mnogi HTTP serveri koriste BASIC autentifikacioni mehanizam. Ovo je vrlo jednostavna šema koja koristi base64 način kodiranja cleartext formata korisničkih imena i šifri. Ukoliko je zlonamerni napadač u mogućnosti da prati HTTP saobraćaj (na primer sa sniffer-om) može ukrasti imena korisnika i šifre dekodiranjem tih base64 zaštićenih podataka, da bi obezbedio neovlašćen pristup sistemu. WEB servisi sa konfigurisanom „basic“ autentifikacijom, ftp, telenet su samo neki od primera koji omogućavaju komunikaciju u slabo zaštićenom obliku ili u formi „čistog teksta“ .

   Rešenje : *Izbegavati upotrebu servisa koji omogućavaju komunikaciju u čistom tekstu. Umesto njih upotrebljavati servise koji omogućuju zaštićenu komunikaciju kao na primer SSH i HTTPS (HTTP over TLS/SSL). Segmentiranja mreže sa korišćenjem VLAN-ovim (eng. virtual local area networks) na svičevima i ruterima može pomoći u zaštiti od sniffer-a.*

4. Ranjivosti zbog dozvola nad fajlovima (eng. file permissions) – Upotreba nedgovarajućih dozvola nad fajlovima može biti potencijalni bezbednosni problem iz nekoliko razloga. Kao prvo dozvole nad fajlovima ne određuju samo pristup nekom fajlu. nego i mogućnost pokratanja programa na sistemu. Drugo, određeni programi su pokrenuti u ime korisnika sa najvećim privilegijama, pa se lošim konfigurisanjem privilegija nad ovim programima može desiti da napadač dobije veća prava pristupa. U praksi se dešava da su određeni programski direktorijumi podešeni tako da grupa “everyone“ ima sva prava (pod Windows-om pod Linuxom bi to bila grupa „other“), što ostavlja zlonamernim napadačima otvorena vrata na sistemu.

   Rešenje : *Periodično pregledati dozvole nad fajlovima i folderima i postaviti ih na najrestriktivniji mogući nivo koji omogućuje neophnodnu operativnost u mreži sa deljenim resursima.*

5. Ranjivost usled korišćenja slabih šifri – Jedna od najvećih ranjivosti na sistemu jeste upotreba slabih šifri za autentifikaciju i slabih autentifikacionih metoda. I pored

postojanja načina da se zapamte jake šifre, u praksi je čest slučaj da korisnici izaberu šifre koje se lako pamte, a koji su nebezbedne. Razlog je uglavnom nedostatak svesti o bezbednosti kod korisnika. Novi tzv. crack-password progarami su u stanju da razbiju šifru koja se nalazi u rečniku za manje od minuta. Ovi programi, takođe su u stanju da lako razbiju i male modifikacije sa rečima iz rečnika kao na primer dodavanjem broja ispred ili iza reči, permutacija reči unazad. Veoma je čest slučaj da korisnici upotrebljavaju još jednostavnije šifre kao na primer imena, datumi, sportski timovi i druge činjenice koje se mogu lako pretpostaviti, čineći šifre još ranjivijim. Međutim, u praksi se dešavaju i situacije u kojima se najmoćnijim nalozima (admin, root) daju slabe šifre da bi više administratora moglo da zapamti tu šifru, ili se šifre ne ažuriraju na redovnoj osnovi.

Rešenje: *Svaki administrator mora da ima svoj nalog koji pripada grupi "administrators" (kod Windows sistema), odnosno prijava administratora na svoj nalog i upotreba komande „su" odnosno „sudo" prilikom izvršenja admin operacija (kod Linux sistema). Korisnici i administratori moraju da odaberu jake šifre koje sadrže upotrebu velikih i malih slova, brojeva i znakova sa minimum 10 karaktera bez upotrebe reči iz rečnika. Šifra se mora podesiti da ističe često (u zavisnosti od pristupa osetljivim informacijama) uz sprečavanje upotrebe starih šifri. Ima dosta alata za testiranje šifri koji se mogu naći na Internetu, a najčešće korišćeni su L0phtCrack*[471] *i John the Ripper*[472]*. Na Windows računarskim sistemima u politici administriranja sistema, potrebno je zahtevati upotrebu jakih šifri (eng. strong password enforcement). Postupak je prikazan u Microsoft dokumentu „Strong Password Enforcement and Passfilt.dll"*[473]*. Da bi se dodatno zaštitila SAM (Security Accounts Management) baza*[474] *na Windows sistemima, moguća je upotreba SysKey alatke prema preporuci Microsoft-a*[475]*. Cilj upotrebe ove alatke jeste dodavanje drugog sloja zaštite nad heširanim šiframa. Na starijim Linux sistemima (kao na primer Slackware 2.3, Slackware 3.0) obavezno omogućiti shadowing šifri (čime se omogućava pristup heširanim šiframa samo root korisniku) uz pomoć* Shadow Suite-a[476]*. Kad je reč o autentifikacionom problemu treba istaći da se u praksi većina sistema oslanjaju na upotrebu korisničkih imena i šifri, matičnih brojeva ili kolačića kao autentifikacione mehanizme. U praksi forenzičke analize zlonamerni napadači su zaobilazili pomenute autentifikacione mehanizme i dobijali neovlašćen pristup nalogu, podacima i servisima. Ključ za poboljšanje bezbednosti na sistemu jeste upotreba jakih autentifikacionih mehanizama kao što je postojanje PKI, korišćenje digitalnih sertifikata, smart-kartica, jednovremenskih šifri, dvofaktorske autentifikacije (nešto što korisnik ima-Token i nešto što korisnika zna-PIN) ili trofaktorske autentifikacije (nešto što korisnik ima-Token, nešto što korisnika zna-PIN i nešto što jeste - biometrija) u zavisnosti od osetljivosti podataka na sistemu. Pomenuti mehanizmi za proveru identiteta su odlični primeri za poboljšanje bezbednosti na sistemu ali su veoma skupi i složeni za implementaciju pa je to jedan od razloga što nisu dostupni na većini sistema.*

6. Ranjivost usled korišćenja šifri koje ne ističu - Postavljene šifre koje ne ističu predstavljaju bezbednosni propust. Time se omogućava napadaču efikasniji brute force napad na šifre. Ovaj napad može imati više uspeha ukoliko je na sistemu podešeno da lozinka ne ističe.

[471] http://www.l0phtcrack.com/
[472] http://www.openwall.com/john/
[473] http://msdn.microsoft.com/en-us/library/Windows/desktop/ms722458%28v=vs.85%29.aspx
[474] SAM baza sadrži kopije heš vrednosi korisničkih šifri.
[475] http://support.microsoft.com/kb/310105
[476] http://www.tldp.org/HOWTO/Shadow-Password-HOWTO-3.html

Rešenje : *Podesiti isticanje korisničkih šifri. Ukoliko se korisnički nalog ne koristi, obrisati ga ili ga onemogućiti. Kod Microsoft Windows sistema, ukoliko je u pitanju nalog koji je ugrađen (eng. built-in) u sistem kao na primer IUSR_ ili IWAM_ , podesiti za njih opciju "User cannot change password" da se prikazuje kao ranjivosti u izveštaju (Microsoft-ova preporuka je da se sistemskim nalozima zabrani izmena šifri). Sa druge strane omogućiti isticanje šifri nečekiranom opcijom "Password never expires".*

Za Microsoft Windows Vistu, Microsoft Windows Server 2008 postupak je sledeći :

a. Otvoriti Windows Control Panel.
b. Odabrati "Administrative Tools".
c. Da bi se promenile domain-wide lockout policy, odabrati "Domain Security Policy" (ili "Domain Controller Security Policy" ukoliko je računar domenski kontroler). U slučaju da se ova politika menja na lokalnom računaru odabrati "Local Security Policy."
d. Proširiti folder "Account Policies" i odabrati "Password Policy".
e. Podesiti Maximum Password Age. Ova vrednost predstavlja maksimalnu dužinu trajanja šifre. Preporučena vrednost može kreće da se između 30 i 90 dana u zavisnosti od privilegija naloga.
f. Restartovati sistem da bi se efekti primenili.

Za Microsoft Windows 2000 Server, Microsoft Windows Server 2003 postupak je sledeći :

a. Otvoriti "Administrative Tools" iz Control panel-a.
b. Dvokliknuti na "Active Directory Users and Computers".
c. Dvokliknuti na željenog korisnika.
d. Kliknuti na "Account" tab.
e. Odčekirati "Password never expires".

Za Microsoft Windows XP Professional i Windows 2000 Professional postupak je sledeći:

a. Desni klik na "My Computer";
b. Odabrati opciju "Manage";
c. Otvoriti folder "Local Users and Groups";
d. Otvoriti folder "Users";
e. Dvokliknuti na željenog korisnika;
f. Odčekirati "Password never expires".

Za Microsoft Windows NT postupak je sledeći :

a. Kliknuti na dugme "Start" na Task Bar-u;
b. Odabrati folder "Programs";
c. Odabrati folder "Administrative Tools";
d. Odabrati "User Manager";
e. Dvokliknuti na željenog korisnika;
f. Odčekirati "Password never expires".

Kod Linux operativnih sistema upravljanje isticanjem korisničkih šifri radi se sa alatom „chage“ :

```
# chage –M dužina_dana korisničko_ime
```

7. Ranjivosti CGI[477] (eng. common gateway interface) - CGI ranjivosti mogu se pronaći na velikom broju WEB servera. CGI programi omogućuju interaktivnost na WEB stranici kroz prikupljanje informacija, pokretanje programa ili pristup direktorijumima i fajlovima. S obzirom da se CGI programi pokreću sa istim privilegijama kao i WEB server program, to za posledicu može imati da zlonamerni napadač koji zloupotrebi ranjiv CGI može izmeniti WEB strane (ili obrisati), pristupiti osetljivim informacijama ili komrpomitovati sistem.

   Rešenje : *WEB servisi ne smeju da se pokreću u ime administratora ili root-a. Programski interpretori kao što su „perl" i „sh" ne smeju se nalaziti u direktorijumu CGI programa. Njihovim ostavljanjem zlonamerni napadači mogu izvršiti maliciozne CGI skripte. Vršiti analize ranjivosti sa ciljem pronalaženja ranjivih CGI programa i primenom adekvatne zakrpe, sistem će se zaštititi od pomenute potencijalne ranjivosti.*

8. FTP i Telnet ranjivosti – Korišćenje ftp i telenet servisa predstavlja potencijlni bezbednosni problem zbog uspostavljanja nezaštićene komunikacije. U praksi je čest slučaj da sistemi sa omogućenim FTP servisom dopuštaju anonimno logovanje (preko usera anonymous). Korisnik anonymous ima isključivo privilegije za čitanje, ali svako pravo čitanja može se zlupotrebiti za sticanje dodatnih informacija potrebnih zlonamernom napadaču za kompromitovanje sistema. Nepravilnim konfigurisanjem korisnik anonymous može da dobije prava upisa ili čak mogućnost da pristupa direktorijumima van FTP okruženja (na primer u pod Linuxom /etc/passwd, /etc/shadow, ili pod Windowsom /winnt/repair/sam.*). Dodatno mnoge verzije FTP servera imaju ranjivosti koje mogu da dovedu do kompromitovanja računarskog sistema. Na primer određena verzija WFTP servera je imala ranjivost na nekoliko buffer overflows napada sa kojima bi zlonamerni napadač nakon izvršenog koda dobio pristup strukturi fajlova i direktorijum na sistemu [51].

   Rešenje : *Ukoliko telnet i FTP servisi nisu potrebni na sistemu, njih treba ukloniti nakon difoltne instalacije sistema. Umesto njih koristiti SSH i SFTP servise koji obezbeđuju zaštićenu (šifrovanu) komunikaciju. U cilju povećanja bezbednosti bitno je da administratori na sistemu ograniče login pristup sistemu za pomenute aplikacije prema IP adresama uz pomoć TCP Wrapper-a ili upotrebe Denyhost programa*[478].

9. ICMP ranjivost – Icmp je čuven na osnovu korišćenja ping i traceroute (ili tracert) alata (koji generiše icmp pakete) i mnogih drugih dos alata. Ranjivosti ICMP se vezuju za dobijanje informacije o mrežnoj masci, vremenskih pečata i drugih korisnih informacija. U praksi je čest slučaj da se ICMP saobraćaj ne blokira u organizacijima u okviru svojih rutera i fajervola. Razlog jeste taj, što se ping i traceroute alati koriste za rešavanje mrežnih problema na računarima ili mrežnim uređajima (provera rada mrežnih kartica) i detektovanje mesta gde nastaju greške u mrežnoj komunikaciji. Međutim, napadači upravo preko ping komandi su u mogućnosti da identifikuju potencijalne mete. Onemogućavanjem upotrebe ICMP komunikacije u bezbednosnom smislu otežaće se skeniranje mreže od strane zlonamernih napadača. Određeni programi za skeniranje mreže su konfigurisani da ne skeniraju sisteme koji ne reaguju na ping-ovanja.

   Rešenje : *Upotrebu ICMP komunikacije bi trebalo zabraniti na ruteru i fajervolu u okviru organizacije. Ukoliko je ona neophodna zbog potreba rešavanja*

[477] CGI je vrsta programskog jezika kojeg programeri koriste da bi se prikazalo i isčitalo ono što se unosi u web pretraživač (eng. web browser) i omogućava pravljenje dinamičkih web strana. U stvari predstavlja jedan od načina za programe i skripte na serveru kako da komuniciraju sa web pretraživačima .

[478] Dostupno na http://denyhosts.sourceforge.net/

mrežnih problema, ograničiti je samo na određene računarske sisteme. Na operativnim sistemima to se može uraditi na prikazane sledeće načine.

Za Windows 2000 onemogućavanje ICMP timestamps odgovora vrši se uz pomoć IPSec filter-a na osnovu definisanja i primerne IP filter liste koja blokira ICMP types 13 (timestamp request) ICMP type 14 (timestamp response). Mogućnost blokiranja ICMP timestamps-a preko podešavanja u okviru "Networking and Dialup Connections" nije moguće. Detaljan opis korišćenja IPSec IP filter listi pod Windows 2000 prikazano je u Microsoft dokumentu „How to use IPSec IP filter lists in Windows 2000“[479].

Za Windows XP i Windows 2003 onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola :

a. *Network Connections control panel.*
b. *Desni klik na Network adapter i odabrati opciju "properties".*
c. *Odabrati tab "Advanced".*
d. *Pod Windows Firewall box-om, izabrati "Settings".*
e. *Selektovati tab "General".*
f. *Omogućiti fajervol selektovanjem opcije "on (recommended)".*
g. *Odabrati tab "Advanced" tab.*
h. *U ICMP box-u, odabrati opciju "Settings".*
i. *Deselektovati opciju "Allow incoming timestamp request".*
j. *Odabarti opciju "OK" i snimiti podešavanja za ICMP Settings.*
k. *Odabarti opciju "OK" i snimiti podešavanja za Windows Firewall dijaloga.*
l. *Odabarti opciju "OK" i izaći iz Internet adapter dijaloga.*

Za Microsoft Windows Vista i Microsoft Windows Server 2008 onemogućavanje ICMP timestamps odgovora vrši se preko komandne linije alatom „netsh“ :

a. *Otvoriti Windows Control Panel.*
b. *Odabrati "Windows Firewall".*
c. *Odabrati "Change Settings".*
d. *Omogućiti fajervol odabirom opcije "on (recommended)".*
e. *Otvoriti Command Prompt.*
f. *Ukucati komandu "netsh firewall set icmpsetting 13 disable".*

Više detalja oko podešavanja fajervola izloženo je u Microsoft-ovoj dokumentaciji[480]. Najefikasniji i najjednostavniji način onemogućavanja ICMP komunikacije jeste konfigurisanje fajervola da bolokira dolazne i odlazne ICMP pakete tipa ICMP 13 (timestamp request) i tipa ICMP 14 (timestamp response).

Za Linux OS :

Na žalost na Linuxu nije moguće modifikacijom parametra kernela preko sysctl (kao kod OpenBSD[481]) ili preko /proc/sys/net/ipv4 interfejsa onemogućiti ICMP timestamp responses, već se to radi uz pomoć fajervola iptables. Na primer :

ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP

10. Ranjivosti usled nedostatka monitoringa i detekcije upada - Nedostatak monitoringa i detekcije upada, za posledicu može imati neprimećeno testiranje slabosti računarskih sistema ili neprimetan upad na sistem od strane zlonamernog napadača. U praksi česta

[479] http://support.microsoft.com/kb/313190
[480] http://www.microsoft.com/resources/documentation/Windows/xp/all/proddocs/en-us/hnw_understanding_firewall.mspx?mfr=true
[481] Kod OpenBSD sistema onemogućavanje ICMP timestamp odgovora (eng. responses) se vrši podešavanjem "net.inet.icmp.tstamprepl" varijable na nulu : # sysctl -w net.inet.icmp.tstamprepl=0

su sledeća tri slučaja : ne vrši se monitoring ili ne postoji sistem za detektovanje upada, sistem za detekciju postoji, ali nije pravilno iskonfigurisan i sistem za nadziranje postoji, ali se ne proverava redovno. Ukoliko se ne detektuju pokušaji upada na sistem napadač može upotrebljavati veliki broj alata (na primer brute-force napad), dok ne prepozna određene slabosti na sistemu, da bi na kraju izvršio i kompromitovanje sistema.

Rešenje : *Postojanje odgovarajućeg sistema za praćenje i detekcije upada su od suštinskog značaja za bezbednost sistema što ujedno predstavlja i rešenje pomenute slabosti.*

11. Ranjivosti SMTP (Simple Mail Transport Protocol) servisa - SMTP predstavlja osnovni protokol sloja aplikacija za elektronsku poštu, koji koristi uslugu pouzdanog transfera podataka protokola TCP[482]. Definisan je u dokumentu RFC 821[483]. Postoji veliki broj implementacija SMTP servisa kao na primer Sendmail, Postfix, Qmail, Novell GroupWise, Exim, Novel Netmail, Microsoft Exchange Server. Svaka SMTP implementacija ima svoje ranjivosti i u praksi su se pokazale sličnim. Ranjivost Sendmail SMTP implementacije biće prikazana u daljem tekstu. U praksi iskorišćavanje SMTP ranjivosti realizuje se sa exploitima koji mogu da izvode prepunjavanje bafera (eng. buffer overflow), slanje spam poruka kao i onemogućavanja servisa.

    Rešenje : *Upotreba najnovijih implementacija SMTP servisa. Konstantno praćenje informacija koje se odnose na ranjivist i primena poslednjih zakrpa za SMTP servis.*

12. Ranjivost usled postojanja pokaznih tj. fajlova primera (eng. sample files) na WEB serveru – U praksi sa instalacijom WEB servisa po difoltu dolaze i fajlovi sa primerima za pomoć pri instalaciji i konfigurisanje servisa. Microsoft IIS [484] , Apache[485], Adobe ColdFusion[486], Oracle iPlanet Web Server[487] i drugi Web serveri takođe dolaze sa pomenutim pokaznim fajlovima. Ovi fajlovi, iako su veoma korisni administratorima za konfigurisanjem servisa i programerima za razvoj WEB servisa, mogu biti ranjivi kao na primer IIS Showcode.asp[488]. U praksi zlonamerni napadači kompromituju poznati kod iz pokaznih fajlova, tako da on izvršava neautorizovane funkcije. S obzirom da napadači poznaju lokacije ovih fajlova na sistemima, mogu planirati precizan napad na njih.

    Rešenje : *Najbolja odbrana ovih fajlova jeste njihovo uklanjanje sa WEB servera. Ipak, ukoliko su oni neophodni izvršiti njihovo premeštanje na druge lokacije tako da ne budu na produkcijskim sistemima. Dodatno izvršiti skeniranje ranjivosti sa ciljem identifikovanja slabosti koje se odnose na WEB servise.*

13. Ranjivost usled pristustva virusa i skrivenog malicioznog koda – Bezbednosne pretnje od virusa variraju u zavisnosti od tipa zlonamernih aktivnosti koje će se izvršiti. Dok neki virusi donose samo jednostavne neprijatnosti, drugi omogućavaju neautorizovan pristup računarskom sistemu, onemogućavanje servisa i mnoge druge protivpravne aktivnosti. Kada su virusi u pitanju. široko rasprostranjeni problem nastao je zbog sposobnosti zlonamernih napadača da vešto sakriju maliciozni kod. Na taj način

[482] http://sr.wikipedia.org/sr/SMTP
[483] http://tools.ietf.org/html/rfc821
[484] http://www.iis.net/
[485] http://httpd.apache.org/
[486] http://www.adobe.com/products/coldfusion-family.html
[487] http://www.oracle.com/technetwork/middleware/iplanetwebserver-098726.html
[488] http://www.securityfocus.com/bid/167

korisnik nesvesno izvršava ovaj kod čime može biti ugrožena bezbednost sistema ili mreže u okviru organizacije. Antivirusni skeneri su prilično napredovali ali njihova efikasnost bazirana je na ažuriranosti virusnih definicija. Problem se javlja kada se pojavi novi virus koji nije uvršćen u antivirusne definicije. Antivirusni skener ga neće prepoznati i on može biti propušten. Antivirusni alati koji primenjuju heuristično pristup i sandbox mogu biti od koristi za pronalaženje novih nedefinisanih virusnih pretnji. Heuristika podrazumeva sistemsku pretragu na zlonamerne kodove ili programe koji liče ili koji bi mogli biti virusi. Sandbox pristup podrazumeva izvršavanje koda u strogo konrolisanom okruženju (karantin) ispitujući njegove aktivnosti. Ukoliko je program prepoznat kao virus, on se pakuje u karantin i šalje se upozorenje o virusu. Heuristika i sandbox su od velike pomoći za prepoznavanje virusa koji još nisu uvršćeni u najnovije virusne definicije. Pomenuto skrivanje malicioznog koda je u direktnoj vezi sa virusima. Zlonamerni napadač može prevariti korisnika tako da korisnik nije svestan da je pokrenuo zlonamerni kod i omogućio napadaču pristup internoj mreži ili sistemu. Na primer, zlonamerni napadači mogu da sakriju zlonamerni JAVA ili Active X kod na udaljenom WEB serveru. Prilikom pretraživanja strana na malicioznom WEB serveru korisnik neznajući pokreće zlonamerni kod čime kompromituje sistem. Takođe, u praksi je čest slučaj da je zlonamerni kod ubacivan u elektronske poruke ili atačmente poruke. Izvršenjem tih kodava ili skripti iz elektronskih poruka, otvara se pristup kako samom sistemu omogućujući napadaču zaobilaženje fajervila i drugih vidova kontrole, tako i direktan pristup internoj mreži.

Rešenje : *Uklanjanje ranjivosti ovog tipa, podrazuma slojevit pristup zaštiti. Na prvom mestu jeste edukacija korisnika o riziku koji nosi otvaranje elektronske pošte nepoznatog porekla. Postojanje antivirusnog servera sa heurističnim skeniranjem pozicioniran je na tački pristupa mreži (na samoj granici) na mestu gde može da se skenira sva elektronsku pošta, atačmenti i Internet download-i pre njihovog ulaska u mrežu. Zaštitom na osnovu upotrebe slojevitog skeniranja (heuristika, desktop skeniranje, skeniranje gateway-a) povećavaju se šanse za zaustavljanje onih virusa koji su zaobišli prvu ili drugu liniju odbrane od virusa. Dodatno, onemogućiti pokretanje udaljenih (eng. remote) JAVA i Active X skripti na WEB pretraživačima.*

4.1.2 Ranjivosti na Windows sistemima

1. Postojanje UNICODE ranjivosti na IIS serveru kod Operativnih sistema Windows NT, i Windows 2000[489] - IIS predstavlja Web server koji je prisutan na Microsoft Windows familiji servera. Nekoliko malicioznih programa (crva, eng. worm) tipa Red Worm, Red Worm II i Nimda, su isprogramirani da zloupotrebe IIS Unicode ranjivost. Iskorišćavanjem ovih ranjivosti, osim omogućavanja zloanamernim napadačima administratorske privilegije (mada ne nužno), moguće je i pokretanje zlonamernog koda na kompromitovanom sitemu sa eskaliranjem daljeg kompromitovanja. UNICODE ranjivosti se mogu vizuelno otkriti u log fajlovima zbog karakterističnog znaka „%“ praćenog brojevima kao na primer „%255a“ ili „%a1%1a“ (kao NIMDA crva)[490].

   Rešenje : *Sisteme je moguće zaštiti od ovih ranjivosti instaliranjem najnovijih bezbednosnih update-a i service pack-a. Preporuka je da se ne koriste difoltna imena*

[489] http://www.sans.org/security-resources/malwarefaq/wnt-unicode.php
[490] http://www.sans.org/security-resources/idfaq/iis_unicode.php

za direktorijume i deljene resurse prilikom instalacije IIS-a uz pažljivo postavljanje dozvola na direktorijumima. Takođe, izvršiti onemogućavanje svih nepotrebnih funkcija i ekstenzija u okviru IIS-a[491].

2. Programske ranjivosti – predstavljaju opštu kategoriju koja se odnosi na programske greške ili propuste koji omogućavaju zlonamernim napadačima da izvrše kompromitovanje sistema. Na primer, ranjivost Compaq Web-Based Management buffer overflow može da omogući napadaču da iskopira SAM fajl na Windows serveru 2000 van direktorijuma „system repair" [98]. Ukoliko se ova programska ranjivost prepozna na vreme i program zakrpi, to će zaštititi sistem od potencijalnog kompromitovanja izazvanog propustom u pomenutom programu.

   Rešenje : *Vršiti analize ranjivosti sa ciljem prepoznavanja instaliranih programa na sistemu da bi se ustanovilo, da li za instalirane programa postoji exploit koji može da dovede do kompromitovanja sistema. Ukoliko se pronađe takav program primenom adekvatne zakrpe, sistem će se zaštititi od pomenute potencijalne ranjivosti.*

3. Ranjivost ISAPI (eng. Internet Server Application Programming Interface) extension prepunjavanje bafera (eng.buffer overflows) [492] - neke od ISAPI aplikacija realizovane preko ISAPI ekstenzija su [493] :
   -ASP (eng. Active Server Pages)[494], standardno je instaliran na IIS.
   -ASP.NET[495], standardno je instaliran od verzije IIS 6.0 pa nadalje.
   -ColdFusion[496], poslednja verzija može se instalirati na IIS.
   -Perl ISAPI (Perliis)[497], besplatan je za instalaciju.
   -PHP[498], besplatan je za instalaciju.
   Primer za prepunjavanje bafera bi se mogao opisati na sledeći način : program očekuje da unesete maksimalno 90 karaktera i ukoliko on za input dobije 5000 karaktera, postavlja se pitanje kako će program, odnosno kôd, da reaguje na to. Iskorišćavanjem ISAPI ranjivosti moguće je dobiti punu putanju do Web root direktorijuma kao što je to slučaj kod ranjivosti „Microsoft IIS HTR ISAPI Extension Buffer Overflow"[499].

   Rešenje : *Vršiti analize ranjivosti sa ciljem prepoznavanja ranjivosti na IIS servisu koji mogu dovesti do kompromitovanja sistema. Ukoliko se ona pronađe primenom adekvatne zakrpe za sistem ili bezbednosnog update-a, sistem će se zaštititi od pomenute ranjivosti.*
4. Ranjivost RDS-a (eng. Remote Data Service, komponente MDAC-a (eng. Microsoft Data Access) [500501] - predstavlja bezbednosni propust u okviru Microsoft IIS-a (eng. Internet information server). Ukoliko se bezbednosni propust ne prepozna na vreme i ne zakrpi, može doći do kompromitovanja Web servera kao što su to učinili crvi tipa Nimda i Code red[502]. Zlonamerni napadač može pokrenuti komande na udaljenom

[491] http://www.sans.org/security-resources/idfaq/iis_unicode.php
[492] http://www.iss.net/security_center/reference/vuln/HTTP_IIS_Index_Server_Overflow.htm
[493] http://en.wikipedia.org/wiki/Internet_Server_Application_Programming_Interface
[494] http://en.wikipedia.org/wiki/Active_Server_Pages, 31.03.2012
[495] http://en.wikipedia.org/wiki/ASP.NET, 31.03.2012
[496] http://en.wikipedia.org/wiki/Adobe_ColdFusion, 31.03.2012
[497] http://en.wikipedia.org/wiki/Perl, 31.03.2012
[498] http://en.wikipedia.org/wiki/PHP, 31.03.2012
[499] https://www.rapid7.com/db/vulnerabilities/http-iis-0013
[500] Dostupno na http://www.giac.org/paper/gsec/19/vulnerability-microsoft-data-access-components-mdac-internet-information-server-iis/101517, 31.12.2012
[501] http://en.wikipedia.org/wiki/Microsoft_Data_Access_Components, 31.03.2012
[502] http://en.wikipedia.org/wiki/Nimda, 24.04.2012

sistemu bez direktnog pristupa. Zloupotrebu ove ranjivosti prema Microsoft-u moguće je prepoznati iz IIS "POST" logova na osnovu postojanja "/msadc/msadcs.dll" stavki.

Rešenje: *Da bi se izvršila adekvatna zaštita ispratiti uputstva date od strane Microsoft-a*[503] *ili preporuke iz SANS dokumenata* [182][190].

5. Nezaštićeni deljeni mrežni resursi realizovane preko NETBIOS-a – Deljenje resursa na NT sistemima je ranjivost baš kao i na Linux sistemima. Komunikacija sa deljenim resursima se obavlja preko portova 135-139. Na Windows 2000 port za komunikaciju je 445. Preko ovih portova dobijaju se informacije o broju korisnika, otvorenim deljenim resursima i sistemske informacije. Putem ovih portova zlonamerni napadač može zloupotrebljavati „NET" komande kako bi došao do informacija koje mogu poslužiti za dalju zloupotrebu. U praksi je čest slučaj da se deljeni resursi zloupotrebljavaju u svrhu prostora za skladištenje nedozvoljenog sadržaja.

   Rešenje : *Svi neopotrebni portovi bi trebalo biti onemogućeni na fajlervolu od spolja, a administrator bi posebno morao da proveri da li su portovi 135-139 i 445 zatvoreni.*

6. Null session ranjivost - Curenje informacija (eng. leakage) preko konekcije null sesije (eng. null session). Konekcija null sesije je poznata kao anonimno logovanje (eng. anonymous logon) i predstavlja mehanizam koji omogućava korisniku da anonimno preuzima informacije sa mreže ili da se anonimno autentifikuje na sistem[504]. Null sesije iskorišćavaju greške u CIFS (eng. Common Internet file system)/SMB (eng. Server Messaging Block). Nul sesija zahteva pristup preko porta TCP 139 ili TCP 445.Pogođeni sistemi su Microsoft Windows NT, 2000 and XP.
   Postavlja se pitanje na koji način otkriti ovu slabost ? Najbolji način je testirati sistem konektovanjem preko Null sesije sa sledećim komandama (u zavisnosti od tip NT sistema):
   NET USE \\ime ili adresa računara\IPC$ * /USER:
   NET USE \\ime ili adresa računara\IPC$ * /USER:""
   NET USE \\ime ili adresa računara\IPC$ "" /USER:""
   Ili iz Linuxa : # smbclient \\\\target\\ipc\$ "" –U ""

Navedena sintaksa podrazumeva kontekovanje na skriveni Inter-procesni komunikacioni share (IPC$) ciljanog računara preko anonimnog korisničkog naloga (/u:"") koji je ugrađen u sistem sa blanko šifrom (""). Ukoliko je odgovor "connection failed" sistem nije ugrožen na ovaj tip slabosti. Ukoliko odgovora nema ili je odgovor "command was successfull", sistem je ranjiv. Ukoliko je sistem ranjiv napadač može pristupiti skirvenim deljenim resursima (eng. shares). Takođe, napadač može saznati postojeće korisničke naloge i grupe, njihov status, imena računara, registarska podešavanja, postojeće deljene resurse i računarske i korisničke bezbednosne identifikatore (eng. Security Identifiers, SID) i druge informacije koje mogu pomoći da se organizuje zlonamerana aktivnost. U praksi napadači koriste i dodatne alate kao što su Wininfo i NAT (netbios auditing tool) kako bi saznali korisnička imena na ciljanom serveru i izvršili dictinary napad, a neretko se za napad na Windows NT se koristio i sid2user alat[505].

[503] http://technet.microsoft.com/en-us/security/bulletin/ms01-044, 24.04.2012

[504] Pod Windowsom 2000 mnoštvo lokalnih servisa radi pod nalogom LocalSystem koji se koristi za razne kritične sistemske operacije. Kada jedan računar treba da preuzme podatke iz drugog računara (na primer pristup deljenim resursima i ostali network neighborhood funkcionalnosti) nalog LocalSystem će otvoriti nul sesije za drugi računar. Specifičnost je ta da taj nalog LocalSystem ima gotovo neograničene privilegije i nema šifre (što znači da se na sistem i ne može logovati preko LocalSystem naloga). Opasnost je ta što zlonamerni korisnici mogu da iskoriste neki exploit i da se prijave na nul sesiju da bi dobili pristup ciljanom računarskom sistemu.

[505] http://evgenii.rudnyi.ru/programming.html#sid2user

Rešenje: *Onemogućiti logovanje anonimnih korisnika. Na ovaj način će se zabraniti pristup informacijama anonimnim korisnicima kojima eksplicitno nije dozvoljen pristup uključujući grupu Everyone i korisnike nulte sesije. Treba skrenuti pažnju da ova restrikcija može imati implikacija na sinhronizovanje sa domenom ili drugim servisima, pa je pre upotrebe treba testirati za postojeće okruženje.*

Postupak za Microsoft Windows NT

a. Izmena registarstkog ključa :
„HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\“
sa sledećim podešavanjima:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1
Posle ovih podešavanja neophodan je restart računarskog sistema.
Postupak za Microsoft Windows *2000 :*

b. Izmena registarskog ključa :
„HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\“
sa sledećim podešavanjima :
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 2

c. Dodatno otvoriti „Local Security Settings“ postaviti sledeće podešavanje :
Local Security Settings - Local Policies- Security Options-Additional restrictions of anonymous connections:No access without explicit anonymous permissions.

Posle ovih podešavanja neophodan je restart računarskog sistema.

Postupak za Microsoft Windows XP :

a. Izmena registarstkog ključa :
„*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa*\“
sa sledećim podešavanjima:
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1
Value Name: RestrictAnonymousSAM
Data Type: REG_DWORD
Data Value: 1
Value Name: EveryoneIncludesAnonymous
Data Type: REG_DWORD
Data Value: 0

b. Izmena registarskog ključa :
„*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters*\“
sa sledećim podešavanjima:
Value Name: RestrictNullSessAccess
Data Type: REG_DWORD
Data Value: 1
Value Name: NullSessionPipes
Data Type: REG_MULTI_SZ
Data Value: "" (prazan string bez navodnika)

c. Dodatno otvoriti „Local Security Settings“ postaviti sledeće podešavanje :

Security Settings - Local Policies - Security Options - Network access: Allow anonymous SID/Name translation: Disabled

Posle ovih podešavanja neophodan je restart računarskog sistema. Treba napomenuti da onemogućavanje „NULL sessions“ može imati uticaj na funkcionalnost kao i na neke mrežne programe[506].

Postupak za Microsoft Windows 2003:

a. Izmena registarskog ključa :
„HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\“
sa sledećim podešavanjima :
Value Name: RestrictAnonymous
Data Type: REG_DWORD
Data Value: 1
Value Name: RestrictAnonymousSAM
Data Type: REG_DWORD
Data Value: 1
Value Name: EveryoneIncludesAnonymous
Data Type: REG_DWORD
Data Value: 0
Value Name: TurnOffAnonymousBlock
Data Type: REG_DWORD
Data Value: 0

b. Izmena registarskog ključa :
„*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\“*
sa sledećim podešavanjima :
Value Name: RestrictNullSessAccess
Data Type: REG_DWORD
Data Value: 1
Value Name: NullSessionPipes
Data Type: REG_MULTI_SZ
Data Value: "" (prazan string bez navodnika)

c. Dodatno otvoriti „Local Security Settings“ i postaviti sledeće podešavanje :
Security Settings - Local Policies - Security Options - Network access: Allow anonymous SID/Name translation: Disabled

Posle ovih podešavanja neophodan je restart računarskog sistema. Treba napomenuti da, onemogućavanje „NULL sessions“ može imati uticaj na funkcionalnost kao i na neke mrežne programe[507].

Postupak za SAMBU na Linuxu:

Da bi se onemogućilo anonimno logovanje na SAMBU neophodno je modifikovati konfiguracioni fajl SAMBA servera „smb.conf“ sa sledećim podešavanjima :

```
guest account = nobody
restrict anonymous = 1
```

Obavezno proveriti, da li postoji korisnik sa imenom „nobody“.

[506] Efekti onemogućavanja NULL sesije objašnjeni u Microsoft članku „The effects of removing null sessions from the Microsoft Windows 2000 and Microsoft Windows NT environment“ koji je dostupan na http://support.microsoft.com/kb/890161

[507] Uticaji onemogućavanja NULL sesije objašnjeni su i u Microsoft članku „Client, service, and program issues can occur if you change security settings and user rights assignments“ dostupno na http://support.microsoft.com/kb/823659

7. Slabost heširanja u SAM (eng. Security accounts manager) bazi putem LAN menadžer heša (eng. Lan manager hash - LM hash) - Windows generiše i skladišti šifre korisničkih naloga na dva različita načina poznatog kao heširanje. Ukoliko se postavlja šifra čija je dužina ispod 15 karaktera, Windows generiše dve heš vrednosti LM heš i Windows NT heš šifre. Ove heš vrednosti se smeštuju u SAM bazu lokalno ili u Aktvini direktorijum. LM heš je slabija u poređenju sa NT heš i zato je sklonija bržem brute-force napadu[508]. Zato je preporuka da se onemogući u Windowsu čuvanje LM heš vrednosti od šifri .

   Rešenje : *Detaljno uputstvo koje se odnosi na sprečavanje Windows operativnog sistema da skladišti LM heširane šifre u Aktivni direktorijum i lokalnu SAM bazu prikazano je u Microsoft članku „How to prevent Windows from storing a LAN manager hash of your password in Active Directory and local SAM databases“[509]. Verzije Windowsa na koji se članak odnosi su : Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows Server 2003.*

8. Remote Administration Services - Ova ranjivost potiče od načina upravljanja udaljenih sistema od strane administratora sistema. Ovi sistemi upravljanja na daljinu, iako su relativno sigurni imaju svoje ranjivosti. U praksi najčešće upotrebljavani sistemi za udaljeno administriranje sistema su Symantec PcAnywhere[510], Radmin[511], DameWare Remote Support[512], TeamViewer[513], RealVNC[514]. Kompromitovanje ovih servisa prema forenzičkoj praksi najčešće je posledica kompromitovanja nedovoljnih ili loše konfigurisanih bezbednosnih kontrola uz upotrebu određenih exploita kako bi zlonamerni napadači dobili administratorske privilegije.

   Rešenje: *Upotrebljavati samo bezbedne sisteme za udaljeno administriranje. Takvi sistemi moraju da omoguće zaštićenu komunikaciju (šifrovanu), sa podrškom za jaku autentifikaciju, mogućnost zaključavnja naloga nakon određenog broja neuspelog logovanja uz podršku za logovanje neautorizovanih pokušaja. Dodatno, potrebno je podesiti, da se od korisnika računarskog sistema očekuje potvrda, da prihvata udaljeno administriranje kao i ograničavanje programa na samu IP adresu administratorske radne stanice.*

4.1.3 Ranjivosti na Linux sistemima

1. Prepunjavanje bafera RPC (eng. Remote procedure call, RPC buffer overflows) servisa - Ovi RPC servisi omogućavaju programima sa jednog računara da izvršavaju programe na nekom drugom računaru. Koriste se za pristup mrežnim servisima kao na primer NFS. Greške i ranjivosti u RPC-u mogu biti aktivno eksploatisane. Postoje i dokazi da je prilikom izvršavanja DDOS napada tokom 1999. i početkom 2000. godine izvršeno upravo preko računara sa kompromitovanih RPC servisa [189].

   Rešenje : *Ograničiti upotrebu RPC servisa samo na računare koji nemaju pristup Internetu. Ukoliko su neophodni, na fajervolu blokirati pristup RPC servisima, tako da zlonamerni napadači ne mogu pristupati tom servisu. Zaštitu od napada na RPC servis, iz unutrašnje mreže, moguće je ostvariti kroz onemogućavanje ovog servisa na sistemima gde on nije potreban. Na sistemima kojima je neophodan RPC*

[508] Kako sprečiti Windows mermorisanje LM heš vrednosti šifri na računarskim sistemima. izvor : http://support.microsoft.com/kb/299656, 31.03.2012
[509] http://support.microsoft.com/kb/299656
[510] http://www.symantec.com/pcanywhere
[511] http://www.radmin.com/
[512] http://www.dameware.com/
[513] http://www.teamviewer.com/sr/
[514] http://www.realvnc.com/

servis obavezno je vršiti redovno ažuriranje i krpljenje servisa. Analizom ranjivosti na redovnoj osnovi moguće je otkriti ranjivu verziju RPC servisa.

2. Sendmail ranjivosti - Sendmail je program koji procesira, odnosno prima, šalje i prosleđuje elektronsku poštu na Linux operativnim sistemima. S obzirom na njegovu široku rasprostranjenost vrlo često je na meti napadača. Tokom godina pronađene su neke slabosti vezane za Sendmail koje mogu napadaču da omoguće pokretanje komadni bez direktnog logovanja na kompromitovani računar i da omoguće napadaču punu kontrolu. U praksi su prepoznata tri najčešća exploita : exploit sa kojim se šalje spam, exploit koji šalje fajl sa šiframa i exploit koji izvršava DOS napad. Primer explota : napadač šalje osmišljenu e-mail poruku sa zlonamernim kodom na server na kome se nalazi Sendmail, Sendmail procesira tu poruku kao instrukciju u kojoj se zahteva slanje fajla sa šiframa. Sendmail šalje fajl sa šiframa napadaču na njegov računar gde će moći da razbijanje šifre.

   Rešenje: *Osavremenjivanje Sendmail-a poslednjom verzijom ili primena zakrpa (eng. patches) za postojeći Sendmail servis. Dodatno, ne pokretati Sendmail servis u demon modu (eng. daemon mode) (isključivanjem -bd sviča) na računarima koji nisu podešeni kao mail serveri niti kao serveri, za slanje pošte. (eng. mail relay server)*[515].

3. Slabosti BIND (The Berkeley Internet Name domain) programa - Bind je najrasprostranjeniji način implementacije DNS-a (eng. Domain name service) na osnovu koga se lociraju svi sistemi na Internetu prema njihovim imenima, kao na primer www.mi.sanu.ac.rs, bez potrebe da se znaju određene IP adrese. Ovaj sistem koristi DNS da bi izvršio prevođenje imena računara u IP adrese i obrnuto. S obzirom da su DNS servisi od krucijalnog značaja za normalno funkcionisanje Interneta, njegova dostupnost na Internetu ga čini omiljenom metom napadača. Prema SANS institutu u anketi koja je rađena 1999, godine čak 50% svih DNS servera koji su povezani na Internet su imali ranjive verzije BIND servisa. Tipičan primer BIND napada bi se mogao opisati na sledeći način : zlonamerni napadač briše sve logove na sistemu, instalira alate koje će mu omogućiti administratorska prava. Zatim kompajlira i instalira IRC alate i alate za skeniranje mreže u potrazi za dodatnim sistemima koji imaju ranjive verzije BIND servisa. Za manje od minuta moguće je zloupotrebiti stotine udaljenih računarskih sistema što za posledicu nosi dalje kompromitovanje ostalih sistema. Ovaj primer ilustruje na koji način ranjivost DNS servera odnosno BIND-a koji je odgovoran za realizaciju DNS-a može da napravi potpuni haos. Takođe, korišćenje zastarelih verzija BIND-a nosi sa sobim i rizik zloupotrebe putem buffer overflow eksploita čime napadač može dobiti neovlašćeni pristup računarskom sistemu, a prema SANSU česti su i DOS napadi na ovaj servis.

   Rešenje: *Osavremenjivanje Binda-a poslednjom verzijom ili primena zakrpa (eng. patches) za postojeći BIND servis. Preporuka je da se BIND servis pokreće u ime neprivilegovanog korisnika iz bezbednosnih razloga u slučaju nekog budućeg udaljenog napada. Takođe, preporuka je da se BIND realizuje u izolovanom (chroot) direktorijumskom okruženju*[516] *zbog zaštite takođe od budućih udaljenih napada. To znači da ukoliko neko uspe da izvrši udaljeni napad na BIND servis, najviše što će moći je manipulisanje sa fajlovima u direktorijumu u kome je BIND zaključan.*

[515] http://www.deer-run.com/~hal/sysadmin/sendmail.html

[516] Podešavanje Chroot okruženje podrazumeva da se za određeni program kao na primer za BIND neki folder proglasi za koren fajl sistema na primer "/isolation" umesto "/"). To zapravo znači da program koji radi u chroot okruženju ne vidi realan fajl sistem tj. "/", već samo taj izolovan folder "/isolation" i samim tim ne može da se nanese šteta operativnom sistemu u slučaju kompromitovanja izolovanog servisa. To na primer znači da program koji radi u izolovanom chroot-ovanom okruženju, ukoliko želi da pristupi folderu /var/named, on će zapravo pristupiti folderu /isolation/var/named.

4. Slabosti DNS servisa : kao što BIND servis ima svoje ranjivosti tako i DNS servis na osnovu svoje izloženosti može uticaj na bezbednost sistema. Kao što je već pomenuto sistemi koriste DNS za prevođenje imena računara u IP adrese i obrnuto. U praksi je slučaj da su serveri konfigurisani na takav način da šalju veliki broj informacija o svojoj mreži. Na primer, DNS može biti tako konfigurisan da putem transfera zone sistem napadač dobije informacije i o kompletnom domenu. Dodatno DNS rekordi mogu sadržati informacije kao što su adrese internih servera, tekstualni opisi servera, imena sekundarnih sistema kao i uloge određenih servera što može pomoći napadaču da organizuje napad.

   Rešenje : *Analizom ranjivosti potrebno je, utvrditi koje informacije se šalju od strane DNS servera da bi se onemogućilo slanje suvišnih informacija koje za posledicu imaju povećanje rizika od napada. Takođe, neophodno je konfigurisanje DNS servera tako da se ograniči transfer zone samo za određene IP adrese koje zahtevaju ažuriranje zonskih informacija.*

5. Upotreba "trust" komandi (eng. r commands ili relationship trust commands) - Ukoliko je korisnik ulogovan na server koji sa drugim serverima ima uspostavljen "trust" odnos, korisnik može da se slobodno prijavljuje na te servere bez re-autentifikacije uz pomoć komandi rlogin (remote login), rsh (remote shell), rcp (remote copy)[517]. Ove komande ne zahtevaju potvrdu identiteta što znači da korisnik ne mora ponovo da kuca šifru. Sa stanovišta praktičnosti "trust " odnos je odlična ideja, ali sa stanovišta bezbednosti predstavlja veliku potencijalnu opasnost. Ukoliko zlonamerni napadač; dobije kontrolu na bilo kom računarskom sistemu koji je u "trust" odnosu, on može da dobije pristup svim drugim računarskim sistemima koji imaju "trust" odnos sa kompromitovanim sistemom.

   Rešenje : *Proveriti da li postoje fajlovi .rhosts i i /etc/hosts.equiv . Ukoliko postoje onemogućiti upotrebu "trust" komandi editovanjem fajla /etc/inetd.conf .*

6. LPD (eng. remote print protocol daemon) - Ovaj servis (in.lpd) se upotrebljava za interakciju Linux korisnika sa lokalnim printerom preko porta TCP 515. Međutim, u praksi se pokazalo (Solaris 2.6-8 Linux je primer) da ima buffer overflow ranjivost što za posledicu može da donese zlonamernom napadaču root privilegije na računarskom sistemu , u slučaju kompromitacije ovog servisa.

   Rešenje : *Sistem je ranjiv ukoliko nije odrađeno patch-ovanje ranjive verzije lpd. Zaštita se izvodi instaliranjem poslednje verzije ovog servisa ili patchovanjem lpd ranjive verzije. Ukoliko ovaj servis nije neophodan ukloniti ga sa sistema onemogućavanjem print servisa u /etc/inetd.conf i blokiranjem porta 515.*

7. Sadmind i Mountd - Sadmind je Solarisov program koji omogućava udaljeni pristup računarskom sistemu i služi za administriranje računarskog sistema (ima i svoj grafički interfejs). Izvršava sa na serveru uz pomoć klijentskog programa koga kontroliše sam korisnik. Mountd kontroliše pristup deljenim datotekama na mreži preko NFS na Linux sistemima. I ovi programi su ranjivi pa bi zlonamerni napadač preko exploita mogao da izazove buffer overflow i na taj način da dobije root privilegije. Ovo je bio jedan od glavnih načina na koji su organizovani DDOS napadi na CNN Yahoo i druge sajtove [119].

   Rešenje : *Instaliranje poslednjih zakrpa za sadmind i mountd.*

8. Upotreba difoltnih SNMP stringova - SNMP (eng. The simple network management protocol) je protokol koji se najčešće koristi kao način praćenja i upravljanja uređaja

[517] Umesto zahteva za korisničkim imenom i šifrom udaljenom računaru je dovoljno samo definisana "trust" IP adresa.

na mreži kao na primer rutera, svičeva, štampača, računara i ostalih mrežnih uređaja. Svrha upotrebe ovog protokola je dobijanje statusa, performansi i dostupnosti uređaja koji se prati. Koristi nešifrovan "community string" kao jedini autentifikacioni mehanizam što je ujedno i velika slabost ovog protokola. Difoltna vrednost community stringa zavisi od proizvođača same mrežne opreme i uglavnom je postavljena na "public" (sa pravima čitanja) ili "private" (sa pravima čitanja i upisa). Ukoliko napadač dobije pravo upisa na uređaju moguće su zloupotrebe u vidu rekonfiguracije samog uređaja, isključivanja uređaja ili instaliranja neautorizovanih servisa koji omogućuju "zadnja vrata" (eng. Back door). Prisluškivanjem SNMP saobraćaja potencijalni napadač može otkriti mnogo, kako o strukturi same mreže, tako i o računarskom sistemu i njegovim pridruženim uređajima kako bi što bolje planirao napad i fingirala meta. Iako SNMP nije karakterističan samo za Linux već se koristi i na Windows računarskim sistemima, u praksi se pokazalo da je najviše napada bila upravo na Linux računarskim sistemima zbog loše SNMP konfiguracije.

Rešenje : *Prilikom konfigurisanja, izabrati jake šifre (community strings) sa većim brojem karaktera*[518] *i postaviti SNMP bazu podataka (eng. management information base - MIB)*[519] *na read only. Dodatno, SNMP pristup treba blokrati na fajervolu i vršiti njegovu kontrolu kroz pristupne liste (eng. Access control list) na internim i eksternim ruterima.*

9. Globalno deljenje fajlova (eng. global file sharing) - Globalno deljenje faljova na mreži podrazumeva deljenje datoteka između računara koji koriste Network Neighborhood (kod Microsoft Windows računara) ili NFS (kod Linux računara). Pristup prema podrazumevanoj postavci je i čitanje i pisanje (eng. read-write). To znači da svako na istoj mreži može pristupiti svim fajlovima. Na početku mreže su bile relativno male, ali sada kada postoji globalna mreža tj. Internet, to nosi rizik da bilo ko može pristupiti fajlovima koji se dele na mreži. U stvari najveća opasnost je za kućne korisnike koji imaju direktan pristup Internetu preko modema (adsl modemi, kablovski modemi, telefonski modemi). Zlonamerni napadači mogu dobiti pristup ličnim podacima korisnika, kao što su na primer, brojevi kreditnih kartica, tekućih računa, šifre od e-mail naloga.

   Rešenje : *Potrebno je pažljivo odrediti podatke za deljenje na mreži i osigurati da se podaci dele samo sa onima kojima su namenjeni.*

10. Ranjivosti IMAP i POP - Internet message access protocol (eng. IMAP)[520] i Post Office Protocol (eng. POP) [521] su najčešće korišćeni e-mail protokoli koji korisnicima omogućavaju naprednije mogućnosti prilikom pristupanja svojim e-mail nalozima sa udaljenih lokacija. IMAP i POP servisi takođe imaju svoje slabosti. Zaštitni zidovi (eng. firewalls) obično su konfigurisani da propuštaju ove servise. Opasnost se krije u tome što zlonamerni napadači mogu da dobiju pristup internoj mreži i da kompromituju IMAP i POP mail server. Ukoliko je napad bio uspešan moguće je da preuzmu kontrolu nad sistemom.

    Rešenje : *Analizom ranjivosti moguće je detoktovati prisutnost ranjivih IMAP i POP servera. Ove servise postavljati samo na sistemima namenjenim za poštu*

[518] Korišćenje jakih šifara podrazumeva upotrebu alfa-numeričkih karaktera dužine najmanje 10 karaktera uključujući velika i mala slova (eng. case sensitive).

[519] MIB opisuje strukturu upravljanja podacima za određeni SNMP uređaj, dospupno na http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol, 04.04.2012

[520] Ovaj protokol predstavlja protokol kojim se omogućava pristup e-mail porukama na udaljenom serveru putem korisničkog lokalnog klijenta http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol, 26.04.2012

[521] Ovaj protokol predstavlja protokol za prenos elektronske pošte preko IP mreža (primanje e-mail poruka sa udaljenog servera na lokalni e-mail klijent korisnika), razvijan je kroz nekoliko verzija i trenutna verzija je POP3.
Dosupno na http://sh.wikipedia.org/wiki/Post_Office_Protocol

odnosno mail serverima, ukoliko za njih ne postoji potreba ukloniti ih sa sistema. Redovno instalirati zakrpe koje se pojavljuju za pomenute servise, odnosno i osvežavati ih najnovijim verzijama.

11. Ranjivosti na NFS-u (Network File system) – NFS se koristi za deljenje fajlova i drajvova na Linux fajl sistemima. Eksportovani NFS sistemi koji su dostupni od spolja (putem Interneta), su potencijalna meta za zlonamerne napadače. Kompromitovanje NFS deljenih resursa od strane napadača može biti prouzrokovano lošim konfigurisanjem NFS dozvola. Posledica može biti takva da napadač može pristupiti osetljivim informacijma ili dobiti dozvole upisa na NFS sistem. Na primer, napadač može da unese ili izmeni .rhosts fajl u kome dodeljuje za svoju IP adresu pristup sistemu putem rlogin-a. Postojanje ranjivosti NFS servisa, zavisi od verzije nfsd-a, a one kritične omogućuje zlonamernom napadaču pristup fajl sistemu sa root privilegijama.

    Rešenje : *Ukoliko je NFS neophodan treba proveriti da li je ispravno konfigurisan. Portovi koji se koriste za NFS (port 2049) treba biti blokiran na fajervolu i filtriran na ruteru. Takođe, dozvole za kontrolu pristupa moraju biti podešene na odgovarajući način (izbegavati korišćenje „**no_root_squash**“ opcije). Vršiti periodičnu analizu ranjivosti, pratiti publikovane NFS ranjivosti i instalirati najnovije sigurnosne zakrpe za NFS servise.*

Na kraju ovog dela treba spomenuti da postoji nekoliko besplatnih servisa koji publikuju nove ranjivosti koje se pojave. Sajtovi kao što su Security Focus[522], The Computer Security Division of the National Institute for Standards and Technologies (NIST) ICAT[523], sadrže pretražive baze ranjivosti. Pretražive baze omogućuju administratorima da pretražuju nove ranjivosti koje se odnose na proizvode koji se koriste na sistemima. Mnoge od ovih pretraživanja omogućuju predefinisano pretraživanje prema određenim kriterijumima na primer prema operativnom sistemu, programu, značajnosti, datumu i drugim kriterijumima.

4.2 NAJČEŠĆI NAČINI ZLONAMERNOG ISKORIŠĆAVANJA SISTEMA

U prethodnoj klasifikaciji prikazane su prepoznate ranjivosti koje su prisutne na sistemima i načini njihove prevencije.

U daljem tekstu biće navedeni najčešći načini zlonamernog iskorišćavanja ranjivosti na sistemima : upad na sistem sa ciljem dobijanja pristupa, dobijanje privilegija, i onemogućavanje servisa.

4.2.1 Upad na sistem sa ciljem dobijanja pristupa

Upad na sistem podrazumeva dobijanje pristupa kroz iskorišćavanja ranjivosti sistema kao i dobijanje privilegija na sistemu. Zlonamerno dobijanje pristupa na sistemu najčešće se ostvaruje na sledeće načine :

a. **Napad na operativni sistem** - Kada je reč o napadu na operativni sistem, glavne slabosti koje su predmet iskorišćavanja su servisi i otvoreni portovi. Što je više servisa i otvorenih

[522] http://www.securityfocus.com/
[523] http://nvd.nist.gov/

portova to je više pristupnih tačaka na sistemu. Na osnovu ovakvog gledišta, difoltna instalacija operativnog sistema treba biti sa što manjim brojem pokrenutih servisa (samo neophodnim) i otvorenih portova (ukoliko je potreban veći broj mogu se naknadno instalirati servisi). Nažalost u realnosti to nije slučaj. Difoltna instalacija sadrži veliki broj startovanih servisa i otvorenih portova. U poglavlju 4.3 u praktičnom primeru biće prikazane brojne ranjivosti u Windows i Linux operativnim sistemima nakon jedne takve difotlne instalacije (zbog obimnosti, tabelarni prikaz svih skeniranih sistema biće izdvojeni na kompakt disku, kao poseban prilog ovog rada). Razlog za instaliranje velikog broja servisa pri difoltnoj instalaciji operativnog sistema koja sa sobom nosi ogroman bezbednosni rizik, jeste materijalan. Cilj proizvođača jeste da korisnik operativnog sistema može da instalira i konfiguriše sistem sa najmanje napora (ukoliko postoji problem zove se tehnička podrška proizvođača, a nije skupa). To znači da, sa jedne strane imamo smanjenje troškova za proizvođača, a sa druge strane imamo veću funkcionalnost na sistemu i veće zadovoljstvo korisnika prilikom instalacije sistema (instalirano je i šta je potrebno i šta nije). Sa gledišta proizvođača to je prihvatljivo, ali sa stanovišta bezbednosti nije. Dodatan problem leži u činjenici da korisnici računarskih sistema nisu dovoljno svesni ranjivosti sistema koje koriste. Isto tako, u organizacijama smatraju da je instaliranjem operativnog sistema na računaru posao završen i ne primenjuju krpljenje i ažuriranje sistema (eng. update) koje se preporučuje na dnevnom nivou [177]. Rezultat jeste organizacija sa zastarelim operativnim sistemom koji ima veliki broj ranjivosti odnosno veliki bezbednosni rizik.

b. **Napad na programe instalirane na sistemu** - Kada je reč o napadima na programe instaliranih na sistemu, uzroke treba tražiti u njihovom razvoju, jer bezbednost nije implementirana u dizajn samog programa. U praksi programeri koji razvijaju programe susreću se sa postavljenim vrlo kratkim rokovima za realizaciju programa. To znači da se testiranje ne izvršava detaljno. Takođe, dodatni problemi što se tiče bezbednosti nastaju prilikom povećavanja funkcionalnosti i kompleksnosti programa pa su šanse za testiranje svih funkcija još manje. Zloupotreba funkcionalnosti otvara vrata za kompromitovanje bezbednosti na sistemu. Na primer, jedan e-mail klijent može da sadrži funkciju koja omogućuje direktno isčitavanje HTML poruke za korisnika. Napadač ovo može da iskoristi tako što osmisli lažnu poruku koja u HTML izgleda regularno, ali koja sadrži hyperlink koji vodi do zlonamerne WEB stranice kada korisnik klikne na nju [168]. Drugi problem koji se odnosi na programe, jeste ispitivanje na greške (eng. error-checking). Jedan od razloga za veliki broj bezbednosnih propusta u programima je upravo nedostatak ispitivanja grešaka. Buffer overflow je jedan od primera ovog problema i tu ranjivost može zloupotrebiti napadač da dobije pristup sistemu, privilegije, a može i da onemogući servise na sistemu. Prekoračenje bafera može izazvati krah ili nepravilno izvršenje programa; najčešća posledica je ranjivost kôda koju napadači mogu iskoristiti [148]. Napad tipa buffer overflow nastaje kada napadač pokušava da uskladišti veći broj podataka u bafer memorije u odnosu na onu koji je programer predvideo prouzrokujući prelivanje podataka sa malicioznim kodom u druge bafere. Primer za prepunjavanje bafera mogao bi se ilustrovati na sledeći način : program očekuje niz od 80 znakova, a korisnik unese 300. Kada se izvrši ovaj kod, napadač može da dobije potpunu kontrolu nad sistemom. Jako dobar rad autora Aleph One-a, koji opisuje ranjivost tipa buffer overflow jeste „*Smashing the Stack for Fun and Profit*“[524] objavljen u online časopisu Phrack[525] koji se bavi problemima sa bezbednošću na računarskim sistemima [147]. Postoje dva dipa prepunjavanja bafera “stack” i “heap”. Stack i heap predstavljaju dve oblasti u memorijskoj strukturi koje se dodeljuju prilikom pokretanja programa [174]. Pozivi funkcija se čuvaju u stack oblasti, a dinamičke promenljive se čuvaju u heap

[524] Dostupno na http://www-inst.eecs.berkeley.edu/~cs161/fa08/papers/stack_smashing.pdf
[525] Dosutpno na http://www.phrack.com/

oblasti. Zlonamerni napadači mogu da koriste buffer overflow heap sa ciljem da izmene šifru, ime fajla ili drugih podataka. Ukoliko se ime fajla izmeni drugi fajl će biti otvoren. To znači da ukoliko je to neka izvšna datoteka buće izvršen kod koji nije trebao da se pokrene.

c. **Napad na skripte i primere programa** - Napadi na skripte i probne programe posebno se odnose na Linux sisteme. Razlog leži u činjenici da prilikom instaliranja operativnog sistema ili programa, proizvođač distribuira i probne fajlove tj. skripte i programe za bolje razumevanje sistema i za budući razvoj programa. Sa stanovišta programera koji razvija programe, ovakav pristup je dragocen, jer se vreme potrebno za razvoj drastično smanjuje, ali nosi rizik po pitanju bezbednosti. Naime, najveća prisutnost ovih probnih skripti je u oblasti WEB razvoja. Na primer, prethodne verzije Apache WEB servera su dolazile sa probnim skriptama od kojih su većina imale ranjivosti. Dodatan problem predstavlja i veliki broj predefinisanih skript alata koji dolaze u sklopu WEB pretraživača koji omogućuju ljudima, da sa malo programerskog znanja razvijaju programe za kratko vreme. Rezultat je takav da program jeste funkcionalan, ali ono što je u pozadini jeste veliki bezbednosni problem. Skripte mogu biti pune nepotrebnog koda, a testiranje na greške je izostalo (ili je zanemarljivo) što otvara vrata potencijalnom napadaču. Primera ima mnogo, a jedan koji može da ilustruje bezbenosni problem jeste difiltna instalacija WEB sajta koji dolazi sa IIS (eng Internet Information Services, nekadašnji Internet Information Server). Nakon instaliranja alati za udaljenu administraciju su dostupni na glavnoj strani. Ovi alati mogu biti zloupotrebljeni od strane napadača da kompromituju sistem. Koliko ranjivosti za sistem nose difoltne instalacije WEB-a (Apache), MySql-a, PHP na LINUX platformi, biće prikazane u praktičnom delu rada u kome se opisuju ranjivosti na Windows i Linux platformama.

d. **Napadi usled loše konfiguracije** (sistema, programa, servisa, fajervola) - Napadi zbog pogrešne konfiguracije nisu retka pojava. Primera u forenzičkoj praksi ima mnogo kao na primer, sistem administrator pokušavajući da podesi sistem uključuje gomilu opcija dok ne proradi ono što želi da iskonfiguriše. Međutim zbog uključivanja velikog boja opcija nikada neće razumeti šta one rade i samim tim neće biti uklonjen višak nepotrebnih opcija koje predstavljaju potencijalnu bezbednosnu pretnju. Tu leži problem! Da bi se mašina konfigurisala ispravno i da bi se smanjili potencijalni bezbednosni rizici, neophodno je ukloniti servise i programe sa sistema koji nisu potrebni. Ovo je oblast na koju se treba dodatno skoncentrisati, jer se može kontrolisati dobrom administracijom.

Treba napomenuti da upad na sistem radi dobijanja pristupa nije samo po sebi cilj (izuzetno retko), već je cilj da se obavi niz zlonamernih aktivnosti na serveru. Najčešće posle dobijenog pristupa napadač vrši upload (određenih malicioznih programa, fajlova, ilegalnih fajlova) ili download (osetljivih informacija) sa kompromitovanog sistema. U forenzičkoj praksi uglavnom se dešava da napadač učitava program na sistemu koji služi za dobijanje većih privilegija na sistemu, za onemogućavanje servisa, za kompromitovanje drugih računara u mreži ili van nje, kao i za podešavanje zadnjih vrata za ponovni pristup sistemu (gde je najjednostavniji način, dodavanje novog korisničkog naloga na sistem, preko kreiranja zadnjih vrata po određenom portu kao na primer „*Back Orifice*“, do sofisticiranih Trojanskih verzija logon deamon-a koji ima skrivene mogućnosti logovanja određenog korisnika na sistem sa root privilegijama).

4.2.2 Dobijanje privilegija na sistemu

Jedan od ciljeva napada na sistem jeste i dobijanje privilegija na njemu, bilo kao root (na Linux sistemima), bilo kao administrator (na Windows sistemima). Dobijanje privilegija najčešće se ostvaruje upotrebom lokalnog ili udaljenog exploita. Da bi napadač upotrebio lokalni exploit mora da ima pristup sistemu sa standarnim privilegijama i pomoću njega dobija admin tj. root privilegije. Udaljeni exploit je skoro isti kao i lokalni, samo što napadač ne mora da ima pristup računarskom sistemu, već može da ga pokrene sa bilo koje Internet lokacije. U izuzetno retkim slučajevima napadač može direktno da dobije najveće privilegije, ali u većini slučajeva napadač mora da ima ili da dobije pristup sistemu, pa tek onda može da povećava svoje privilegije na njemu. Na primer, u forenzičkoj praksi čest je sledeći scenario na Windows sistemu: napadač može da pristupi sistemu kroz nalog Gost (eng. Guest) sa ciljem prikupljanja dodatnih informacija i uz upotrebu određenih alata može pridobiti administratorski pristup na Windows sistemu. Preporuka je da se na sistemima zabrani upotreba gostujućih naloga i da se vrši revizija korisničkih naloga kako bi se detektovali sumnjivi nalozi (jer napadač može sa dobijenim privilegijama kreirati maliciozni nalog preko koga bi mogao da ima normalan pristup sistemu).

4.2.3 Napadi sa ciljem onemogućavanja servisa

Ovi napadi su detaljno opisani u početnim poglavljima ovog rada i njihov cilj je da na sistemu blokiraju servise ili raspoloživost resursa namenjenih korisnicima. Na primer, blokiranje korisnika da posete određeni sajt, zaključavanje korisničkih naloga. U praksi napadi ovog tipa se relativno lako obavljaju na Internetu, jer ne zahtevaju prethodni pristup sistemu.

4.3 ISPITIVANJE SERVISA WINDOWS I LINUX PLATFORMI NA RANJIVOSTI – PRAKTIČNI PRIMER

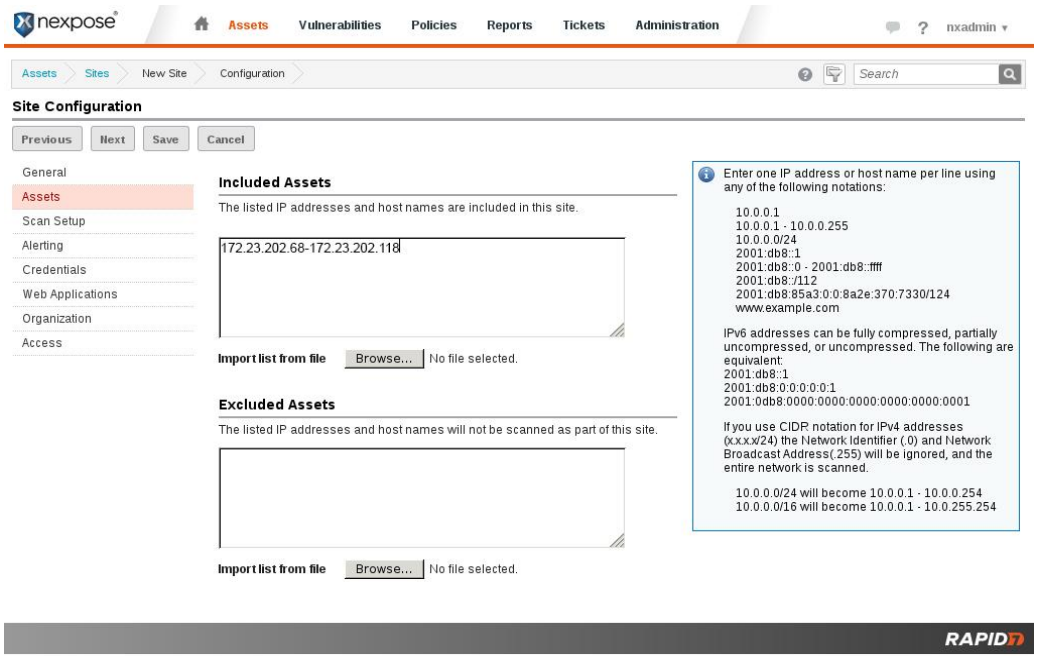
U prethodnom poglavlju opisan je veliki broj najčešćih ranjivosti koje su pristutne na računarskim sisemima. U sistemu zaštite, ranjivosti mogu biti u softveru, hardveru, konfiguraciji i ljudima [76]. U ovom radu težište je na otkrivanju ranjivosti softvera – Operativnog sistema, odnosno njegovih servisa. Upotrebom alata za analizu ranjivih servisa na sistemu moguće je dobiti dragocene informacije o sistemu i mreži sa stanovišta zaštite. Kao što će biti prikazano, prikupljene informacije obuhvataće veliki broj podataka o prisustvu različitih mrežnih servisa na sistemu koji predstavljaju potencijalne bezbednosne propuste. Ovi propusti mogu nastati zbog pogrešno konfigurisanih servisa, poznatih grešaka (eng. Well known bug) u sistemu ili programu, neažuriranosti sistema i njegovih servisa, kao i zbog upotrebe slabe zaštite u konfiguraciji. Cilj ovog ispitivanja jeste da se identifikuju i koriguju svi prepoznati bezbednosni propusti (ranjivi servisi) na difoltnim sitememima. Obuhvaćeni su svi relevantni izvori koji publikuju ranjivosti na sistemima i prikazani su u tabeli 13. :

Tabela 13. Izvori koji publikuju ranjivosti na operativnim sistemima

Naziv izvora u radu	Web adresa izvora
APPLE-SA (Apple Security Announce)	http://lists.apple.com/archives/security-announce
BID	http://www.securityfocus.com/bid/
CERT CA	http://www.us-cert.gov/ncas/alerts/
CERT TA	http://www.us-cert.gov/ncas/alerts/
CERT-VN	http://www.kb.cert.org/vuls/
CVE (Common Vulnerabilities and Exposures)	http://web.nvd.nist.gov/view/vuln/search i http://cve.mitre.org/
DEBIAN DSA (Debian Security Announce)	http://www.debian.org/security/
IAVM (Information Assurance Vulnerability Management)	http://iase.disa.mil/index2.html
MANDRAKE MDKSA (Mandrake Security Announce)	http://www.mandriva.com/en/support/security/advisories/
MS (Microsoft security)	http://technet.microsoft.com/en-us/security/dn481339
MSKB (Microsoft Knowledge Base)	http://support.microsoft.com/
NETBSD	ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/
OSVDB (Open Sourced Vulnerability Database)	http://www.osvdb.org/
OVAL (Open Vulnerability and Assessment Language)	http://oval.mitre.org/find/
REDHAT RHSA (Redhat Security Announce)	http://www.redhat.com/mailman/listinfo/rhsa-announce
SANS	http://www.sans.org/critical-security-controls/
SECTRACK (SecurityTracker)	http://securitytracker.com/
SECUNIA	http://secunia.com/advisories
SGI	ftp://patches.sgi.com/support/free/security/advisories/
SUSE SUSE-SA (SUSE Security Announce)	https://www.suse.com/support/security/advisories/

XF (X-force)	http://xforce.iss.net/

Problem ranjivosti se može sagledati i kroz Symantec-ov izveštaj o ranjivostima za 2011. godinu prema kome je broj ranjivosti iznosio 4989[526], što znači da se svake nedelje pojavljuje skoro 95 novih ranjivosti [527] . Kritičan period predstavlja period između publikovanja ranjivosti i primene zakrpe nad ranjivim programom ili servisom na sistemu. Alat korišćen za potrebe ovog rada zove se RAPID 7 Nexpose (slika 75). Datum skeniranja ranjivosti odnosi se na avgust 2011. godine i novembar 2013. godine (podrazumeva se da će se nakon završetka ovog rada pojaviti nove ranjivisti koje se odnose na operativne sisteme i servise). Pomoću ovog alata moguće je vršiti planirana i selektivna testiranja nad mrežnim servisima, nad serverima u okviru organizacije i ključnim servisima u potrazi za ranjivostima koje mogu biti zloupotrebljene od strane napadača. Nakon izvršenog skeniranja sistema biće predložene korektivne mere. Ukupan broj Operativnih sistema obuhvaćenih istraživanjem je 80 (51



Windows operativnih sistema i 29 Linux operativnih sistema).

Slika 75. Priprema alata Rapid 7 Nexpose za skeniranje servisa

Virtuelno okruženje sa operativnim sistemima prikazanim u tabelama (Tabela 15., Tabela 16.) za potrebe istraživanja realizovano je u sklopu Vmware ESX 5.1.0 platforme, IBM x3650 M3 servera i EMC VNX5300 sistema čime je ostvarena centralizovana konsolidacija svih virtuelnih računarskih sistema namenjinih ispitivanju. Time je obezbeđena stabilna platforma za efikasno ispitivanje ranjivosti uz visok nivo sigurnosti.
Platforma za realizaciju virtuelnog okruženja je VMWare ESXi 5.1.0 koja je implementirana na serveru IBMx3650 (slika 76.) i Storage sistemu EMC VNX5300.
Specifikacija servera IBMx3650 M3:
- 8 CPU Cores (2 x 4C Xeon E5620 80W, 2.4 GHZ 12MB cache
- 56 GB RAM PC3L-10600 ECC DDR3 1333 MHz memorije
- 4x IBM 900 GB SAS HDD
- ServeRAID M5014 SAS/SATA controller
- IBM 460W Redudant Power Supply

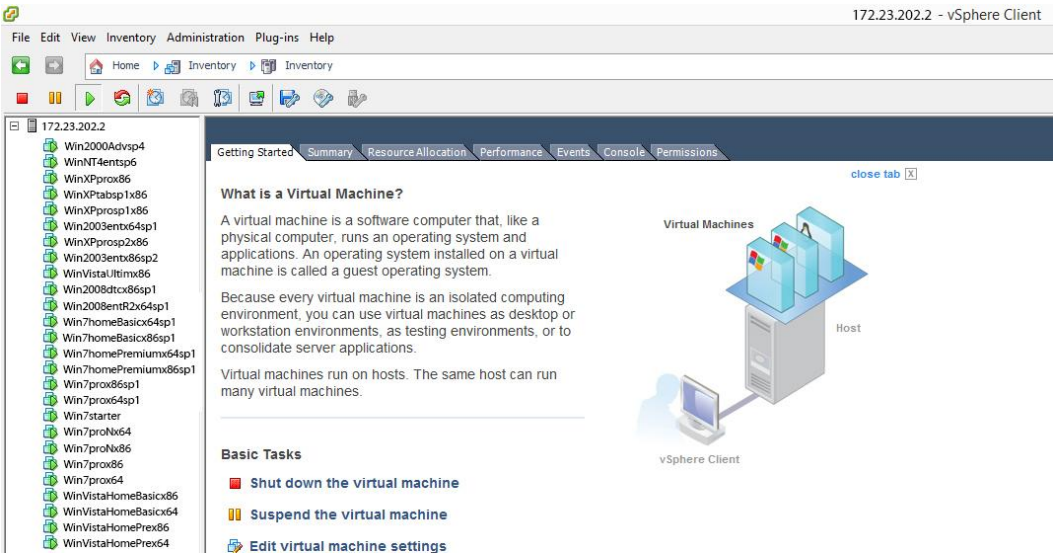
[526] Ovaj broj je baziran na osnovu velikog broja izvora uključujući mailing liste i preporuka velikog broja prozvođača programa i opreme, Izvor : http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=total_number_of_vulnerabilities
[527]Izvor : http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=total_number_of_vulnerabilities

- IBM UltraSlim Enhanced SATA Multi-Burner

Storage sistem EMC VNX5300 na koji su postavljene virtuelne mašine za potrebe ispitivanja, sastoji se od Intel Xeon 5600 procesora, sa 16GB cache memorije, 8 x 8Gbit FC porta, 8 x 1GbE porta, 25 x 600GB SAS 15k RPM, 25 x 2TB NL-SAS 7k RPM diskovima, 5 x 100GB FAST Cache Flash diska, rack ormanom VNX-40U, podrškom za dodatno proširenje kapaciteta, podrškom za CIFS, NFS, iSCSI i FC protokole, Local Protection Suite licencama, Security & Compliance Suite licencama, redundantnim napajanjima. Tabela 14. sadrži detaljniju specifikaciju ovog sistema.

Tabela 14. Specifikacija EMC VNX 5300 storage sistema

VNX5300 CONTROL STATION - EMC RACK
2 x 1GBE DM MODULE 4 PORT FOR VNX5300
VNX5300 ADD ON DM+FC SLIC-EMC RACK
VNX5300 DME: 1 D M+FC SLIC-EMC RACK
VNX5300 DPE; 15X3.5 DRIVES EMC RACK 8X600GB 15K
3 x 3U DAE WITH 15X3.5 INCH DRIVE SLOTS WITH RACK
5 x 100GB FAST CACHE FLSH 15X3.5IN DPE/DAE
17x 600GB 15K SAS DISK DRIVE
VNX 40U RACK WITH CONSOLE
EMC VNX5300 4 PORT 8G FC IO MODULE PAIR
ADDITIONAL 8 G FC SFP FOR VNX 51/53
RACK-40U-60 PWR CORD IEC 309
EMC DOCUMENTATION KIT FOR VNX5300
SECURITY & COMPLIANCE SUITE FOR VNX5300
LOCAL PROTECTION SUITE FOR VNX5300
FAST CACHE FOR VNX5300
BASE FILE LICENSE (CIFS AND FTP) FOR VNX5300
ADV FILE LICENSE (NFS; MPFS AND PNFS) FOR VNX5300
UNISPHERE UNIFIED & VNX OE VNX5300
25 x 2TB 7200RPM 6GB SAS DISK DRIVE
EMC 2ND OPTIONAL SPS
EMC ENHANCED SOFTWARE SUPPORT



Slika 76. Deo virtuelnih mašina pripremljenih za skeniranje ranjivih sistema

Sledeće tabele (Tabela 15. i Tabela 16.) prikazuju operativne sisteme obuhvaćene skeniranjem ranjivosti sa RAPID 7 Nexpose[528] alatom :

[528] https://www.rapid7.com/products/nexpose/

U tabeli 15. navedene su verzije Windows operativnih sistema, imena računara sa IP adresama obuhvaćenih skeniranjem alatom Rapid7 Nexpose. Windows operativni sistemi su difotlno instalirani bez dodatnih servisa.

Tabela 15. Windows operativni sistemi

Rbr	Operativni sistem	Ime računara	Ip adresa
1.	Windows nt 4 enterprise sp6	NT4entsp6	172.23.202.101
2.	Windows 95 OSR 2.5	Win95OSR	172.23.202.102
3	Windows 98 se	WIN98SE	172.23.202.103
4.	Windows ME	WINME	172.23.202.104
5.	Windows XP pro x86	WINXPprox86	172.23.202.105
6.	Windows xp pro sp1 x86	WINXPproSP1x86	172.23.202.106
7.	Windows xp pro sp2 x86	WINXPproSP2x86	172.23.202.107
8.	Windows xp pro sp3 x86	WINXPproSP3x86	172.23.202.108
9.	Windows xp tablet pc SP1	WINXPTabX86sp1	172.23.202.109
10.	Windows 2000 advanced server sp4	WIN2000ADVsp4	172.23.202.110
11.	Windows server 2003 Enterprise x64 SP1	WIN2003ENX64sp1	172.23.202.111
12.	Windows Server 2003 Enterprise x86 sp2	WIN2003ENSP2x86	172.23.202.112
13.	Windows Vista ultimate x86	VISTAx86ULT	172.23.202.113
14.	Windows Vista Ultimate SP2 x86	VISTAx86ULTSP2	172.23.202.114
15.	Windows 7 ultimate x86 sp1	WIN7x86ULTSP1	172.23.202.115
16.	Windows 7 ultimate x64	WIN7x64ULT	172.23.202.116
17.	Windows 2008 server datacenter x86 SP1 (kernel kao Windows Vista ultim sp2)	2008DTCX86SP1	172.23.202.117
18.	Windows 2008 enterprise x64 server R2 SP1 update jun2011SP1 (kernel kao Windows 7)	2008entR2X64SP1	172.23.202.118
19.	Windows 7 Home Basic SP1 x64	WIN7x64HoBaSp1	172.23.202.100
20.	Windows 7 Home Basic SP1 x86	WIN7x86HoBaSp1	172.23.202.99
21	Windows 7 Home Premium SP1 x64	WIN7x64HoPreSp1	172.23.202.98
22.	Windows 7 Home Premium SP1 x86	WIN7x86HoPreSp1	172.23.202.97
23.	Windows 7 Professional SP1 x64	WIN7x64ProSp1	172.23.202.96
24.	Windows 7 Professional SP1 x86	WIN7x86ProSp1	172.23.202.95
25.	Windows 7 starter	WIN7starter	172.23.202.94
26.	Windows 7 Professional N x64	WIN7ProNx64	172.23.202.93
26.	Windows 7 Professional N x86	WIN7ProNx86	172.23.202.92
28.	Windows 7 Professional x64	WIN7Prox64	172.23.202.91
29.	Windows 7 Professional x86	WIN7Prox86	172.23.202.90
30.	Windows Vista Home Basic x86	VISTAx86HoBa	172.23.202.89
31.	Windows Vista Home Basic x64	VISTAx64HoBa	172.23.202.88
32.	Windows Vista Home Premium x86	VISTAx86HoPre	172.23.202.87
33.	Windows Vista Home Premium x64	VISTAx64HoPre	172.23.202.86
34.	Windows Vista Business x86	VISTAx86Bsn	172.23.202.85
35.	Windows Vista Business x64	VISTAx64Bsn	172.23.202.84
36.	Windows Vista Ultimate x64	VISTAx64ULT	172.23.202.83
37.	Windows Vista Home Basic x86 SP2	VISTAx86HoBaSp2	172.23.202.82
38.	Windows Vista Home Basic x64 SP2	VISTAx64HoBaSp2	172.23.202.81
39.	Windows Vista Business x86 SP2	VISTAx86BsnSp2	172.23.202.80
40.	Windows Vista Business x64 SP2	VISTAx64BsnSp2	172.23.202.79

41.	Windows Vista Home Premium x86 SP2	VISTAx86HoPrSp2	172.23.202.78
42.	Windows Vista Home Premium x64 SP2	VISTAx64HoPrSp2	172.23.202.77
43.	Windows 2000 server Sp4	Win2000srv	172.23.202.76
44.	Windows server 2003 Enterprise x86 SP1	WIN2003ENX86sp1	172.23.202.75
45.	Windows server 2003 Standard x86 SP1	WIN2003StX86sp1	172.23.202.74
46.	Windows server 2003 Standard x64 SP1	WIN2003StX64sp1	172.23.202.73
47.	Windows Server 2003 Enterprise x64 SP2	WIN2003ENSP2x64	172.23.202.72
48.	Windows server 2003 Standard x86 SP2	WIN2003StX86sp2	172.23.202.71
49.	Windows server 2003 Standard x64 SP2	WIN2003StX64sp2	172.23.202.70
50.	Windows XP pro sp1 x64	WINXPproSP1x64	172.23.202.69
51	WWindows 2008 server Enterprise x86 SP1	2008EntX86SP1	172.23.202.68

U tabeli 16. navedene su verzije Linux operativnih sistema sa pridodanim servisima, imena računara sa IP adresama koji su obuhvaćeni skeniranjem, alatom Rapid7 Nexpose.

Tabela 16. Linux operativni sistemi

Rbr	Operativni sistem	Ime računara	Ip adresa
1.	Mandriva Linux Enterprise Server 5.2 x86	mandriva52enx86	172.23.202.124
2.	Mandriva Linux Enterprise Server 5.2 x64	mandriva52enx64	172.23.202.220
3.	Red Hat Enterprise Linux 4.8 AS x64	rhel48asx64	172.23.202.126
4.	Red Hat Enterprise Linux 4.8 AS x86	rhel48asx86	172.23.202.225
5.	Red Hat Enterprise Linux 5.2 x86	redhat52entx86	172.23.202.194
6.	Red Hat Enterprise Linux 5.2 x64	redhat52entx64	172.23.202.226
7.	Red Hat Enterprise Linux 5.1 x86	redhat51entx86	172.23.202.193
8.	Red Hat Enterprise Linux 5.1 x64	redhat51entx64	172.23.202.227
9.	Red Hat Enterprise Linux 5.6 x64	redhat56entx64	172.23.202.195
10.	Red Hat Enterprise Linux 5.6 x86	redhat56entx86	172.23.202.222
11.	Centos 5.6 x64	centos56x64	172.23.202.196
12.	Centos 5.6 x86	centos56x86	172.23.202.221
13.	Kubuntu 11.04 x86 desktop	kubun1104dskx86	172.23.202.122
14.	Ubuntu 11.04 x64 desktop	ubunt1104dskx64	172.23.202.200
15.	Ubuntu 11.04 x86 desktop	ubunt1104dskx86	172.23.202.230
16.	Ubuntu 11.04 x64 server	ubunt1104srvx64	172.23.202.135
17.	Ubuntu 11.04 x86 server	ubunt1104srvx86	172.23.202.231
18.	Kubuntu 11.04 x86 desktop	kubun1104dskx64	172.23.202.232
19.	Ubuntu 10.04.2 lts x64 server	ubunt1004srvx64	172.23.202.133
20.	Ubuntu 10.04.2 lts x86 server	ubunt1004srvx86	172.23.202.132
21.	Kubuntu 10.04.2 desktop x86	kubun1004dskx86	172.23.202.123
22.	Kubuntu 10.04.2 desktop x64	kubun1004dskx64	172.23.202.229
23.	Debian 60 x86	debian60x86	172.23.202.197
24.	SciLinux 60 x64	sciLinux60x64	172.23.202.199
25.	SciLinux 60 x86	sciLinux60x86	172.23.202.224
26.	Fedora 15 x86	fedora15x86	172.23.202.198
27.	Fedora 15 x64	fedora15x64	172.23.202.223
28.	Slackware 13.37 x86	slackware1337	172.23.202.131
29.	Opensuse 11.4 x86	opensuse1104x86	172.23.202.125

U sledećoj tabeli (Tablela 17.) prikazani su servisi koji su dodatno podignuti na Linux operativnim sistemima nakon difoltne instalacije operativnog sistema.

Tabela 17. Servisi podignuti na Linux operativnim sistemima

Rbr	Operativni sistem	Ip adresa	Dodati Servisi
1.	Mandriva Linux Enterprise Server 5.2 x86	172.23.202.124	Apache, PHP, MySql, Tomcat, SSH, FTP, HTTPS
2.	Mandriva Linux Enterprise Server 5.2 x64	172.23.202.220	Apache, PHP, MySql, Tomcat, SSH, FTP, HTTPS
3.	Red Hat Enterprise Linux 4.8 AS x64	172.23.202.126	Apache, PHP, MySql, SSH, FTP, HTTPS
4.	Red Hat Enterprise Linux 4.8 AS x86	172.23.202.225	Apache, PHP, MySql, SSH, FTP, HTTPS
5.	Red Hat Enterprise Linux 5.2 x86	172.23.202.194	Apache, PHP, MySql, SSH, FTP
6.	Red Hat Enterprise Linux 5.2 x64	172.23.202.226	Apache, PHP, MySql, SSH, FTP
7.	Red Hat Enterprise Linux 5.1 x86	172.23.202.193	Apache, PHP, MySql, SSH, FTP
8.	Red Hat Enterprise Linux 5.1 x64	172.23.202.227	Apache, PHP, MySql, SSH, FTP
9.	Red Hat Enterprise Linux 5.6 x64	172.23.202.195	Apache, PHP, MySql, SSH, FTP
10.	Red Hat Enterprise Linux 5.6 x86	172.23.202.222	Apache, PHP, MySql, SSH, FTP
11.	Centos 5.6 x64	172.23.202.196	Apache, PHP, MySql, SSH, FTP
12.	Centos 5.6 x86	172.23.202.221	Apache, PHP, MySql, SSH, FTP
13.	Kubuntu 11.04 x86 desktop	172.23.202.122	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
14.	Ubuntu 11.04 x64 desktop	172.23.202.200	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
15.	Ubuntu 11.04 x86 desktop	172.23.202.230	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
16.	Ubuntu 11.04 x64 server	172.23.202.135	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
17.	Ubuntu 11.04 x86 server	172.23.202.231	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
18.	Kubuntu 11.04 x86 desktop	172.23.202.232	Apache, PHP, MySql, SSH, FTP, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
19.	Ubuntu 10.04.2 lts x64 server	172.23.202.133	Apache, PHP, MySql, SSH, FTP, Tomcat, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
20.	Ubuntu 10.04.2 lts x86 server	172.23.202.132	Apache, PHP, MySql, SSH, FTP, Tomcat, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
21.	Kubuntu 10.04.2 desktop x86	172.23.202.123	Apache, PHP, MySql, SSH, FTP, Tomcat, IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
22.	Kubuntu 10.04.2 desktop	172.23.202.229	Apache, PHP, MySql, SSH, FTP, Tomcat,

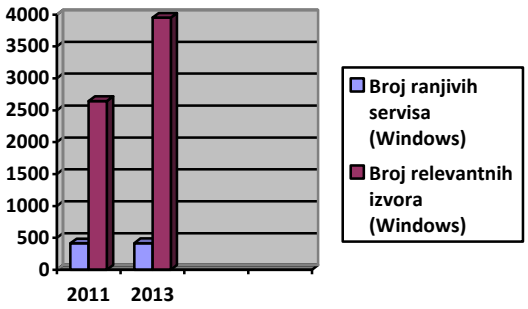
	x64		IMAP (Dovecot), IMAPS, POP, POPS, SAMBA
23.	Debian 60 x86	172.23.202.197	Apache, PHP, MySql, SSH, FTP, IMAP, IMAPS, POP, SAMBA
24.	SciLinux 60 x64	172.23.202.199	Apache, PHP, MySql, SSH, FTP
25.	SciLinux 60 x86	172.23.202.224	Apache, PHP, MySql, SSH, FTP
26.	Fedora 15 x86	172.23.202.198	Apache, PHP, MySql, SSH, FTP, NTP
27.	Fedora 15 x64	172.23.202.223	Apache, PHP, MySql, SSH, FTP, NTP
28.	Slackware 13.37 x86	172.23.202.131	Apache, PHP, MySql, SSH, FTP, NTP, SMTP
29.	Opensuse 11.4 x86	172.23.202.125	Apache, PHP, MySql, SSH, FTP

U tabeli 18. dat je prikaz ukupnog broja otkrivenih ranjivosti i njihovih relevantnih izvora koji se odnose na Windows operativne sisteme u 2011. i 2013. godini (grupisanih u 16 tabela u prilogu na disku, prema familiji Windows-a koji imaju iste ranjive servise):

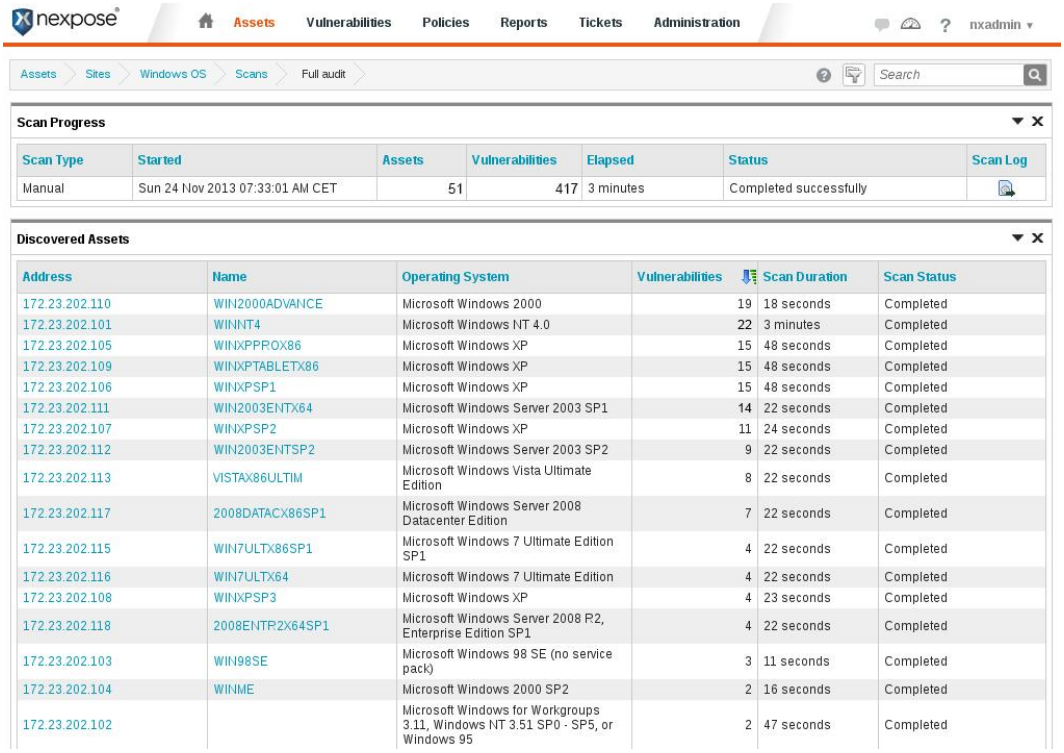
Tabela 18. Windows ranjivosti i njihovi izvori iz 2011. i 2013. godine

Rbr	**Operativni sistem**	**Ip adresa**	**Broj ranjivosti u 2011.**	**Broj ranjivosti u 2013.**	**Razlika**	**Br. izvora 2011.**	**Br. izvora 2013.**
1.	Windows nt 4 enterprise sp6	172.23.202.101	21	22	1	97	139
2.	Windows 95 OSR 2.5	172.23.202.102	2	2	0	23	27
3	Windows 98 SE	172.23.202.103	3	3	0	22	27
4.	Windows ME	172.23.202.104	2	2	0	23	23
5.	Windows XP pro x86	172.23.202.105	15	15	0	174	247
6.	Windows XP pro sp1 x86	172.23.202.106	15	15	0	174	248
7.	Windows XP pro sp2 x86	172.23.202.107	11	11	0	54	54
8.	Windows XP pro sp3 x86	172.23.202.108	4	4	0	9	10
9.	Windows XP tablet pc SP1 x86	172.23.202.109	15	15	0	174	248
10.	Windows 2000 advanced server sp4	172.23.202.110	18	19	1	225	54
11.	Windows server 2003 Enterprise x64 SP1	172.23.202.111	14	14	0	89	10
12.	Windows Server 2003 Enterprise x86 sp2	172.23.202.112	9	9	0	41	248
13.	Windows Vista ultimate x86	172.23.202.113	8	8	0	53	307
14.	Windows Vista Ultimate SP2 x86	172.23.202.114	7	7	0	24	135
15.	Windows 7 ultimate x86 sp1	172.23.202.115	4	4	0	8	73
16.	Windows 7 ultimate x64	172.23.202.116	4	4	0	8	57
17.	Windows 2008 server datacenter x86 SP1 (kernel kao Windows Vista ultim sp2)	172.23.202.117	7	7	0	24	42
18.	Windows 2008 enterprise x64 server R2 SP1 update jun2011SP1 (kerenel kao Windows 7)	172.23.202.118	4	4	0	8	8
19.	Windows 7 Home Basic SP1 x64	172.23.202.100	4	4	0	8	8
20.	Windows 7 Home Basic SP1 x86	172.23.202.99	4	4	0	8	42
21	Windows 7 Home Premium SP1 x64	172.23.202.98	4	4	0	8	8
22.	Windows 7 Home Premium SP1 x86	172.23.202.97	4	4	0	8	8

23.	Windows 7 Professional SP1 x64	172.23.202.96	4	4	0	8	8
24.	Windows 7 Professional SP1 x86	172.23.202.95	4	4	0	8	8
25.	Windows 7 starter	172.23.202.94	4	4	0	8	8
26.	Windows 7 Professional N x64	172.23.202.93	4	4	0	8	8
26.	Windows 7 Professional N x86	172.23.202.92	4	4	0	8	8
28.	Windows 7 Professional x64	172.23.202.91	4	4	0	8	8
29.	Windows 7 Professional x86	172.23.202.90	4	4	0	8	8
30.	Windows Vista Home Basic x86	172.23.202.89	8	8	0	53	57
31.	Windows Vista Home Basic x64	172.23.202.88	8	8	0	53	57
32.	Windows Vista Home Premium x86	172.23.202.87	8	8	0	53	57
33.	Windows Vista Home Premium x64	172.23.202.86	8	8	0	53	57
34.	Windows Vista Business x86	172.23.202.85	8	8	0	53	57
35.	Windows Vista Business x64	172.23.202.84	8	8	0	53	57
36.	Windows Vista Ultimate x64	172.23.202.83	8	8	0	53	57
37.	Windows Vista Home Basic x86 SP2	172.23.202.82	7	7	0	24	42
38.	Windows Vista Home Basic x64 SP2	172.23.202.81	7	7	0	24	42
39.	Windows Vista Business x86 SP2	172.23.202.80	7	7	0	24	42
40.	Windows Vista Business x64 SP2	172.23.202.79	7	7	0	24	42
41.	Windows Vista Home Premium x86 SP2	172.23.202.78	7	7	0	24	42
42.	Windows Vista Home Premium x64 SP2	172.23.202.77	7	7	0	24	42
43.	Windows 2000 server Sp4	172.23.202.76	18	19	1	225	307
44.	Windows server 2003 Enterprise x86 SP1	172.23.202.75	14	14	0	89	135
45.	Windows server 2003 Standard x86 SP1	172.23.202.74	14	14	0	89	135
46.	Windows server 2003 Standard x64 SP1	172.23.202.73	14	14	0	89	135
47.	Windows Server 2003 Enterprise x64 SP2	172.23.202.72	9	9	0	41	73
48.	Windows server 2003 Standard x86 SP2	172.23.202.71	9	9	0	41	73
49.	Windows server 2003 Standard x64 SP2	172.23.202.70	9	9	0	41	73
50.	Windows XP pro sp1 x64	172.23.202.69	15	15	0	174	248
51	Windows 2008 server Enterprise x86 SP1	172.23.202.68	7	7	0	24	42
UKUPNO			**414**	**417**	**3**	**2646**	**3951**



Grafikon 1. Prikaz pronađenih ranjivih servisa na Windows OS sa brojem relevantnih izvora publikovanih u 2011. i 2013. godini



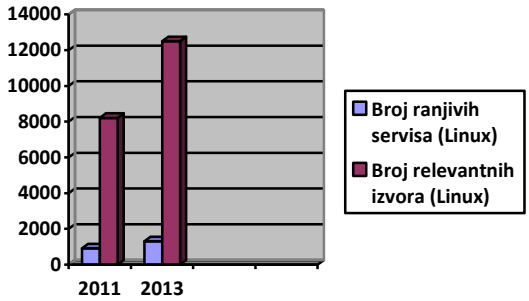
Slika 77. Izgled završenog skeniranja ranjivih servisa na Windows platformama u 2013. godini sa alatom Rapid 7 Nexpose

Tabela 19. daje prikaz ukupnog broja otkrivenih ranjivosti i njihovih relevantnih izvora koji se odnose na Linux operativne sisteme u 2011. i 2013. godini :

Tabela 19. Linux ranjivosti i njihovi izvori iz 2011. i 2013. godine

Rbr	Operativni sistem	Ip adresa	Broj ranjivosti u 2011.	Broj ranjivosti u 2013.	Razlika	Br. izvora 2011.	Br. izvora 2013.
1.	Mandriva Linux Enterprise Server 5.2 x86	172.23.202.124	43	58	15	314	483
2.	Mandriva Linux Enterprise Server 5.2 x64	172.23.202.220	43	58	15	314	483

3.	Red Hat Enterprise Linux 4.8 AS x64	172.23.202.126	50	56	6	698	801
4.	Red Hat Enterprise Linux 4.8 AS x86	172.23.202.225	50	56	6	698	801
5.	Red Hat Enterprise Linux 5.2 x86	172.23.202.194	47	57	10	599	735
6.	Red Hat Enterprise Linux 5.2 x64	172.23.202.226	47	57	10	599	735
7.	Red Hat Enterprise Linux 5.1 x86	172.23.202.193	47	57	10	599	735
8.	Red Hat Enterprise Linux 5.1 x64	172.23.202.227	47	57	10	599	735
9.	Red Hat Enterprise Linux 5.6 x64	172.23.202.195	45	56	11	578	722
10.	Red Hat Enterprise Linux 5.6 x86	172.23.202.222	45	56	11	578	722
11.	Centos 5.6 x64	172.23.202.196	45	56	11	578	722
12.	Centos 5.6 x86	172.23.202.221	45	56	11	578	722
13.	Kubuntu 11.04 x86 desktop	172.23.202.122	22	39	17	55	210
14.	Ubuntu 11.04 x64 desktop	172.23.202.200	22	39	17	55	210
15.	Ubuntu 11.04 x86 desktop	172.23.202.230	22	39	17	55	210
16.	Ubuntu 11.04 x64 server	172.23.202.135	22	39	17	55	210
17.	Ubuntu 11.04 x86 server	172.23.202.231	22	39	17	55	210
18.	Kubuntu 11.04 x86 desktop	172.23.202.232	22	39	17	55	210
19.	Ubuntu 10.04.2 lts x64 server	172.23.202.133	30	44	14	151	308
20.	Ubuntu 10.04.2 lts x86 server	172.23.202.132	30	44	14	151	308
21.	Kubuntu 10.04.2 desktop x86	172.23.202.123	30	44	14	151	308
22.	Kubuntu 10.04.2 desktop x64	172.23.202.229	30	44	14	151	308
23.	Debian 60 x86	172.23.202.197	23	39	16	99	261
24.	SciLinux 60 x64	172.23.202.199	19	35	16	103	261
25.	SciLinux 60 x86	172.23.202.224	19	35	16	103	261
26.	Fedora 15 x86	172.23.202.198	14	30	16	50	194
27.	Fedora 15 x64	172.23.202.223	14	30	16	50	194
28.	Slackware 13.37 x86	172.23.202.131	11	26	15	53	212
29.	Opensuse 11.4 x86	172.23.202.125	8	22	14	48	185
UKUPNO			**914**	**1307**	**393**	**8172**	**12456**



Grafikon 2. Prikaz pronađenih ranjivih servisa na Linux OS sa brojem relevantnih izvora koji publikuju ranjivosti u 2011. i 2013. godini

U tabeli 20. prikazan je broj ranjivih servisa na Windows OS sa detaljima prikaza prema značajnostima (Kritičan-Kr, Ozbiljan-Oz, Umere-Um, Ukupno-Uk)

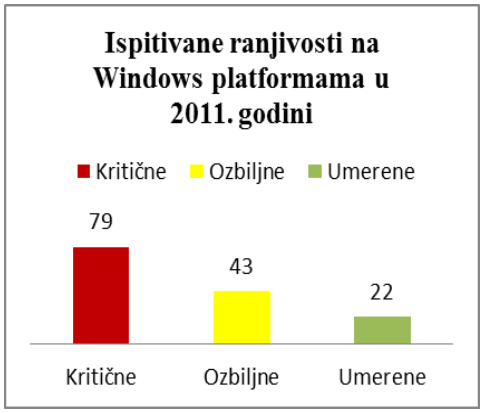
Tabela 20. Broj pronađenih ranjivih servisa na Windows OS klasifikovanih prema značajnosti

Rbr	**Operativni sistem**	**Ip adresa**	**Broj ranjivosti u 2011.**				**Broj ranjivosti u 2013.**			
			Kr	**Oz**	**Um**	**Uk**	**Kr**	**Oz**	**Um**	**Uk**
1.	Windows nt 4 enterprise sp6	172.23.202.101	9	11	1	21	10	11	1	22

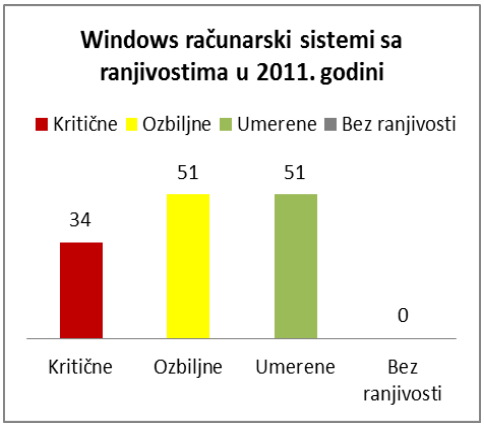
2.	Windows 95 OSR 2.5	172.23.202.102	0	1	1	2	0	1	1	2
3	Windows 98 se	172.23.202.103	0	1	2	3	0	1	2	3
4.	Windows ME	172.23.202.104	0	1	1	2	0	1	1	2
5.	Windows XP pro x86	172.23.202.105	11	3	1	15	11	3	1	15
6.	Windows xp pro sp1 x86	172.23.202.106	11	3	1	15	11	3	1	15
7.	Windows xp pro sp2 x86	172.23.202.107	8	2	1	11	8	2	1	11
8.	Windows xp pro sp3 x86	172.23.202.108	1	2	1	4	1	2	1	4
9.	Windows xp tablet pc SP1	172.23.202.109	11	3	1	15	11	3	1	15
10.	Windows 2000 advanced server sp4	172.23.202.110	13	1	4	18	14	4	1	19
11.	Windows server 2003 Enterprise x64 SP1	172.23.202.111	10	3	1	14	10	3	1	14
12.	Windows Server 2003 Enterprise x86 sp2	172.23.202.112	6	2	1	9	6	2	1	9
13.	Windows Vista ultimate x86	172.23.202.113	4	2	2	8	4	2	2	8
14.	Windows Vista Ultimate SP2 x86	172.23.202.114	3	2	2	7	3	2	2	7
15.	Windows 7 ultimate x86 sp1	172.23.202.115	0	2	2	4	0	2	2	4
16.	Windows 7 ultimate x64	172.23.202.116	0	2	2	4	0	2	2	4
17.	Windows 2008 server Datacenter x86 SP1 (kernel kao Windows Vista ultimate sp2)	172.23.202.117	3	2	2	7	3	2	2	7
18.	Windows 2008 enterprise x64 server R2 SP1 update jun 2011 (kernel kao Windows 7)	172.23.202.118	0	2	2	4	0	2	2	4
19.	Windows 7 Home Basic SP1 x64	172.23.202.100	0	2	2	4	0	2	2	4
20.	Windows 7 Home Basic SP1 x86	172.23.202.99	0	2	2	4	0	2	2	4
21	Windows 7 Home Premium SP1 x64	172.23.202.98	0	2	2	4	0	2	2	4
22.	Windows 7 Home Premium SP1 x86	172.23.202.97	0	2	2	4	0	2	2	4
23.	Windows 7 Professional SP1 x64	172.23.202.96	0	2	2	4	0	2	2	4
24.	Windows 7 Professional SP1 x86	172.23.202.95	0	2	2	4	0	2	2	4
25.	Windows 7 starter	172.23.202.94	0	2	2	4	0	2	2	4
26.	Windows 7 Professional N x64	172.23.202.93	0	2	2	4	0	2	2	4
26.	Windows 7 Professional N x86	172.23.202.92	0	2	2	4	0	2	2	4
28.	Windows 7 Professional x64	172.23.202.91	0	2	2	4	0	2	2	4
29.	Windows 7 Professional x86	172.23.202.90	0	2	2	4	0	2	2	4
30.	Windows Vista Home Basic x86	172.23.202.89	4	2	2	8	4	2	2	8
31.	Windows Vista Home Basic x64	172.23.202.88	4	2	2	8	4	2	2	8
32.	Windows Vista Home Premium x86	172.23.202.87	4	2	2	8	4	2	2	8
33.	Windows Vista Home Premium x64	172.23.202.86	4	2	2	8	4	2	2	8
34.	Windows Vista Business x86	172.23.202.85	4	2	2	8	4	2	2	8
35.	Windows Vista Business x64	172.23.202.84	4	2	2	8	4	2	2	8
36.	Windows Vista Ultimate x64	172.23.202.83	4	2	2	8	4	2	2	8
37.	Windows Vista Home Basic x86 SP2	172.23.202.82	3	2	2	7	3	2	2	7
38.	Windows Vista Home Basic x64 SP2	172.23.202.81	3	2	2	7	3	2	2	7
39.	Windows Vista Business x86 SP2	172.23.202.80	3	2	2	7	3	2	2	7
40.	Windows Vista Business x64 SP2	172.23.202.79	3	2	2	7	3	2	2	7
41.	Windows Vista Home Premium x86 SP2	172.23.202.78	3	2	2	7	3	2	2	7
42.	Windows Vista Home Premium x64 SP2	172.23.202.77	3	2	2	7	3	2	2	7
43.	Windows 2000 server Sp4	172.23.202.76	13	4	1	18	14	4	1	19
44.	Windows server 2003 Enterprise x86 SP1	172.23.202.75	10	3	1	14	10	3	1	14
45.	Windows server 2003 Standard x86 SP1	172.23.202.74	10	3	1	14	10	3	1	14

46.	Windows server 2003 Standard x64 SP1	172.23.202.73	10	3	1	14	10	3	1	14
47.	Windows Server 2003 Enterprise x64 SP2	172.23.202.72	6	2	1	9	6	2	1	9
48.	Windows server 2003 Standard x86 SP2	172.23.202.71	6	2	1	9	6	2	1	9
49.	Windows server 2003 Standard x64 SP2	172.23.202.70	6	2	1	9	6	2	1	9
50.	Windows XP pro sp1 x64	172.23.202.69	11	3	1	15	11	3	1	15
51	Windows 2008 server Enterprise x86 SP1	172.23.202.68	3	2	2	7	3	2	2	7
UKUPNO			**211**	**117**	**86**	**414**	**214**	**120**	**83**	**417**

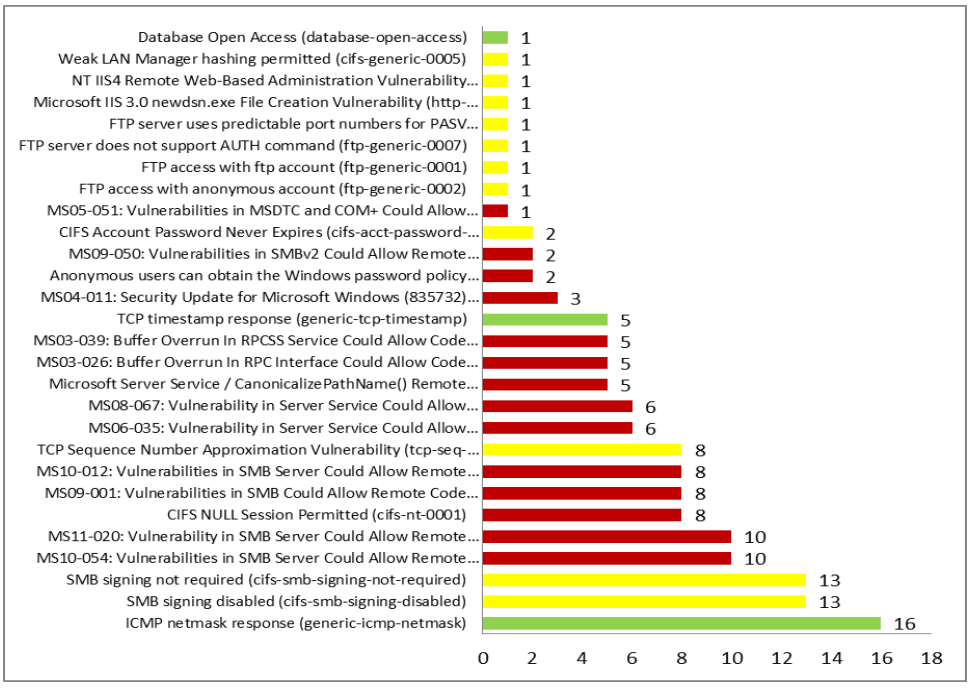
Ispitivanje je izvršeno na 51 Windows operativnom sistemu. U 2011. godini pronađeno je 144 jedinstvene ranjivosti, a na nivou svih skeniranih Windows sistema ukupan broj iznosi 414 ranjivosti (tabela 20, grafikon 1). Od toga je pronađeno jedinstvenih 79 kritičnih, 43 ozbiljnih i 22 umerene ranjivosti (grafikon 3a.), odnosno posmatrajući sve skenirane sisteme zajedno 211 kritičnih, 117 ozbiljnih i 86 umerenih ranjivosti (tabela 20). Kritične ranjivosti zahtevaju hitnu intervenciju. One relativno lako mogu da se zloupotrebe od strane zlonamernog napadača i njihovim iskorišćavanjem moguće je dobijanje putpune kontrole nad pogođenim računarskim sistemom. Ozbiljne ranjivosti su teže za iskorišćavanje i u većini slučajeva ne mogu da obezbede istovremen pristup sistemu. Kada je reč o umerenim ranjivostima, one najčešće pružaju informacije koje napadači mogu da iskoriste za organizovanje budućeg napada na računarske sisteme u mreži. Umerene ranjivosti takođe moraju biti blagovremeno razrešene, ali nisu hitne prethodne dve opisane. Kao što je već spomenuto, kada se posmatraju računarski sistemi pojedinačno, ukupno je pronađeno 211 kritičnih, 117 ozbiljnih i 86 umerenih ranjivosti. Kritične ranjivosti su pronađene kod ukupno 34 računarska sistema i oni su najviše podložni napadu (grafikon 3b.). Kod ukupno 51-og računarskog sistema su pronađene ozbiljne ranjivosti. Umerene ranjivosti su takođe prisutne na 51-om operativnom sistemu. Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima u 2011. godini dat je na grafikonu 4. Iako nisu dodavani dodatni servisi nakon difoltne instalacije, može se zaključiti da nijedan ispitivani sistem nije bez ranjivosti.



Grafikon 3a. Pronađene ranjivosti na ispitivanim Windows OS u 2011. godini

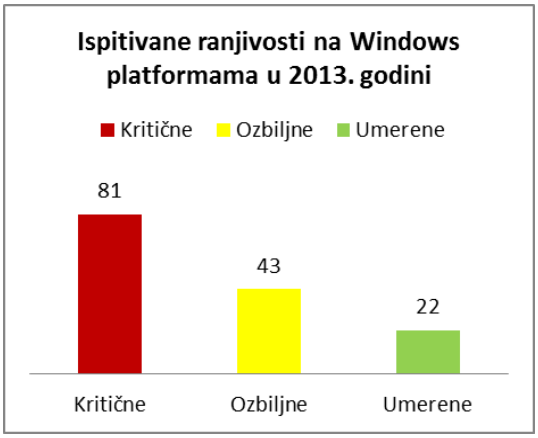


Grafikon 3b. Prikaz broja Windows računarskih sistema prema težini ranjivosti u 2011.godini

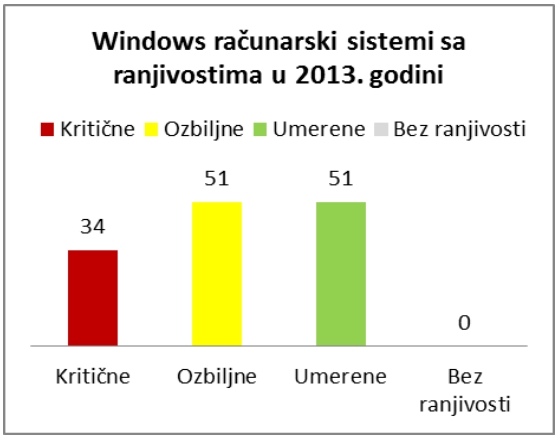


Grafikon 4. Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima u 2011. godini za Windows OS

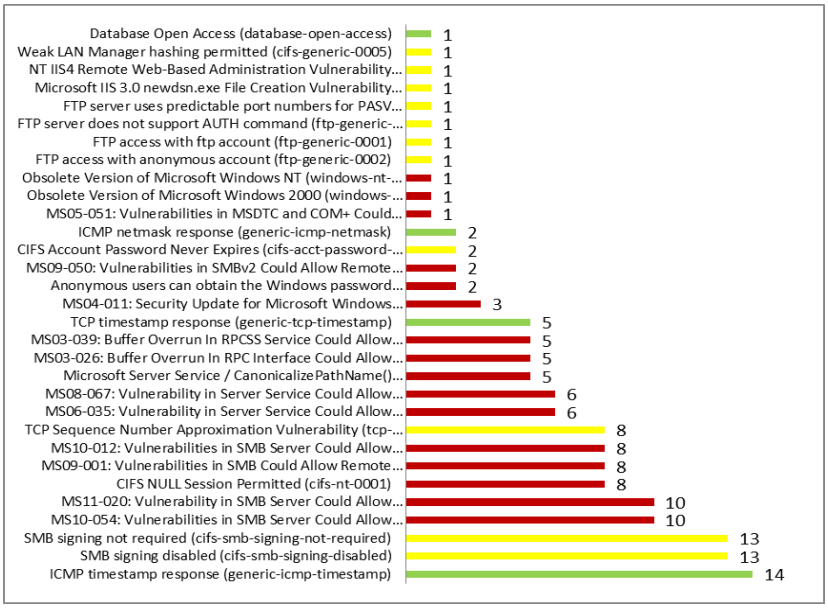
U 2013. godini pronađeno je 146 jedinstvenih ranjivosti, a na nivou svih skeniranih Windows sistema ukupan broj iznosi 417 ranjivosti (tabela 20., grafikon 1., slika 77.). Od toga je pronađeno 81 kritične, 43 ozbiljne i 22 umerene ranjivosti (grafikon 5.). Kada se posmatraju računarski sistemi pojedinačno, pronađeno je 214 kritičnih, 120 ozbiljnih i 83 umerenih ranjivosti. Kritične ranjivosti su pronađene na 34 računarska sistema i oni su najviše podložni napadu. Kod 51-og računarskog sistema su pronađene ozbiljne ranjivosti. Umerene ranjivosti su takođe prisutne na 51-om operativnom sistemu (grafikon 6.). Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima u 2013. godini dat je na grafikonu 7. Iako nisu dodavani dodatni servisi nakon difoltne instalacije može se zaključiti da nijedan ispitivani sistem nije bez ranjivosti.



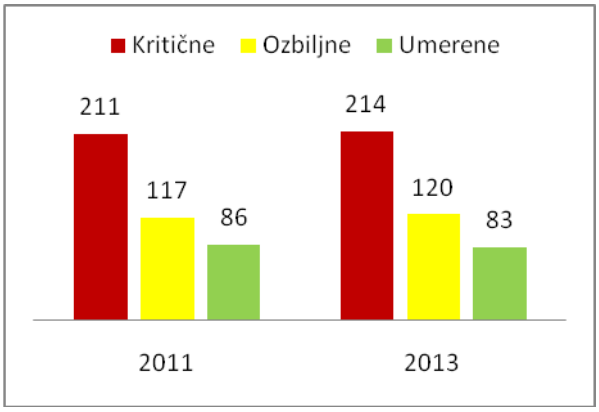
Grafikon 5. Pronađene ranjivosti na ispitivanim Windows OS u 2013. godini



Grafikon 6. Prikaz broja Windows računarskih sistema prema težini ranjivosti iz 2013.godine



Grafikon 7. Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima iz 2013. godine



Grafikon 8. Ranjivosti globalno posmatrano po godinama za sve Windows operativne sisteme

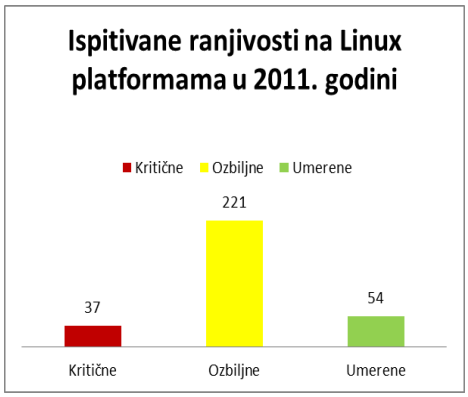
Prema prikazanom može se zaključiti da su svi skenirani sistemi ranjivi, ali da nije došlo do značajnog povećanja ranjivosti u periodu između 2011. i 2013 godine (kada su u pitanju skenirani Windows operativni sistemi bez instaliranih dodatnih servisa, videti grafikon 8). Zabeležen je značajan rast izvora o ranjivostima na Windows operativnim sistemima sa 2646 na 3951 (tabela 18., grafikon 1.). S obzirom da nije zabeležen značajan rast ranjivosti, a da je zabeležen značajan rast izvora o ranjivostima, može se zaključiti da su se postojeće ranjivosti zloupotrebljavale na različite načine.
U tabeli 21. prikazan je broj ranjivosti na Linux OS sa detaljima prikaza prema značajnostima (Kritičan-Kr, Ozbiljan-Oz, Umere-Um, Ukupno-Uk)

Tabela 21. Broj pronađenih ranjivih servisa na Linux OS klasifikovanih prema značajnosti

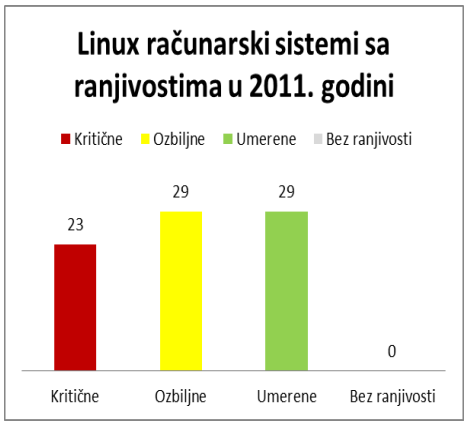
Rbr	**Operativni sistem**	**Ip adresa**	**Broj ranjivosti u 2011.**				**Broj ranjivosti u 2013.**			
			Kr	**Oz**	**Um**	**Uk**	**Kr**	**Oz**	**Um**	**Uk**
1.	Mandriva Linux Enterprise Server 5.2 x86	172.23.202.124	6	30	7	43	7	40	11	58
2.	Mandriva Linux Enterprise Server 5.2 x64	172.23.202.220	6	30	7	43	7	40	11	58
3.	Red Hat Enterprise Linux 4.8 AS x64	172.23.202.126	10	35	5	50	10	41	5	56
4.	Red Hat Enterprise Linux 4.8 AS x86	172.23.202.225	10	35	5	50	10	41	5	56
5.	Red Hat Enterprise Linux 5.2 x86	172.23.202.194	5	37	5	47	5	46	6	57
6.	Red Hat Enterprise Linux 5.2 x64	172.23.202.226	5	37	5	47	5	46	6	57
7.	Red Hat Enterprise Linux 5.1 x86	172.23.202.193	5	37	5	47	5	46	6	57
8.	Red Hat Enterprise Linux 5.1 x64	172.23.202.227	5	37	5	47	5	46	6	57
9.	Red Hat Enterprise Linux 5.6 x64	172.23.202.195	5	35	5	45	5	45	6	56
10.	Red Hat Enterprise Linux 5.6 x86	172.23.202.222	5	35	5	45	5	45	6	56
11.	Centos 5.6 x64	172.23.202.196	5	35	5	45	5	45	6	56
12.	Centos 5.6 x86	172.23.202.221	5	35	5	45	5	45	6	56
13.	Kubuntu 11.04 x86 desktop	172.23.202.122	4	12	6	22	7	23	9	39
14.	Ubuntu 11.04 x64 desktop	172.23.202.200	4	12	6	22	7	23	9	39
15.	Ubuntu 11.04 x86 desktop	172.23.202.230	4	12	6	22	7	23	9	39
16.	Ubuntu 11.04 x64 server	172.23.202.135	4	12	6	22	7	23	9	39
17.	Ubuntu 11.04 x86 server	172.23.202.231	4	12	6	22	7	23	9	39
18.	Kubuntu 11.04 x86 desktop	172.23.202.232	4	12	6	22	7	23	9	39
19.	Ubuntu 10.04.2 lts x64 server	172.23.202.133	5	19	6	30	7	30	7	44
20.	Ubuntu 10.04.2 lts x86 server	172.23.202.132	5	19	6	30	7	30	7	44
21.	Kubuntu 10.04.2 desktop x86	172.23.202.123	5	19	6	30	7	30	7	44
22.	Kubuntu 10.04.2 desktop x64	172.23.202.229	5	19	6	30	7	30	7	44
23.	Debian 60 x86	172.23.202.197	2	17	4	23	4	30	5	39
24.	SciLinux 60 x64	172.23.202.199	0	15	4	19	0	29	6	35

25.	SciLinux 60 x86	172.23.202.224	0	15	4	19	0	29	6	35
26.	Fedora 15 x86	172.23.202.198	0	10	4	14	0	23	7	30
27.	Fedora 15 x64	172.23.202.223	0	10	4	14	0	23	7	30
28.	Slackware 13.37 x86	172.23.202.131	0	6	5	11	1	18	7	26
29.	Opensuse 11.4 x86	172.23.202.125	0	5	3	8	0	17	5	22
UKUPNO			**118**	**644**	**152**	**914**	**149**	**953**	**205**	**1307**

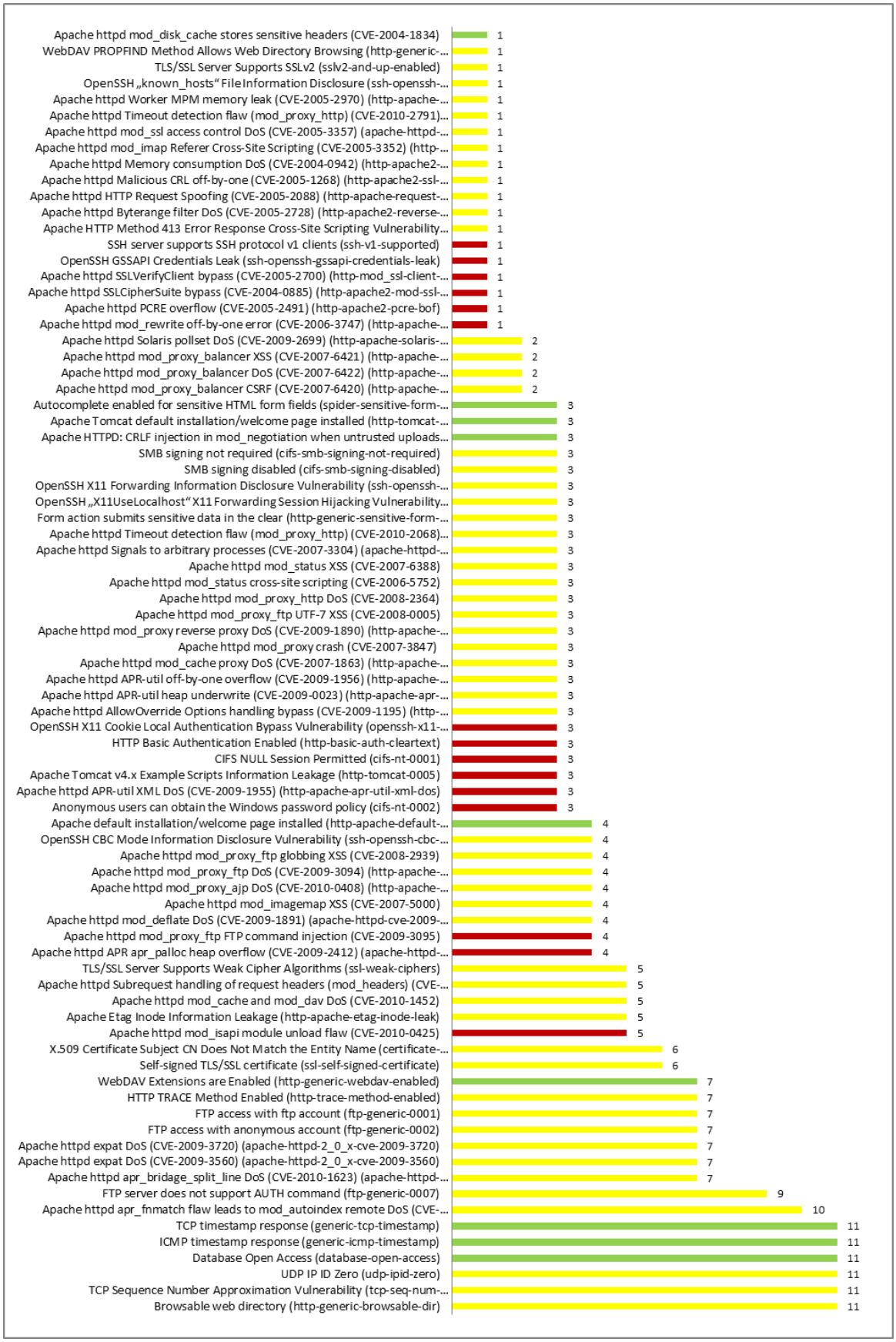
Ispitivanje je izvršeno na 29 Linux operativnih sistema. U 2011. godini pronađeno je 312 jedinstvene ranjivosti, a na nivou svih skeniranih Linux sistema ukupan broj iznosi 914 ranjivosti (tabela 21., grafikon 2.). Od toga je pronađeno 37 kritičnih, 221 ozbiljne i 54 umerene ranjivosti (grafikon 9.), odnosno posmatrajući sve skenirane sisteme zajedno 118 kritičnih, 644 ozbiljnih i 152 umerene ranjivosti (tabela 21.). Kao i kod Windows sistema treba spomenuti da kritične ranjivosti zahtevaju hitnu intervenciju. One relativno lako mogu da se zloupotrebe od strane zlonamernog napadača i njihovim iskorišćavanjem moguće je dobijanje putpune kontrole nad pogođenim računarskim sistemom. Ozbiljne ranjivosti su teže za iskorišćavanje i u većini slučajeva ne mogu da obezbede istovremen pristup sistemu. Kada je reč o umerenim ranjivostima, one najčešće pružaju informacije koje napadači mogu da iskoriste za organizovanje budućeg napada na računarske sisteme u mreži. Umerene ranjivosti takođe moraju biti blagovremeno razrešene, ali nisu hitne kao prethodne dve opisane. Kada se posmatraju računarski sistemi pojedinačno, pronađeno je 118 kritičnih, 644 ozbiljne i 152 umerene ranjivosti. Kritične ranjivosti su pronađene kod 23 računarska sistema i oni su najviše podložni napadu. Kod 29 računarskih sistema su pronađene ozbiljne ranjivosti. Umerene ranjivosti su takođe prisutne na 29 operativnih sistema (grafikon 10.). Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima u 2011.godini dat je na grafikonu 11. Nijedan ispitivani sistem nije bez ranjivosti.



Grafikon 9. Pronađene ranjivosti na ispitivanim Linux OS u 2011. godini

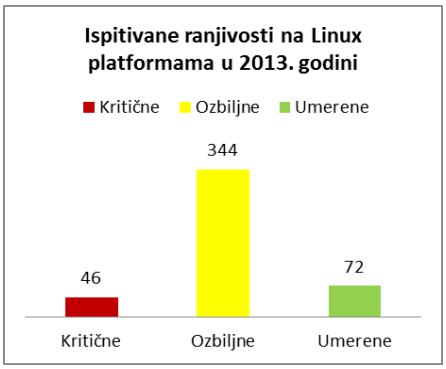


Grafikon 10. Prikaz broja Linux računarskih sistema prema težini ranjivosti u 2011.godini

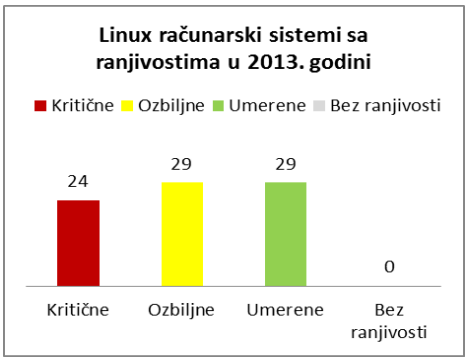


Grafikon 11. Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima u 2011. godini za Linux OS

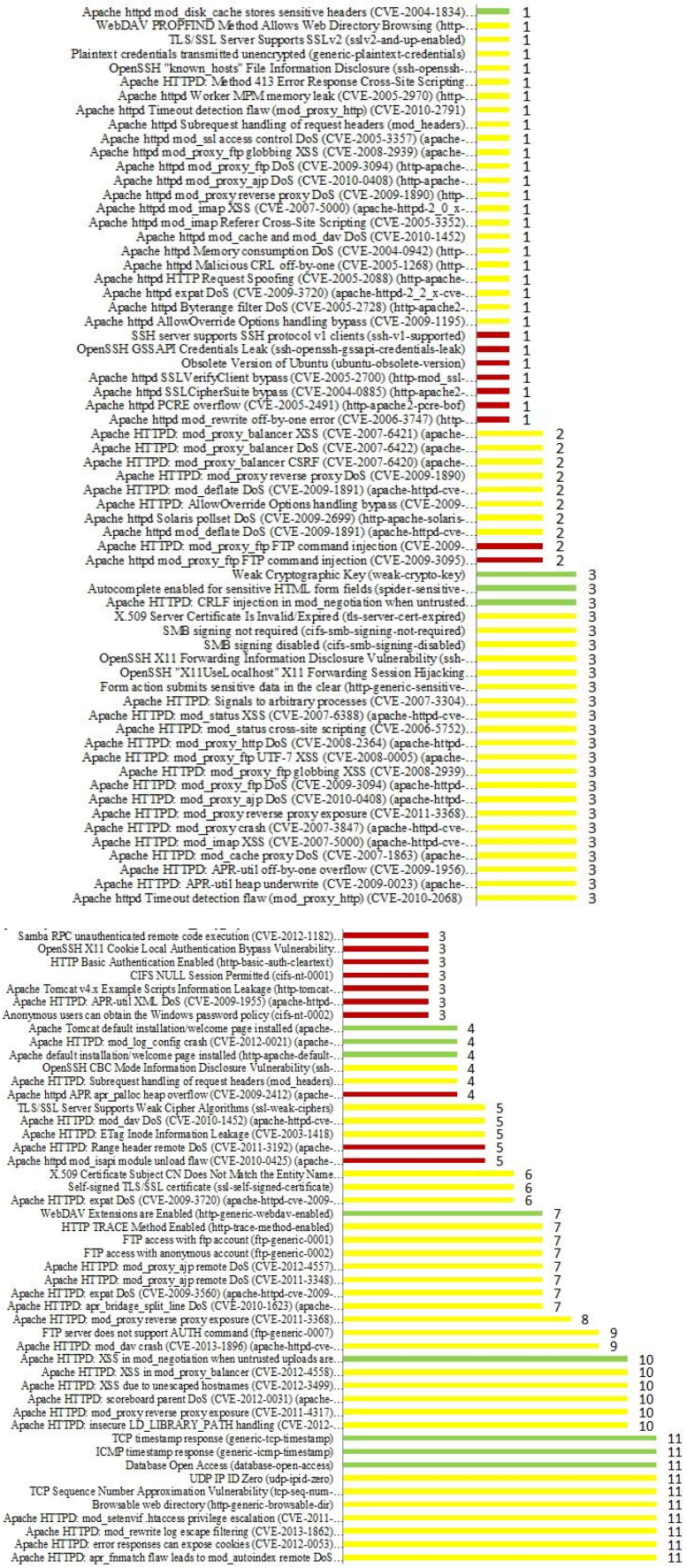
U 2013. godini pronađeno je 462 jedinstvene ranjivosti, a na nivou svih skeniranih Linux sistema ukupan broj iznosi 1307 ranjivosti (tabela 19., Grafikon2.). Od toga je pronađeno 46 kritične, 344 ozbiljne i 72 umerene ranjivosti (grafikon 12.). Kada se posmatraju računarski sistemi pojedinačno, pronađeno je 149 kritičnih, 953 ozbiljnih i 205 umerenih ranjivosti (tabela 21.). Kritične ranjivosti su pronađene na 34 računarska sistema i oni su najviše podložni napadu. Kod 51-og računarskog sistema su pronađene ozbiljne ranjivosti. Umerene ranjivosti su takođe prisutene na 51-om operativnom sistemu (grafikon 13.). Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima u 2013. godini dat je na grafikonu 14. Nijedan ispitivani sistem nije bez ranjivosti.



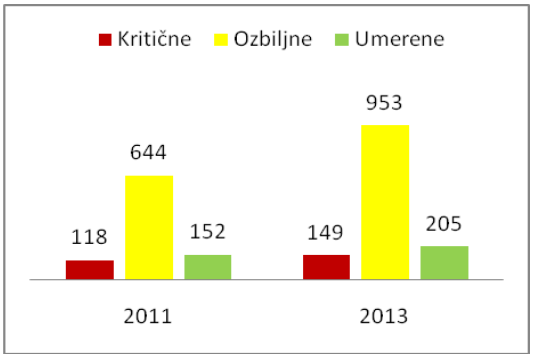
Grafikon 12. Pronađene ranjivosti na ispitivanim Linux OS u 2013. godini



Grafikon 13. Prikaz broja Linux računarskih sistema prema težini ranjivosti u 2013.godini



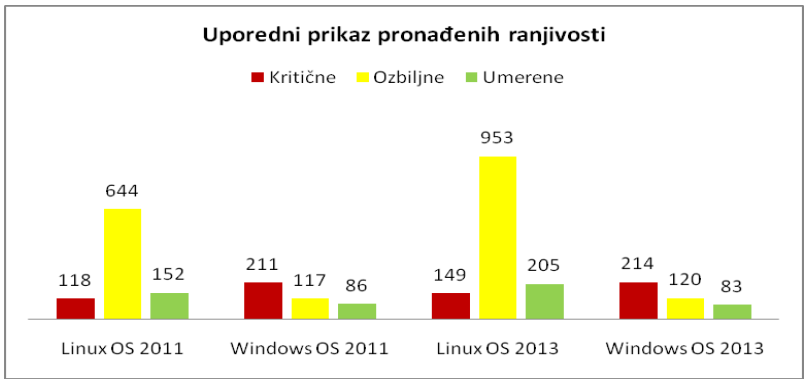
Grafikon 14. Prikaz pronađenih ranjivosti prema učestalosti na ispitivanim sistemima u 2013. godini za Linux OS



Grafikon 15. Ranjivosti globalno posmatrano po godinama za sve Linux operativne sisteme

Za razliku od Windows operativnih sistema na Linux sistemima su dodati određeni servisi da bi se pokazalo koliki je zapravo uticaj nastao na ranjivost sistema, povećavanjem broja servisa. Pridodati servisi prikazani su u Tabeli 17. a mogu se videti i u prilogu na disku. Nakon difoltne instalacije i dodatnih servisa može se zaključiti da nijedan ispitivani sistem nije bez ranjivosti. Takođe, primetan je značajan porast ranjivosti na sistemima u periodu od 2011. do 2013. godine (Tabela 21.). Kao što se može primetiti na grafikonu 15, kritične ranjivosti su porasle sa 118 na 149, ozbiljne ranjivosti su porasle sa 644 na 953 i umerene su porasle sa 152 na 205.

Takođe zabeležen je značajan rast izvora o ranjivostima na Linux operativnim sistemima sa 8172 na 12456 (tabela 19, grafikon 2.) što pokazuje na značajan porast ranjivosti i njihove zloupotrebe na različite načine. Uporedni prikaz pronađenih ranjivosti za Windows i Linux operativne sisteme u periodu između 2011. godine i 2013. godine, prema značajnosti dat je na grafikonu 16. :



Grafikon 16. Uporedni prikaz pronađenih ranjivosti na Linux i Windows operativnim sistemima

Globalno posmatrano, s obzirom je očekivano da kod Linux operativnih sistema nakon dodavanih servisa bude znatnog povećanja broja ranjivosti (što se može primetiti kroz rast kritičnih, ozbiljnih i umerenih ranjivosti na sistemu) značajan podatak jeste taj da je povećani broj kritičnih ranjivosti i dalje manji od kritičnih ranjivosti na Windows operativnim sistemima difoltno instaliranih bez dodavanih servisa.

Rezultati skeniranja svih operativnih sistema tabelarno prikazanih, izdvojeni su u poseban prilog ovog rada na disku. Windows operativni sistemi (ukupno 51) grupisani su u 16 tabela, prema familiji kojoj pripadaju i podudarajućim ranjivostima. Linux operativni sistemi (ukupno 29) grupisani su u 11 tabela prema familiji kojoj pripadaju i podudarajućim ranjivostima. S obzirom da je skeniranje vršeno u dve godine, to čini ukupno 54 tabele. U tabelama opisane su pronađene ranjivosti, utvrđen je njihov broj, dati su relevantni izvori koji ukazuju na ranjivost zajedno sa odrednicom značajnosti i data je preporuka za rešavanje

pronađene ranjivosti. Zbog obimnosti rezultata u radu će biti izdvojen samo jedan primer tabelarnog prikaza skeniranog Windows operativnog sistema koji sledi u nastavku :

Tabela 22. Tabelarni prikaz skeniranog Windows Xp pro SP2 operativnog sistema

Datum: 20.08.2011		**Operativni sistem i ime računara**			**Broj ranjivosti**
IP adresa: 172.23.202.107		**OS: Microsoft Windows XP P**ro Sp2 x86 IME: WINXPproSP2x86			**11**
Rbr	Ime ranjivosti	Opis ranjivosti	Izvor preporuke	Značaj	Rešavanje ranjivosti
1.	Microsoft Server Service / CanonicalizePathName( ) Remote Code Execution Vulnerability (dcerpc-msnetapi-netpathcanonicalize-dos)	Određene verzije Microsoft Windows-a su ranjive na daljinsko preopterećenje bafera (privremene memorije) koja bi mogla da kompromituje napadnuti računar. Posebno izrađen paket se može koristiti sa pozivom ka NetPathCanonicalize RPC ruti na servisu servera, pri čemu bi napadač mogao da izvrši kôd pod sistemskim nivoom pristupa	CVE: CVE-2006-3439[529], MS: MS06-040 [530], MSKB: 921883[531], SANS-06: W4[532], SANS-07: S2[533]	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB921883-x86-ENU.EXE[534]
2.	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (Windows-hotfix-ms08-067)	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava ranjivost koja je prijavljena od strane privatnog lica. Ranjivost bi mogla da omogući daljinsko izvršavanje koda ukoliko je napadnuti sistem primio posebno izrađen RPC zahtev. Na sistemima Microsoft Windows 2000, Windows XP, i Windows Server 2003, napadač bi mogao da iskoristi ovu ranjivost bez proveravanja autentičnosti i da pokrene proizvoljan kôd. Moguće je da ova ranjivost može biti upotrebljena za intenziviranje skrivenog korišćenja exploit-a. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije.	MS: MS08-067[535] MSKB: 958644[536] CVE: CVE-2008-4250[537] SECUNIA: 32326[538] URL1[539] URL2[540] URL3[541]	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB958644-x86-ENU.exe (648560 bytes)[542]
3.	MS09-001: Vulnerabilities in SMB Could Allow Remote	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava	MS: MS09-001[543] MSKB: 958687[544] CVE: CVE-2008-4114[545]	Kritičan	Uraditi download, a zatim instalirati Microsoft patch WindowsXP-KB958687-

[529] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3439
[530] http://technet.microsoft.com/en-us/security/bulletin/ms06-040
[531] http://support.microsoft.com/default.aspx?scid=kb;EN-US;921883
[532] http://www.sans.org/critical-security-controls/#w4
[533] http://www.sans.org/critical-security-controls/#s2
[534] download.microsoft.com/download/c/2/b/c2b41862-1113-4e40-a81a-d6971733e361/WindowsXP-KB921883-x86-ENU.exe
[535] http://technet.microsoft.com/en-us/security/bulletin/ms08-067
[536] http://support.microsoft.com/default.aspx?scid=kb;EN-US;958644
[537] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250
[538] http://secunia.com/advisories/32326/
[539] blogs.technet.com/swi/archive/2008/10/23/More-detail-about-MS08-067.aspx
[540] http://blogs.msdn.com/b/sdl/archive/2008/10/22/ms08-067.aspx
[541] http://blogs.technet.com/b/msrc/archive/2008/10/23/ms08-067-released.aspx
[542] http://download.Windowsupdate.com/msdownload/update/software/secu/2008/10/Windowsxpkb958644-x86-enu_5c135a8dae5721849430afe27af255f83e64f62b.exe
[543] http://technet.microsoft.com/en-us/security/bulletin/MS09-001
[544] http://support.microsoft.com/default.aspx?scid=kb;EN-US;958687
[545] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114

	Code Execution (Windows-hotfix-ms09-001)	nekoliko ranjivosti koje su privatno prijavljene a odnose se na protokol Microsoft Server Message Block-a (SMB). Ranjivosti mogu da omoguće daljinsko izvršenje kôda na ugroženim sistemima. Napadač koji je uspešno iskoristio ove ranjivosti može da instalira programe, pregleda, menja ili briše podatke ili otvara nove naloge sa potpunim korisničkim pravima. Praksa je pokazala da zaštitni zid i njegove standardne konfiguracije po difoltu mogu da pomognu u zaštiti mrežnih resursa od napada koji potiču izvan okvira organizacije. Za sisteme koji su stalno povezani na Internet preporuka je da imaju što manji broj izloženih portova.	CVE: CVE-2008-4835[546] CVE: CVE-2008-4834[547] SECUNIA: 31883[548] URL1[549] URL2[550] URL3[551]		x86-ENU.exe (658288 bytes)[552]
4.	MS10-012: Vulnerabilities in SMB Server Could Allow Remote Code Execution (Windows-hotfix-ms10-012)	172.23.202.107:139 172.23.202.107:445 Ovo ažuriranje bezbednosti rešava nekoliko ranjivosti koje su privatno prijavljene Microsoft Windows-u. Opasnost od ove ranjivosti leži u tome što bi ona omogućila daljinsko izvršavanje koda ukoliko bi napadač kreirao posebno opremljen SMB paket i poslao ga ugroženom sistemu. Praksa je pokazala da upotreba zaštitnog zida može da pomogne u zaštiti mrežnih resursa od napada (koji bi pokušali da iskoriste ove ranjivosti) koji potiču izvan okvira organizacije.	MS: MS10-012[553] MSKB - 971468[554] CVE: CVE-2010-0020[555] CVE: CVE-2010-0021[556] CVE: CVE-2010-0022[557] CVE CVE-2010-0231[558] SECUNIA 38510[559]	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB971468-x86-ENU.exe (664952 bytes)[560]
5.	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (Windows-hotfix-ms10-054)	172.23.202.107:139 172.23.202.107:445 Opis je isti kao kod ranjivosti MS10-012	CVE: CVE-2010-2550[561] CVE: CVE-2010-2551[562] CVE: CVE-2010-2552[563] MS: MS10-054[564] MSKB 982214[565]	Kritičan	Uraditi download a zatim instalirati Microsoft patch Windowsxp-kb982214-x86-enu.exe (661368 bytes)[566]
6.	MS11-020: Vulnerability in SMB	172.23.202.107:139 172.23.202.107:445 Opis je isti kao kod ranjivosti MS10-	CVE: CVE-2011-0661[567] MS: MS11-020[568]	Kritičan	Uraditi download a zatim instalirati Microsoft patch

[546] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835
[547] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834
[548] http://secunia.com/advisories/31883/
[549] http://www.vallejo.cc/proyectos/vista_SMB_write_DoS.htm
[550] http://www.zerodayinitiative.com/advisories/ZDI-09-001/
[551] http://www.zerodayinitiative.com/advisories/ZDI-09-002/
[552]http://download.Windowsupdate.com/msdownload/update/software/secu/2008/12/Windowsxp-kb958687-x86-enu_a9b85264e9b75e552ae10cd212937b8686a96833.exe
[553]http://technet.microsoft.com/en-us/security/bulletin/MS10-012
[554]http://support.microsoft.com/default.aspx?scid=kb;EN-US;971468
[555]http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020
[556]http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021
[557]http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022
[558] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231
[559] http://secunia.com/advisories/38510/
[560]http://download.Windowsupdate.com/msdownload/update/software/secu/2010/01/Windowsxp-kb971468-x86-enu_68d7899c8b8462219daf40f02c6fb9f362b1ee6b.exe
[561] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2550
[562] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2551
[563] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2552
[564] http://technet.microsoft.com/en-us/security/bulletin/MS10-054
[565] http://support.microsoft.com/default.aspx?scid=kb;EN-US;982214
[566]http://download.Windowsupdate.com/msdownload/update/software/secu/2010/07/Windowsxp-kb982214-x86-enu_a24853f682dad3157da4e4a39372951a8ec1e407.exe
[567] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661
[568] http://technet.microsoft.com/en-us/security/bulletin/ms11-020

	Server Could Allow Remote Code Execution (Windows-hotfix-ms11-020)	012	MSKB: 2508429[569]		Windowsxp-kb2508429-x86-enu.exe (664960 bytes)[570]
7.	MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (Windows-hotfixms06-035)	Ovo ažuriranje rešava nekoliko otkrivenih i privatno prijavljenih ranjivosti. Preporučuje se da korisnici odmah primene update.	CVE: CVE-2006-1314[571] CVE:VE-2006-1315[572] MS: MS06-035[573] MSKB: 917159[574] SANS-06: W4[575] SANS-07: S2[576] SECUNIA: 21007[577] XF: win-mailslot-bo(26818)[578] XF win-smb-information-disclosure(26820)[579]	Kritičan	Uraditi download a zatim instalirati Microsoft patch WindowsXP-KB917159-x86-ENU.exe (725304 bytes)[580]
8.	SMB signing disabled (cifs-smb-signing-disabled)	172.23.202.107:139 172.23.202.107:445 Ovaj sistem ne dozvoljava SMB potpisivanje. SMB potpisivanje omogućava primaocu SMB paketa da potvrdi autentičnost i pomaže u sprečavanju posrednika da izvrši napad na SMB. SMB potpisivanje može biti konfigurisano na jedan od tri načina: potpuno onemogućen (najmanje bezbedno), omogućen i zahtevan (najsigurnije).	MSKB: 887429[581] URL1[582]	Ozbiljan	Metoda za konfigurisanje SMB potpisivanja je specifična za svaki sistem i opisana je u KB 887429[583]. Napomena: proveriti da li je konfiguracija SMB potpisivanja podešena prema serveru. Na Samba serveru (u konfiguracijskom fajlu pod „global section“) podesiti da se omogući SMB potpisivanje: *server signing = auto* ili da se zahteva SMB potpisivanje: *server signing = mandatory*
9.	SMB signing not required (cifs-smb-signing-not-required)	172.23.202.107:139 172.23.202.107:445 Sistem omogućava ali ne zahteva SMB potpisivanje.	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti	Ozbiljan	Isto kao kod „SMB signing disabled (cifs-smb-signing-disabled)“ ranjivosti
10.	CIFS NULL Session Permitted (cifs-nt-0001)	NULL sesije omogućavaju anonimnim korisnicima da kreiraju CIFS sesije bez autentifikacije sa Windows-om ili third-party CIFS implementacijom kao što su Samba ili Solaris CIFS Server.. Ovi anonimni korisnici bi mogli biti u mogućnosti da prebroje lokalne korisnike, grupe, servere, deljene resurse, domene, polise domena, a mogli bi biti u	BID: 494[584] CVE: CVE-1999-0519[585] MSKB: 143474[586] URL1[587]	Kritičan	Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.2 pod primerom Null session ranjivost.

[569] http://support.microsoft.com/default.aspx?scid=kb;EN-US;2508429
[570] http://download.Windowsupdate.com/msdownload/update/software/secu/2011/03/Windowsxp-kb2508429-x86-enu_e0b40d81f2ecc1bad43439a6bd0a9e2a0ab7dd56.exe
[571] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1314
[572] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-1315
[573] http://technet.microsoft.com/en-us/security/bulletin/ms06-035
[574] http://support.microsoft.com/default.aspx?scid=kb;EN-US;917159
[575] http://www.sans.org/critical-security-controls/#w4
[576] http://www.sans.org/critical-security-controls/#s2
[577] http://secunia.com/advisories/21007/
[578] http://xforce.iss.net/xforce/xfdb/26818
[579] http://xforce.iss.net/xforce/xfdb/26820
[580] http://www.download.Windowsupdate.com/msdownload/update/v3-19990518/cabpool/Windowsxp-kb917159-x86-enu_5ed838e18ceae61a8d94f8c4be2462a8e19212d7.exe
[581] http://support.microsoft.com/default.aspx?scid=kb;EN-US;887429
[582] http://blogs.technet.com/b/josebda/archive/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2.aspx
[583] http://support.microsoft.com/kb/887429
[584] http://www.securityfocus.com/bid/494
[585] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519
[586] http://support.microsoft.com/default.aspx?scid=kb;EN-US;143474
[587] http://www.hsc.fr/ressources/presentations/null_sessions/

		mogućnosti i da pristupe različitim MSRPC servisima preko poziva udaljenih procedura (RPC). Ovi servisi su i u prošlosti bili skloni ranjivostima. Mnoštvo informacija koje napadačima postaju dostupne preko NULL sesija mogu im omogućiti da sprovedu i mnogo prefinjenije napade.			
11.	ICMP timestamp response (generic-icmp-timestamp)	Udaljeni host je odgovorio na ICMP-ov zahtev za vremenski pečat. Odgovor na ICMP-om zahtev za vremenski pečat sadrži datum i vreme udaljenog host-a. Teoretski, ova informacija bi mogla biti iskorišćena protiv nekih sistema da eksploatiše slabe time-based generatore slučajnih brojeva na drugim serverima. Dodatno, verzije nekih operativnih sistema mogu precizno biti detektovane pomoću analize njihovih odgovora na nevažeći ICMP-ov zahtev za vremenski pečat.	CVE: CVE-1999-0524[588] XF: icmp-netmask(306)[589] XF: icmp-timestamp(322)[590]	Umeren	Onemogućavanje ICMP timestamps odgovora vrši se deselektovanjem „allow incoming timestamp request“ opcije u okviru ICMP konfiguracionog panela Windows fajervola. Rešavanje ove ranjivosti detaljno je opisano u poglavlju 4.1.1 (Opšte ranjivosti) pod primerom ICMP ranjivost

Potrebno je istaći da se nakon prikupljenih informacija o ranjivostima na sistemu izračunavaju tzv. bodovi ranjivosti „Vulnerability risk scores“. Oni predstavljaju vrednost koja se izračunava na osnovu verovatnoće napada i uticaja (koji se množe sa brojem ugroženih slučajeva), zasnovano na CVSS (Common Vulnerability Scoring System)[591] metrici. Prikaz i izračunavanje ovih bodova prevazilaze okvire ovog rada. Sa stanovišta bezbednosti prikazani rezultati mogu biti od velike pomoći u pronalaženju najslabije karike na operativnim sistemima, pre nego što je iskoristi zlonamerni napadač, a sa stanovišta digitalne forenzike dobijaju se značajni podaci koji se mogu staviti u kontekst forenzičke istrage.

[588] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524
[589] http://xforce.iss.net/xforce/xfdb/306
[590] http://xforce.iss.net/xforce/xfdb/322
[591] http://nvd.nist.gov/CVSS.aspx

ZAKLJUČAK

Značaj i razvoj novih tehnologija za modernizaciju poslovanja i transfera podataka je u stalnom porastu. Nažalost, istovremeno se šire i protivpravne aktivnosti. Problem računarskog kriminala je kompleksan fenomen. S obzirom da počinioci tih dela imaju potrebna znanja i koriste sofisticirane tehnike za njihovo izvršenje, sve im je teže ući u trag i nesumnjivo dokazati elemente krivičnog dela. Digitalna forenzika je nauka koja jedinstveno kombinuje informatičke discipline sa pravnom regulativom. Prirodna tendencija prava ka konzervativizmu često dolazi u sukob sa životom, s obzirom na njegovu dinamičnost. Brzina takvih promena naročito se ogleda u informatičkoj nauci i tehnologiji koje su predmet stalnih inovacija i promena. Na primer, napredak u dizajnu operativnog sistema i hardvera prati i napredak upotrebe novih zlonamernih tehnika i alata, što postavlja pred digitalnu forenziku veliki izazov, jer prevashodno mora da drži korak sa stalnim promenama.

Da bi se zaustavilo moguće širenje računarskog kriminala, u zvaničnoj istrazi neophodno je uspostaviti multidisciplinarne timove za istragu, koji se sastoje od digitalnog forenzičara, pripadnika organa unutrašnjih poslova i tužilaštva. Za dokazivanje elemenata ovih specifičnih dela, njihovih izvršioca i uzročno-posledičnih veza, neophodno je nesumnjivo i sa preciznošću detektovati napad na računarski sistem, sprovesti adekvatne istražne radnje, analizirati način, vreme izvršenja i obim štete pomoću tehnika i alata digitalne forenzike i uspešno procesuirati ta dela u domaćem pravnom sistemu. U svemu tome najznačajniji doprinos ima upravo digitalna forenzika kao naučna disciplina koja daje precizne odgovore na pitanja koja se postavljaju kako u rešavanju problema izazvanih računarskim kriminalom tako i u postupku preventivne zaštite računarske mreže i sistema.

Digitalni podaci u računarskom sistemu i mreži, a naročito na Internetu veoma su osetljivi na potencijalne zloupotrebe. Digitalna forenzička istraga, digitalni dokazi, njihovo prikupljanje i analiza na forenzički ispravan način, detaljno su opisani u radu u okviru drugog poglavlja. Motiv visokotehnoloških kriminalaca najčešće je u materijalnim ili ređe nematerijalnim dobitima i da uz pomoć najnovijih metoda i malicioznih programa prikrivaju svoje prisustvo na računarskom sistemu. Tragovi kompromitovanja računarskog sistema upravo se otkrivaju forenzičkim alatima, razmatranim u okviru ovog rada. Treće poglavlje analizira forenzičke metode, alate i njihovu primenu sa ciljem pronalaženja dokaza prihvatljivih na sudu i usaglašenim sa zakonom. Detaljno su opisani značaj, načini i ograničenja prikupljanja postojanih i brzo promenljivih podataka na Windows i Linux platformama. U radu je dat prikaz softverskih forenzičkih alata za inicijalni odgovor, pojedinačnih alata za oporavak podataka i particija i prikaz forenzičkih kompleta alata koji mogu realizovati više elemenata forenzičkog procesa.

Potvrđene su opšta i radna hipoteza, postavljene u prvom poglavlju rada u metodologiji naučnog istraživanja.

Jedan od ciljeva istraživanja jeste da se prikaže gde i kako se mogu pronaći digitalni dokazi koji potvrđuju protivpravnu aktivnost koja se realno može dogoditi, a koja je u vezi sa računarskim sistemom. U četvrtom poglavlju prikazani su primeri najčešćih ranjivosti na Windows i Linux sistemima i načini zlonamernog iskorišćavanja sistema koji su otkriveni kroz procese forenzičke istrage i analize. Cilj eksperimentalnog istraživanja prikazanog u četvrtom poglavlju jeste dvostruk. Sa jedne stane, prikazani su ranjivi servisi koji mogu ugroziti bezbednost sistema, a sa druge strane predložene su adekvatne mere proaktivne zaštite. Kada je reč o zaštiti, treba napomenuti da ne postoji jedinstvena tehnologija - srebrni metak koji može rešiti sve bezbednosne probleme u organizaciji. Ukoliko se u životu želi

postići određeni cilj, mora se naporno raditi uz mnogo odricanja. U tom smislu ni postizanje maksimalne zaštite nije izuzetak. Realizovanje prihvatljivog nivoa bezbednosti u organizaciji zavisi od uloženih resursa. Većom upotrebom proceduralnih i tehničkih zaštitinih mera, povećava se zaštita sistema, a time i nivo bezbednosti u celoj organizaciji. U eksperimentalnoj verifikaciji rada izvršeno je skeniranje ranjivosti Windows i Linux operativnih sistema sa alatom *Rapid 7 Nexpose*. Na taj način su prezentovane, ranjivosti difoltno instaliranih Windows i Linux operativnih sistema (poglavlje 4.3 i poseban prilog na disku) sa ciljem ukazivanja na potencijalne bezbednosne ranjivosti, kao i na adekvatne preventivne mere zaštite sistema. Potvrđeno je da nakon difoltnih instalacija nijedan računarski sistem nije bez ranjivosti. Prezentovan je i uporedni prikaz pronađenih ranjivosti na Linux i Windows operativnim sistemima. Kod Linux operativnih sistema nakon dodavanih servisa očekivano je znatno povećan broj kritičnih, ozbiljnih i umerenih ranjivosti na sistemu. Značajan podatak je da je povećani broj kritičnih ranjivosti i dalje manji od kritičnih ranjivosti na Windows operativnim sistemima, difoltno instaliranim bez dodavanih servisa.

Rezultati skeniranja, svih operativnih sistema, tabelarno su prikazani i izdvojeni su u poseban prilog rada, na disku. Ukupan broj skeniranih sistema jeste 80. Windows operativni sistemi (ukupno 51) grupisani su u 16 tabela prema familiji kojoj pripadaju i podudarajućim ranjivostima. Linux operativni sistemi (ukupno 29) grupisani su u 11 tabela prema familiji kojoj pripadaju i podudarajućim ranjivostima. S obzirom da je skeniranje vršeno tokom dve godine, to čini ukupno 54 tabele. U tabelama su opisane pronađene ranjivosti, utvrđen je njihov broj, dati su relevantni izvori koji ukazuju na ranjivost, zajedno sa odrednicom značajnosti i data je preporuka za rešavanje pronađene ranjivosti. Na taj način su detektovane ranjivosti na sistemu i predložene su mere za prevazilaženje ovih bezbednosnih problema, čime se preventivno deluje protiv mogućeg forenzički relevatnog događaja. U tom smislu, ovo sveobuhvatno istraživanje se može posmatrati i kao proaktivna digitalna forenzika u smislu spremnog dočekivanja, ali i otkrivanja i logovanja forenzički relevatnog događaja.

Pravilnom i redovnom upotrebom alata sa kojima se vrše skeniranja i logovanja ranjivosti na sistemima, uz prisustvo forenzičkog stručnjaka, moguće je dobiti detaljan uvid u nezakonite procese u sistemu i sprečiti da se dogode dalje protivpravne aktivnosti u okviru mreže ili određenog računarskog sistema. Integrisanjem rezultata proaktivne digitalne forenzike zajedno sa sistemima preventivne zaštite, detekcije i analize ranjivosti, kao i primenom višeslojne arhitekture zaštite [103] uz pravovremeni odgovor na incidentne, odnosno protivpravne aktivnosti (sa digitalnim foenzičarem), moguće je povećati bezbednost sistema i ostvariti optimalan nivo zaštite adekvatan definisanoj bezbednosnoj politici.

Konačno, ovaj rad je obezbedio koncizan, ali dovoljno detaljan opis najznačajnijih aktuelnih kretanja iz digitalne forenzike i njene implikacije za više različitih oblasti - informatičke nauke, pravne nauke, bezbednost i kriminologiju. Vrlo je verovatno da će ovaj rad biti izuzetno primenljiv i koristan resurs istraživačima, studentima iz ovih oblasti, društveno-pravnim stručnjacima i stručnjacima iz krivičnog pravosuđa. S obzirom da ova tematika pokriva tehnologije i forenzičke alate sa brojnim primerima primene u praksi (na terenu i u laboratorijama), to će biti od interesa i za pravosudne organe i za profesionalce koji rade kao stručnjaci za digitalnu forenziku računarskih sistema.

LITERATURA

[1] Aaron P., Cowen D., Davis. C., *Hacking Exposed Computer Forensics, Second Edition*, The Mcgraw-Hill Companies, 2010.

[2] Acunetix Ltd., *Acunetix Web Vulnerability Scanner, Manual v. 4.0*, Acunetix Ltd, 2006. Izvor: http://www.acunetix.com/vulnerability-scanner

[3] Ahmad D., Dubrawsky I., Flynn H., Grand J., Graham R., Johnson N. L., Kaminsky D., Lynch F. W., Manzuik S. W., Permeh R., Pfeil K., Russell R., *Hack Proofing Your Network, Second Edition*, Syngress Publishing, Inc, Rockland, MA, 2002.

[4] Alghafli K. A., Jones A., Martin T. A., *Forensic Analysis of the Windows 7 Registry*, Khalifa University of Science, Technology and Research, 2010.

[5] Allen B., *Collecting Digital Evidence from Intrusion Detection System*, CGS 5132 - Computer Forensics II, 2002. Izvor : http://www.authorstream.com/Presentation/Kliment-24060-allen-Collecting-Digital-Evidence-Intrusion-Detection-Systems-designed-forensic-use-as-Entertainment-ppt-powerpoint/

[6] Altheide C., Carvey H., *Digital Forensics with Open Source tools*, Elsevier, Waltham USA, 2011.

[7] Ansonand S., Bunting S., *Mastering Windows Network Forensics and Investigation*, Sybex, 2007.

[8] APWG, *Phishing Activity Trends Report, 3rd Quarter (July – September 2012)*, 2013. Izvor : http://www.apwg.org/download/document/84/apwg_trends_report_q3_2012.pdf

[9] Ashcroft J., Electronic Crime Scene Investigation - A Guide for First Responders, U.S. Department of Justice, 2001. Izvor : https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[10] Aycock J., *Computer Viruses, and Malware* , Springer , Canada, 2006.

[11] Baker S., Green P., Meyer T., Cochrane G., *Checking Microsoft Windows Systems for Signs of Compromise version 1.3.4*, 2005. Izvor: http://www.oucs.ox.ac.uk/network/security/documents/win_intrusion.pdf

[12] Banjeglav T., Dimitrijević N., *Istraga aktivnog kompjuterskog incidenta*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2004. Izvor : http://www.itvestak.org.rs/ziteh_04/radovi/ziteh-02.pdf

[13] Barrett D., Kipper G., *Virtualization and Forensics – A digital forensic Investigator's guide to Virtual Environments*, Elsevier Inc., USA, 2010.

[14] Beebe N. L., Clark J. G., *A hierarchical, objective-based framework for the digital investigations process*, In Proceedings of the 2005 Digital Forensics Research Workshop, pp. 146-166, 2005.

[15] Beek C., *Virtual Forensics*, TenICT proffesionals, 2010. Izvor:

http://securitybananas.com/wp-content/uploads/2010/04/Virtual-Forensics_BlackHatEurope2010_CB.pdf, 16.02.2012

[16] Bem D., Huebner E., *Computer Forensic Analysis in a Virtual Environment*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2, 2007.

[17] Bergadano F., Gunetti D., Picardi C., *User Authentication through Keystroke Dynamics*, ACM Transactions on Information and System Security, Vol. 5, No. 4, pp. 367-397, November 2002.

[18] Bradford P. G., Hu N., *A Layered Approach to Insider Threat Detection and Proactive Forensics*, 21st Annual Computer Security Applications Conference, Applied Computer Security Associates (ACSA), 2005. Izvor: http://www.acsac.org/2005/techblitz/hu.pdf

[19] Brown C., *Computer Evidence - Collection and Preservation*, Thomson Delmar Learning, Charles River Media, Inc, Hingham, Massachusetts, pp. 213-218, 2006.

[20] Bunting S., Wei W., *EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide*, Indianapolis, IN: Wiley Publishing, 2006.

[21] Burdach M., *Detecting Rootkits And Kernel-level Compromises In Linux*, Symantec, Novembar 2004. Izvor: http://www.symantec.com/connect/articles/detecting-rootkits-and-kernel-level-compromises-Linux)

[22] Burdach M., *Forensic Analysis of a Live Linux System, Pt. 2*, Symantec, April 2004. Izvor: http://www.symantec.com/connect/articles/forensic-analysis-live-Linux-system-pt-2

[23] Caloyannides M. A., *Privacy Protection and Computer Forensics Second Edition*, Artech ouse Inc., 2004.

[24] Carrier B., *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers*, International Journal of Digital Evidence, Winter 2003.

[25] Carrier B., *File System Forensic Analysis*, Addison Wesley Professional, 2005.

[26] Carrier B., *Open Source Digital Forensics Tools - The Legal Argument*, @tstake, 2002. Izvor : http://www.digital-evidence.org/papers/opensrc_legal.pdf

[27] Carrier B., Spafford H. E., *Getting Physical with the Digital Investigation Process*, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2, 2003.

[28] Carroll O. L., Brannon S. K., Song T., *Vista and BitLocker and Forensics! Oh My!*, Computer Forensics, Volume 56 Number 1, January 2008.

[29] Carvey H., Altheide C., *Tracking USB storage: Analysis of Windows artifacts generated by USB storage devices*, Digital Investigation 2, pp. 94-100, Elsevier Academic Press, Burlington, MA 2005. Izvor: http://www.sciencedirect.com/science/article/pii/S1742287605000320/pdfft?md5=b4d986c553c49a983e66ae2b68a0c4a6&pid=1-s2.0-S1742287605000320-main.pdf

[30] Carvey H., *Pearl scripting Live Response, Forensic Analysis, and Monitoring*, Syngress Publishing, Inc 2007.

[31] Carvey H., *Windows Forensic Analysis DVD Toolkit 2E*, Elsevier, Inc. 2009.

[32] Carvey H., *Windows Forensic Analysis DVD Toolkit*, Elsevier, Inc. 2007.

[33] Carvey H., *Windows Forensics and Incident Recovery***,** Addison Wesley, 2004.

[34] Casey E., *Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet*, Second Edition, Academic Press 2004.

[35] Casey E., *Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet*, third Edition, Elsevier Academic Press, 2011.

[36] Casey E., *Digital Evidence and Computer crime*, Academic press, San Diego 2000.

[37] Casey E., *Handbook of Digital forensics and investigation*, Elsevier Academic Press, Burlington, 2010.

[38] Chad Steel, Windows Forensics: The Field Guide for Corporate Computer Investigations, John Wiley & Sons 2006.

[39] Chaouchi H., Laurent-Maknavicius M., *Wireless and Mobile Network Security, Security Basics, Security in On-the-shelfand Emerging Technologies*, ISTE Ltd and John Wiley & Sons, Inc. USA, 2009.

[40] Ciardhuáin O. S., *An Extended Model of Cybercrime Investigations*, International Journal of Digital Evidence. Summer 2004, Volume 3, Issue1, 2004. Izvor: https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

[41] Citrix, *Citrix Xenserver*, Izvor : http://www.citrix.com/English/ps2/products/product.asp?contentID=683148

[42] Clarke N., *Computer Forensics A Pocket Guide*, IT Governance Publishing, United Kingdom, 2010.

[43] Cole E., *Hackers Beware*, New Riders Publishing, 2002 .

[44] Communication from the Commission to the Council, The European Parliament, The Economic and Social Committee and Committee of the regions, *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer- related Crime*, 2012. Izvor : http://europa.eu.int

[45] Computer Crime and Intellectual Property Section Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, United States Department of Justice, 2002. Izvor : http://www.justice.gov/criminal/cybercrime/searching.html

[46] Convention on cybercrime, Council of Europe, Budapest novembar 2001, Izvor : http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

[47] Council of Europe, Recommendation No. R (95) 13, Izvor : http://www.justice.gov/criminal/cybercrime/crycoe.htm

[48] Cross M., *Scene of the Cybercrime*, Second Edition, syngress, 2008.

[49] Danchev D., *Building and implementing a successful information security policy*, 2003. Izvor : http://www.Windowsecurity.com/pages/security-policy.pdf

[50] Dart K. A., *Deleted Files Can Be Recovered*, February 24, 2008. Izvor :

http://www.akdart.com/priv9.html

[51] Davidovac Z., Korać V., *Vulnerability management and patching it systems*, Arheologija i prirodne nauke, br. 6, pp. 129-144, 2011.

[52] Davis N., *Live Memory Acquisition for Windows Operating System : Tools and Techniques for analyses*, Eastern Michigan University, 2008. Izvor : http://www.emich.edu/ia/pdf/research/Live%20Memory%20Acquisition%20for%20Windows%20Operating%20Systems,%20Naja%20Davis.pdf

[53] Digital Forensics Research Workshop, *A road map for digital forensics research*, Technical report, Digital Forensics Research Workshop, 2001.

[54] Drakulić M., Drakulić R., *Cyber kriminal*, Fakultet organizacionih nauka u Beogradu, ttp://www.bos.rs/cepit/idrustvo/sk/ cyberkriminal.pdf

[55] Drakulić M., Drakulić R., *Cyber kriminal*, Prezentacija, Fon 2011. Izvor: http://www.google.rs/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDMQFjAA&url=http%3A%2F%2Fposlis.fon.bg.ac.rs%2Findex.php%3Foption%3Dcom_docman%26task%3Ddoc_download%26gid%3D295%26Itemid%3D14&ei=QjttUfLgIsnkswawmoDIDg&usg=AFQjCNGqrlDyeh9PUTyZ42pif5r8eyS11Q&bvm=bv.45175338,d.Yms&cad=rja

[56] Ec-Council Press, *Computer Forensics: Investigating Data and Image files*, Course Technology Cengage learning, USA, 2010.

[57] Ec-Council Press, *Computer Forensics: Investigating hard disks, file and operating systems*, Course Technology Cengage learning, USA, 2010.

[58] Ec-Council Press, *Computer Forensics: Investigation procedures and response*, Course Technology Cengage learning, USA, 2010.

[59] Ec-Council Press, *Investigating Network Intrusions and Cybercrime*, Course Technology Cengage learning, USA, 2010.

[60] Farmer D. J., *A Windows Registry Quick Reference. eptuners.com*, October 2007. Izvor : http://www.eptuners.com/forensics/A%20Windows%20Registry%20Quick%20Reference.pdf

[61] Farmer D., Venema W., *Forensic discovery*, Pearson Education Inc, Crawfordsville, 2008.

[62] Fogie S., *VOOM vs The Virus (CIH)*, 2004. Izvor: http://voomtech.com/downloads/Shadow%20Eval%20-%20Fogie.pdf

[63] Forensics science communications, *Digital Evidence : Standards and Principles*, Scientific Working Group on Digital Evidence (SWGDE) International Organization on Digital Evidence (IOCE), Volume 2 - Number 2, April 2000. Izvor: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/

[64] Foster M., Wilson J. N., *Process Forensics: A Pilot Study on the Use of Checkpointing Technology in Computer Forensics*, International Journal of Digital Evidence, Volume 3, Issue 1, 2004.

[65] Frank Adelstein, *Live forensics: Diagnosing your system without killing it first*, Communications of the ACM, , 49(2) pp. 63–66, 2006.

[66] Friedman C.S., *This Alien Shore*, Daw Books INC., New York 1998. Izvor http://rose.digitalmidnight.org/temp/books/CS_Friedman/C.%20S.%20Friedman%20-%20This%20Alien%20Shore.pdf

[67] Garfinkel S., *Anti-Forensics: Techniques, Detection And Countermeasures*, In Proceedings Of The 2nd International Conference On I-Warfare And Security (Iciw), Naval Postgraduate School, Monterey, Ca, March 8-9, 2007.

[68] Garfinkel S., Malan D., Dubec K., Stevens C., Pham C., *Disk imaging with the advanced forensics format, library and tools*, The second Annual IFIP WG 11.9 International Conference on Digital Forensics, National Center for Forensic Science, Orlando, Florida, USA, January 20-February 1, 2006.

[69] Garfinkel S., *The Advanced Forensic Format 1.0*., 2005.
Izvor: http://stuff.mit.edu/afs/sipb/user/simsong/afflib/affdoc.doc, 13.02.2012.

[70] Georgijević U., *Integrisani model procesa digitalne forenzičke istrage*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2006.
Izvor : http://www.itvestak.org.rs/ziteh_06/Radovi/ZITEH%2006-R07.pdf

[71] Georgijević U., *Istražne metodologije, tehnike i alati za digitalnu forenzičku istragu*, master rad, Fakultet za informatiku i menadžment, Univerzitet Singidunum 2010.

[72] Grubor G., Franc I., *Evolucija Modela Digitalne Forenzicke Istrage*, ZITEH - Udruženje sudskih veštaka za informacione tehnologije IT veštak, 2010. Izvor : http://www.singipedia.com/attachment.php?attachmentid=1019&d=1278675669

[73] Grubor G., *Funkcionalni model istrage kompjuterskog događaja*, Udruženje IT Veštak, 2004.

[74] Grubor G., *Funkcionalni model istrage kompjuterskog kriminala*, Ziteh 2010.

[75] Grubor G., Galetin A., *Digitalna forenzička istraga u korporacijskoj zaštiti informacija*, Singidunum Revija, 2010.

[76] Grubor G., Gotić A., *Korporativna aktivna digitalna forenzička istraga primenom Backtrack – a*, 10. Međunarodni naučni skup Sinergija 2012. Univerzitet Sinergija, 2012.

[77] Harms K., *Forensic Analysis of System Restore Points in Microsoft Windows XP*, Mandiant Corporation, 2006. Izvor:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.84.4474&rep=rep1&type=pdf

[78] Harris R., Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem, Journal Digital Investigation: The International Journal of Digital Forensics & Incident Response, vol. 3, pp. 44-49, 2006.

[79] Harrison W., Heuston G., Morrissey M., Aucsmith D. Mocas S., Russelle S., *A Lessons Learned Repository for Computer Forensics*, International Journal of Digital Evidence, Vol. 1 No. 3, 2002.
Izvor : http://www.ijde.org/docs/02_fall_art2.html

[80] Haruyama T., Suzuki H., *One-byte Modification for Breaking Memory Forensic Analysis*, BlackHat Europe, Mart 2012.

[81] Hauck V. R., Atabakhsh H., Ongvasith P., Gupta H., Chen, H., *Using Coplink to analyze criminal-justice data*, IEEE Computer, Vol. 35 No. 3 pp. 30–37, 2002.

[82] Hay B. Nance K.**,** *Forensics Examination of Volatile System Data Using Virtual Introspection***,** SIGOPS Operating Systems Review , Volume 42 Issue 3, ACM, pp. 74–82., 2008.

[83] Hay B., Bishop M., Nance K., *Live Analysis: Progress and Challenges*, IEEE Security and Privacy, vol. 7, pp. 30-37., Mart 2009.
Izvor : http://nob.cs.ucdavis.edu/bishop/papers/2009-ieeesp-2/liveanal.pdf

[84] Home page The United States Department of Justice, *Reporting Computer related crime.* Izvor: http://www.justice.gov/criminal/cybercrime/intl.html

[85] Huebner E., Bem D., Wee K. C., *Data hiding in the NTFS file system*, Digital Investigation 3, Elsevier, October 2006. Izvor : ftp://163.13.201.222/Prof_Liang/%E6%95%B8%E4%BD%8D%E9%91%91%E8%AD%98/Volume%203%20%282006%29/Supplement%201/Issue%204/Pages%20211-226.pdf

[86] Ivaniš N., *Digitalna forenzicka istraga u virtuelnom okruženju*, master rad, Univerzitet Singidunum 2011.

[87] Jakobsson M., Ramzan Z., *Crimeware: Understanding New Attacks and Defenses*, Addison Wesley Professional, 2008.

[88] Johnson T. A., *Forensic Computer Crime Investigation*, Taylor & Francis Group, LLC, 2005.

[89] Jones R., *Internet Forensics***,** O'Reilly Media, 2005.

[90] Kanellis P., Kiountouzis E., Kolokotronis N., Martakos D., *Digital Crime and Forensic Science in Cyberspace*, Idea Group Inc, pp. 217-242, 2006.

[91] Kaufman R. J., *Computer Incident Response*, Texas Security Symposium Agenda, San Antonio TX, 2003.

[92] Kaufman R. J., *Intrusion Detection and Incident Response IS 3523 course*,UTSA Spring, 2012.

[93] Keith J. J., Bejtlich R., Curtis W. R., *Real Digital Forensics Computer Security and Incident Response*, Addison-Wesley, 2006.

[94] Keith J. J., *Forensic Analysis of Internet Explorer Activity Files*, Foundstone.com, Mart 2003.

[95] Keith J. J., *Forensic Analysis of Microsoft Windows Recycle Bin Records*, Foundstone.com, April 2003.

[96] Kent K., Chevalier S., Grance T., Dang H., *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930, August 2006.

[97] Kipper G., *Wireless crime and forensic investigation*, Auerbach Publications Taylor & Francis Group, 2007.

[98] Klevinsky T. J., Laliberte S., Gupta A., *Hack I.T.: Security Through Penetration Testing*, Addison Wesley, 2002.

[99] Kohn M., Eloff J., Olivier M., *Framework for Digital Forensic Investigation: Information and Computer Security Architectures Research Group (ICSA)*, University of Pretoria, 2006. Izvor : http://mo.co.za/open/dfframe.pdf

[100] Kopecký K., *Cyber grooming danger of cyberspace*, study, Olomouc, 2010.

[101] Kopecký K., *Stalking a kyberstalking nebezpečné pronásledování*, study Olomouc, 2010. Izvor: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd

[102] Korać V., *Digital archaeology in a virtual environment*", Arheologija i prirodne nauke, br. 8, str. 129-141, Beograd 2013.

[103] Korać V., *Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja*, Arheologija i prirodne nauke, specijalna izdanja, Centar za nove tehnologije, 2010.

[104] Korać V., *Prevencija širenja virusa kroz autorun funkciju operativnog sistema*, Arheologija i prirodne nauke br.4, pp. 103-107, Beograd 2008.

[105] Korać V., *Zaštita usb prenosnog drajva i operativnog sistema od zlonamernog koda tipa autorun.inf*, Zbornik Radova - Forum BISEC 2010, II konferencija o bezbednosti, pp. 77-82, Univezitet Metropolitan, Fakultet informacionih tehnologija, 2010.

[106] Kornblum J. D., *Exploiting the Rootkit Paradox with Windows Memory Analysis*, International Journal of Digital Evidence Fall 2006, Volume 5, Issue 1, 2006

[107] Kornblum J. D., *The Linux Kernel and the Forensic Acquisition of Hard Disks with an Odd Number of Sectors*, International Journal of Digital Evidence, Volume 3, Issue 2, 2004.

[108] Kruse II G. W., Heiser G. J., *Computer Forensics Incidend response essentials*, 14th printing, New York: Addison Wesley, March 2010.

[109] Kunz M., Wilson P., *Computer Crime and Computer Fraud - Report to the Montgomery County Criminal Justice Coordinating Commission*, University of Maryland Department of Criminology and Criminal Justice, USA, 2004.

[110] Lee H., Palmbach T., Miller M., *Henry Lee's Crime Scene Handbook*, San Diego: Academic Press, 2001.

[111] Leschke T. R., "*Cyber Dumpster Diving: $Recycle Bin Forensics for Windows 7 and Windows Vista*", U.S. Department of Defense Cyber Crime Conference, 2010.

[112] Leschke T. R., *Shadow Volume Trash: $Recycle.Bin Forensics for Windows 7 and Windows Vista Shadow Volumes*, U.S. Department of Defense Cyber Crime Institute, 2010.

[113] Ligh M. H., Adair S., Hartstein B., Richard M., *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*, Wiley Publishing, Inc., Indianapolis, Indiana, 2011.

[114] Lillard T. V., *Digital forensics for network, Internet, and cloud computing - A forensic evidence guide for moving targets and data*, Elsevier Inc, USA, 2010.

[115] Malin C. H., Casey E., Aquilina J. M., *Malware Forensics - Investigating and Analyzing Malicious Code*, Syngress 2008.

[116] Manzuik S., Gold A., Gatford C., *Network Security Assessment: From Vulnerability to Patch*, Syngress Publishing, Inc., 2007.

[117] Maras M., *Computer forensics, cybercriminals, laws and evidence*, Jones &Bartlett learning, USA 2012

[118] Marcella A. J., Greenfield S. R., *Cyber Forensics*, CRC Press LLC, 2002.

[119] Marchany R., *The top 10/20 Internet security vulenrabilities*, Va Tech Computing center, The Sans institute, Covits, 2000. Izvor : http://www.slideshare.net/amiable_indian/the-top-1020-internet-security-vulnerabilities-a-primer

[120] Marković S., *Digitalna forenzika Linux fajl sistema*, master rad, Univerzitet Univerzitet Singidunum, 2010.

[121] Marshall A. M., *Digital Forensics - Digital Evidence in Criminal Investigation*, JohnWiley & Sons, Ltd 2008.

[122] Matijašević J., Ignjatijević S., *Kompjuterski kriminalitet u pravnoj teoriji, pojam, karakteristike, posledice*, Infoteh-Jahorina Vol. 9, Ref. E-VI-8, pp. 852-856, March 2010.

[123] McDougal M., *Windows Forensic Toolchest (WFT)*, 2005. Izvor: http://www.foolmoon.net/security/

[124] McQuade III S. C., *Encyclopedia of Cybercrime*, Greenwood Publishing Westport, Connecticut, 2009.

[125] McRee R., *Memory Analysis with DumpIt and Volatility*, ISSA Journal, September 2011.

[126] Menz M., Bress S., *The fallacy of software write protection in computer forensic, 2004.* Izvor: http://www.mykeytech.com/SoftwareWriteBlocking2-4.pdf

[127] Michaud, D. J., *Adventures in Computer Forensics*, Information Security Reading Room, SANS Institute 2001. Izvor : https://www.sans.org/reading-room/whitepapers/incident/adventures-computer-forensics-638

[128] Microsoft, *Microsoft Hyper-V*, Izvor: http://www.microsoft.com/en-us/server-cloud/hyper-v-server/ , *Pristupljeno 09.02.2012*

[129] Milanović Z., Milanović T., *Digitalna anti-forenzika kao kriminogeno sredstvo zaštite kiber kriminala*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.

[130] Milosavljević M., Grubor G., *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd 2009.

[131] Milosavljević M., Grubor G., *Digitalna forenzika*, Univerzitet Singidunum, Beograd, 2008.

[132] Milosavljević M., Grubor G., *Istraga kompjuterskog kriminala - metodološko tehnološke osnove,* Univerzitet Singidunum 2009.

[133] Mohay G., Anderson A., Collie B., Vel O., McKemmish R., *Computer and Intrusion Forensics*, Artech House, Norwood, MA, 2003.

[134] Mrdović S., Huseinović A., Zajko W., *Combining Static and Live Digital Forensic Analysis in Virtual Environment*, Information, Communication and Automation Technologies, ICAT 2009, XXII International Symposium, 2009. Izvor : http://people.etf.unsa.ba/~smrdovic/publications/ICAT2009-Mrdovic_Huseinovic_Zajko.pdf

[135] National Institute of Justice, *Electronic Crime Scene Investigation. A Guide for First Responder,* 2001. Izvor: https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[136] National Institute of Standards and Technology, *Secure Hash Standard*, FIPS PUB 180, May 1993.

[137] National Policing Improvement Agency, *Core Skills in Data Recovery & AnalysisCourse Reference Book V2.01*, Bradford, UK, maj 2007.

[138] Nelson B., Phillips A., Enfinger F., Steuart C., *Guide To Computer Forensics And Investigations, second edition*, Thomson Course Technology, Boston, 2006.

[139] Nelson B., Phillips A., Enfinger F., Steuart C., *Guide to Computer Forensics and Investigations, third edition,* Thomson Course Technology, Boston, 2008.

[140] Nelson B., Phillips A., Steuart C., *Guide to Computer Forensics and Investigations – fourth edition, Fourth Edition*, Course Technology, Cengage learning, Boston, 2010.

[141] Nestler V., Conklin W. A., White G., Hirsch M., *Principles of Computer Security: CompTIA Security and Beyond Lab Manual, Second Edition*, The McGraw-Hill Companies 2011.

[142] Newsham T., Palmer C., Stamos A., *Breaking Forensics Software: Weaknesses in Critical Evidence Collection*, BlackHat Conference 2007. Izvor : http://www.defcon.org/images/defcon-15/dc15-presentations/Palmer_and_Stamos/Whitepaper/dc-15-palmer_stamos-WP.pdf

[143] Nikačević V., *Korporacijska istraga kompjuterskog kriminala sa implementacijom sigurnosne politike,* Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2010.

[144] Nikolić K. L., *Suzbijanje visokotehnološkog kriminala*, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd 2010.

[145] Nolan R., Baker M., Branson J., Hammerstein J., Rush K., Waits C., Schweinsberg E., *First Responders Guide to Computer Forensics: Advanced Topics*, Software Engeneering Institute Carnegie Mellon, 2005.

[146] Nolan R., Sullivan C. O., Branson J., Waits C., *First Responders Guide to Computer Forensics*, CERT Training and Education, Carnegie Mellon University, March 2005

[147] One A., *Smashing the Stack for Fun and Profit, Phrack, Volume 7, Issue 49, 1996.*

[148] Pleskonjić D., Maček N., Đorđević B., Carić M., *Sigurnost računarskih sistema i mreža*, Mikro knjiga, Beograd, 2007.

[149] Pogue C., Altheide C., Haverkos T., *UNIX and Linux Forensic Analysis DVD Toolkit*, Syngress publishing Inc., 2008.

[150] Popek J. G., Goldberg P. R., *Formal requirements for virtualizable third generation architectures,* Communications of the ACM 17 (7), pp. 412–421. 1974.

[151] Prlja D., Reljanović M., *Pravna informatika*, Pravni fakultet Univerziteta Union, Beograd, 2010.

[152] Prlja D., Reljanović M., *Visokotehnološki kriminal - uporedna iskustva*, Strani pravni život, br. 3/2009, pp. 161-184., 2009.

[153] Prlja D., *Sajberkriminal*, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, 28.12.2008: http//www.prlja.info/sk2008.pdf

[154] Prlja D., Savović M., *E-mail kao dokazno sredstvo u uporednom pravu*, Strani pravni život, br. 2/2009, pp. 71-85., 2009.

[155] Prosise C. Mandia K, *Incident response and computer forensics,* second edition, The McGraw-Hill Companies 2003.

[156] Prosise C. Mandia K., *Incident Response: Investigating Computer Crime*, McGrawHill Osborne Media, 2001.

[157] Qemu, *Qemu open source processor emulator*, http://wiki.qemu.org/Main_Page , Pristupljeno 09.02.2012

[158] Ray A. D., Bradford G. P., *Models of Models: Digital Forensics and Domain-Specific Languages* (Extended Abstract), 2008. Izvor: http://www.ioc.ornl.gov/csiirw/07/abstracts/Bradford-Abstract.pdf

[159] Reith M., Carr C., Gunsch G., *An examination of digital forensics models,* International Journal of Digital Evidence, 1(3), 2002.

[160] Reyes A., *Cyber Crime Investigations :Bridging the Gaps Between Security Professionals, Law Enforcement and Prosecutors*, Syngress Publishing, Inc. 2007.

[161] Reyes A., Wiles J., *The best damn cybercrime and digital forensics book period*, Syngress, 2007.

[162] Ridder C. K., *Evidentiary Implications of Potential Security Weaknesses in Forensic Software*, Center for Internet and Society Stanford Law School, 2007.

[163] Rowlingson R., *A Ten Step Process for Forensic Readiness,* International Journal of Digital Evidence (2:3), pp. 1-28, Winter 2004.

[164] Rude T. *DD and Computer Forensics,* 2000. Izvor: http://www.crazytrain.com/dd.html , 13.02.2012.

[165] Saferstein R., *Criminalistics: An Introduction to Forensic Science*, 7 edition, Pearson , 2000.

[166] Sammes T., Jenkinson B., *Forensic Computing, Second edition*, Springer-Verlag, London, Limited 2007.

[167] Scarfone K., Mell P., *Guide to Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-94, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg MD 20899-8930, February 2007.

[168] Scarfone K., Mell P., *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities (DRAFT)*, NIST Interagency Report 7502 (Second Public Draft), Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology,Gaithersburg, MD 20899-8930, June 2009.

[169] Schatz B., *BodySnatcher: Towards reliable volatile memory acquisition*, Elsevier, pp. 126 – 134, 2007. Izvor: http://www.dfrws.org/2007/proceedings/p126-schatz.pdf

[170] Schneier B., *Secrets & Lies*, Digital Security in a Networked World, John Wiley & Sons, 2000.

[171] Schweitzer D., *Incident Response - Computer Forensics Toolkit*, Wiley Publishing, Inc, Indianapolis, 2003.

[172] Scott M., *Independent Review of Common Forensics Imaging Tools*, Memphis Technology Group, SANS GIAC Paper Submission, 2004.

[173] Shimonski R., *Defining a security policy*, 2003, Izvor : http://www.Windowsecurity.com/articles-tutorials/misc_network_security/Defining_a_Security_Policy.html

[174] Shinder D. L., *Scene of the Cybercrime: Computer Forensics Handbook*, Syngress Publishing, Inc. 2002.

[175] Shipley T. G., Reeve H. R., *Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community*, SEARCH The National Consortium for Justice Information and Statistics, 2006.

[176] Simms M., *Portable Storage Forensics: Enhancing the Value of USB Device Analysis and Reporting*, Faculty of Design and Creative Technologies AUT University, 2012.

[177] Sinchak S., *Hacking Windows XP, Wiley Publishing*, Inc., Indianapolis, Indiana, 2004.

[178] Sindhu K. K, Meshram B. B., *Digital Forensic Investigation using WinHex Tool*, IJCST Vol. 3, Issue 1, March 2012.

[179] Solomon M. G., Barrett D., Broom N., *Computer Forensics JumpStart*, Sybex, Alameda CA, 2005.

[180] Spafford E. H., Weeber S. A., *Software Forensics: Can We Track Code to its Authors?*, Computer Science Technical reports, paper 935, Department of Computer

Sciences, Purdue University, 1992. Izvor : http://spaf.cerias.purdue.edu/tech-reps/9210.pdf

[181] Spernow W., *Microsoft hack may really be a sweet success for honeypot networks*, 2000. Izvor : http://www.gartner.com/resources/93800/93829/microsoft_hack_may_really_be_93829.pdf

[182] Stephen Northcutt, *Computer security incident handling an action plan for dealing with intrusions, cyber-theft, and other security-related events, version 2.3.1*, SANS Institute, March 2003. Izvor : http://itsecurity.gmu.edu/Resources/upload/ComputerIncidentHandling.pdf

[183] Stephenson P., *Investigating computer-related crime a handbook for corporate investigators*, CRC Press LLC, 2000.

[184] Stevanović B., *Kompjuterska forenzika: odgovor na incident*, Ziteh - Udruženje sudskih veštaka za informacione tehnologije It veštak, 2006. Izvor : http://www.itvestak.org.rs/ziteh_06/Radovi/ZITEH%2006-R30.pdf

[185] Street J. E., Nabors K., Baskin B., Carey M., *Dissecting the Hack, Revised Edition*, Elsevier, Inc, 2010.

[186] Tasić A., *Forenzika usb i compact flash memorijskih uređaja*, master rad, Univerzitet Singidunum 2010.

[187] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, *Background paper for the workshop on crimes related to the computer network: Crime-fighting on the Net*, 2000 Izvor : http://www.un.org/events/10thcongress/2088h.htm

[188] The Association of Certified Fraud examiners, *Fraud examiners manual*, ACFE, Texas, USA, 2006.

[189] The Experts Consensus, *The Twenty Most Critical Internet Security Vulnerabilities (Updated)*, Version 2.501 November 15, The SANS Institute , 2001.

[190] The Sans Institute, *Computer security incident handling step by step, version 1.5*, SANS Institute, May 1998. Izvor : http://www.kumanov.com/dox/Ebook_Library/Ebook%20Library_2/Incident%20Handling%20Step%20by%20Step%20%28SANS%29.pdf

[191] Thornton J. I., *The General Assumptions And Rationale Of Forensic Identification*, written at St. Paul, in David L. Faigman, David H. Kaye, Michael J. Saks, & Joseph Sanders, Modern Scientific Evidence: The Law And Science Of Expert Testimony, vol. 2, West Publishing Co., 1997*)*

[192] Tulloch M., *Understanding Microsoft Virtualization Solutions from desktop to the datacentar*, second edition, Microsoft Press A Division of Microsoft Corporation One Microsoft Way Redmond, 2010.

[193] U.S. Department of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, U.S. Department of Justice Office of Justice Programs, April 2004.

[194] U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, NIJ Special Report series, NCJ 199408, Washington DC, April 2004. Izvor: https://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[195] Vacca J. R., *Computer Forensics Computer Crime Scene Investigation 2nd Edition*, Charles River Media, INC., Boston, Massachusetts, 2005.

[196] Visa International, Asia Pacific, *Incident Response Procedure for Account Compromise*, VISA PUBLIC, 2004. Izvor : http://www.visa-asia.com/ap/center/merchants/riskmgmt/includes/uploads/visaap_inc_resp_procedure_2_2004.pdf

[197] VMWare, *VMWare Vsphere ESXi*, http://www.vmware.com/products/vsphere-hypervisor/overview.html , Pristupljeno 09.02.2012

[198] Volonino L., Anzaldua R., *Computer Forensics For Dummies*, Wiley Publishing, Inc., 2008.

[199] Volonino L., Anzaldua R., Godwin J., *Computer forensics principles and practices*, Pearson Education, Inc Upper Saddle River, New Jersey, 2007.

[200] Vugdelija N., Savić A., *Bezbednost računarskih sistema u savremenom elektronskom poslovanju*, Infoteh-Jahorina Vol. 10, Ref. E-III-10, pp. 631-635, March 2011.

[201] Waits C., Akinyele J. A., Nolan R., Rogers L., *Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis*, Software Engeneering Institute Carnegie Mellon, 2008. Izvor : http://repository.cmu.edu/sei/290/

[202] Wang X., Yin Y., Yu H., *Finding Collisions in the Full SHA-1*, Advances in Cryptology-Crypto 05, LNCS 3621, pp. 17-36, 2005.

[203] Wee K. C., *Analysis of hidden data in the NTFS file system*, 2006. Izvor : http://www.forensicfocus.com/hidden-data-analysis-ntfs

[204] Weise J., Powell B., *Using Computer Forensics When Investigating System Attacks*, Sun BluePrints, 2005.

[205] Wilson C., *Computer attack and cyber terrorism : Vulnerabilities and policy issues for Congress*. Us Congressional Research Report RL32114, strana 4. Izvor : http://www.fas.org/irp/crs/RL32114.pdf. October 17 2003

[206] Yasinsac A., *Policies to Enhance Computer and Network Forensics, Proceedings of the 2001 IEEE*, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001.

PRILOZI

PRILOG 1. ČEK-LISTA INICIJALNOG ODGOVORA

Ček-liste Inicijalnog odgovora koji obuhvata pomenute kritične detalje:

Datum:
Vreme:
Ime:
Telefonski broj:
Karakter protivpravne aktivnosti:
Vreme protivpravne aktivnosti:
Kako se otkrila protivpravna aktivnost:
Trenutni uticaj protivpravne aktivnosti:
Kako bi protivpravna aktivnost imala uticaj u budućnosti:
Opis protivpravnih aktivnosti:
Hardver/Operatvni sistem/Programi kompromitovanog računara:
IP adrese i mrežne adrese kompromitovanog računara:
Tip mreže:
Modem:
Značajnost informacija (kritičnost):
Fizička lokacija:
Ime sistem administratora i broj telefona:
Trenutni status računara:
Opis aktivnosti napadača
Aktivnost u toku:
Izvorna adresa:
Umešanost zlonamernog programa:
Odbijanje servisa
Vandalizam
Postojanje spoljašnjih i insajderskih pokazatelja:
Aktvnosti klijenta
Da li je mreža isključena
Mogućnost udaljenog pristupa
Mogućnost lokalnog pristupa
Izmene na firewallu
Postojanje i pregled audit logova na sistemu
Izmene na ACL listama
Obaveštena osoba
Ostale preuzete aktivnosti

Raspoloživi alati
Korišćeni alati za analizu mreže i računara
Dodatne kontakt osobe:
Korisnici:
Sistem administratori
Mrežni administratori
Specijalne informacije
Ko ne treba da zna o incidentu/protivpravnoj aktivnosti
Potpis lica koje odgovara na incidentnu / protivpravnu aktivnost

PRILOG 2 HARDVERSKA PREPORUKA NEOPHODNA ZA ODGOVOR NA PROTIVPRAVNU AKTIVNOST

-2x veoma brza i tehnološki najsavremeniji računara koji će predstvaljati forenzičke računare (što je računar brži, rezultati će se dobiti brže)
-dodatna napajanja za periferne uređaje (dvd, cd i drugi drajvovi) na forenzičkom računaru
-brz dvd rezač, ide drajvovi velikih kapaciteta, sata drajvovi velikih kapaciteta, scsi hard diskovi velikog kapaciteta, scsi kartice i kontroleri sa kablovima i terminatorima za kablove.
-nekoliko različitih operativnih sistema Windows 98, Windows 2000, Linux Slackware, Linux Ubuntu (sa LILO loaderom odnosi se na Linux okruženje) podignutih na jednom računaru
-na drugom računaru realizovano virtuelno okruženje sa velikim brojem operativnih sistema odnosno virtuelnih mašina
-lap top računar
-eksterni tape drajv sa 400GB kapacitetom i 800 gb kompresovanim kapacitetom
-diktafon
-firewire ili usb eksterno kućište
-100 praznih DVD diskove
-nalepnice i obeleživači za dvd diskove
-nalepnice i obeleživači za fascikle sa dokazima
-swichevi i kablovi kategorije 5 5e i 6 za potršku za rad sa mrežama 10/100/1000
-kablovi ATA-33, ATA-100, SATA
-različite vrste adaptera (serial to parallel, paralles to scsi, usb to ps2, ps2 to usb, scsi to ide, scsi to sata, scsi to firewire, scsi to usb,)
-smart ups
-flomaster za obeležavanje dvd diskova
-uputstva za kompletan hardver
-eksterni dvd čitač
-eksterni floppy drajv
-eksterni uređaji za skladištenje podataka (što većeg kapaciteta)
-digitalna kamera i fotoaparat
-odgovarajući alat za otvaranje računara
-produžne kablove
-štampač skener i papir
-prostorija koja se zaključava i koja služi za skladištenje dokaza
-min 10 antistatičnih kesa za računarske dokaze
-min 10 obrazaca za dokumentovanje prikupljenih dokaza
-baterijska lampa
-hardverski blokator upisa
-programski blokator upisa

Preporučeni neophodni programi za odgovor na protivpravnu aktivnost :
-forenzički programi : Encase, AccessData, SnapBack, SafeBack
-Forenzički bootabilni diskovi sa forenzičkim alatima za prikupljanje dokaza
-alati za brisanje diska
-alati za pregledanje fajlova

PRILOG 3 TABELA KRITERIJUMA ZA PRETRAŽIVANJE FAJL SISTEMA KOMANDOM FIND

Kriterijum	Značenje
-name	ime fajla
-iname	ime fajla, ingorišući razlike između malih i velikih slova
-user	korisnik koji je vlasnik fajla
-group	grupa koja je vlasnik fajla
-size	veličina fajla u blokovima (ili karakterima)
-atime	vreme poslednjeg pristupa u danima
-mtime	vreme poslednje promene sadržaja fajla
-ctime	vreme poslednje promene statusa fajla
-newer	univerzalni temporalni kvalifikator
-perm	prava pristupa fajlu
-moun	sprečava da pretraga pređe granice sistema datoteka
-type	tip fajla
-print	štampanje apsolutne putanje i imena datoteka
-regex	ime fajla zadato regularnim izrazom

PRILOG 4. Krivična dela visokotehnološkog kriminala predviđena Krivičnim zakonikom Republike Srbije

KRIVIČNA DELA VISOKOTEHNOLOŠKOG KRIMINALA PREDVIĐENA KRIVIČNIM ZAKONIKOM REPUBLIKE SRBIJE "Sl glasnik RS", br 85/2005, br. 88/2005, br. 107/2005, br. 72/2009, br. 111/2009, i br. 121/2012.

Zakonske definicije koje se odnose na računarska krivična dela:

- Računarski podatak - predstavlja informaciju, znanje, činjenicu, koncept ili naredbu koja se unosi, obrađuje ili pamti ili je uneta, obrađena ili zapamćena u računaru ili računarskoj mreži.
- Računarska mreža- je skup međusobno povezanih računara koji komuniciraju razmenjujući podatke.
- Računarski program - je uređeni skup naredbi koji služe za upravljanje radom računara kao i za rešavanje određenog zadatka pomoću računara.
- Računarski virus - je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.
- Ispravom se smatra svaki predmet koji je podoban ili određen da služi kao dokaz kakve činjenice koja ima značaj na pravne odnose, kao i računarski podatak.
- Pokretna stvar je svaka proizvedena ili sakupljena energija za davanje svetlosti, toplote ili kretanja, telefonski impuls, kao i računarski podatak i računarski program.

KRIVIČNA DELA PROTIV BEZBEDNOSTI RAČUNARSKIH PODATAKA PREDVIĐENA KRIVIČNIM ZAKONOM REPUBLIKE SRBIJE

- **Oštećenje računarskih podataka i programa** (čl. 298). Ko neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program, kazniće se novčanom kaznom ili zatvorom do jedne godine.
- Ako prouzrokovana šteta prelazi četristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od tri meseca do tri godine.
- Ako prouzrokovana šteta prelazi milion i petsto hiljada dinara, učinilac će se kaznti zatvorom od tri meseca do pet godnna.
- Uređaji i sredstva kojima je učinjeno ovo krivično delo, ako su u svojini učinioca, oduzeće se.
- **Računarska sabotaža** (čl. 299). Ko unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program ili uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte, kazniće se zatvorom od šest meseci do pet godina.

- **Pravljenje i unošenje računarskih virusa** (čl. 300). Ko napravi računarsk virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu, kazniće se novčanom kaznom ili zatvorom do šest meseci. Ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, kazniće se novčanom kaznom ili zatvorom do dve godine. Uređaj i sredstva kojima je učinjeno ovo krivično delo oduzeće se.

-Računarska prevara (čl. 301). Ko unese netačan podatak, propusti unošenje tačnog podatka ili na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u namern da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje pmovinsku štetu, kazniće se novčanom kaznom ili zatvorom do tri godine.

Ako pribavljena imovinska korist prelazi iznos od četiristo pedeset hiljada dinara, učinilac će se kazniti zatvorom od jedne do osam godina.

Ako pribavljena imovinska korist prelazi iznos od milion i petsto hiljada dinara, učinilac će se kazniti zatvorom od dve do deset godina. Ko ovo delo učini samo u nameri da drugog ošteti, kazniće se novčanom kaznom ili zatvorom do šest meseci.

- Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (čl. 302). Ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka, kazniće se novčanom kaznom ili zatvorom do šest meseci.

Ko upotrebi ovako dobijen podatak, kazniće se novčanom kaznom ili zatvorom do dve godine.

Ako je došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade prenosa podataka ili mreže ili su nastupile druge teške posledice, učinilac će se kazniti zatvorom do tri godine.

- Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (čl. 303). Ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži, kazniće se novčanom kaznom ili zatvorom do jedne godine. Ako delo učini službeno lice u vršenju službe, kazniće se zatvorom do tri godine.

- Neovlašćeno korišćenje računara ili računarske mreže (čl. 304). Ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist, kazniće se novčanom kaznom ili zatvorom do tri meseca. Gonjenje za ovo krivično delo preduzima se po privatnoj tužbi.

KRIVIČNA DELA PROTIV INTELEKTUALNE SVOJINE PREDVIĐENA KRIVIČNIM ZAKONOM REPUBLIKE SRBIJE

Povreda moralnih prava autora i interpretatora

Član 198

(1) Ko pod svojim imenom ili imenom drugog u celini ili delimično objavi, stavi u promet primerke tuđeg autorskog dela ili interpretacije, ili na drugi način javno saopšti tuđe autorsko delo ili interpretaciju,kazniće se novčanom kaznom ili zatvorom do tri godine.

(2) Ko bez dozvole autora izmeni ili preradi tuđe autorsko delo ili izmeni tuđu snimljenu interpretaciju,kazniće se novčanom kaznom ili zatvorom do jedne godine.

(3) Ko stavlja u promet primerke tuđeg autorskog dela ili interpretacije na način kojim se vređa čast ili ugled autora ili izvođača,kazniće se novčanom kaznom ili zatvorom do šest meseci.

(4) Predmeti iz st. 1. do 3. ovog člana oduzeće se.

(5) Gonjenje za delo iz stava 2. ovog člana preduzima se po predlogu, a za delo iz stava 3. ovog člana po privatnoj tužbi.

Neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava

Član 199

(1) Ko neovlašćeno objavi, snimi, umnoži, ili na drugi način javno saopšti u celini ili delimično autorsko delo, interpretaciju, fonogram, videogram, emisiju, računarski program ili bazu podataka,kazniće se zatvorom do tri godine.

(2) Kaznom iz stava 1. ovog člana kazniće se i ko stavi u promet ili u nameri stavljanja u promet drži neovlašćeno umnožene ili neovlašćeno stavljene u promet primerke autorskog dela, interpretacije, fonograma, videograma, emisije, računarskog programa ili baze podataka.

(3) Ako je delo iz st. 1. i 2. ovog člana učinjeno u nameri pribavljanja imovinske koristi za sebe ili drugog,učinilac će se kazniti zatvorom od šest meseci do pet godina.

(4) Ko proizvede, uveze, stavi u promet, proda, da u zakup, reklamira u cilju prodaje ili davanja u zakup ili drži u komercijalne svrhe uređaje ili sredstva čija je osnovna ili pretežna namena uklanjanje, zaobilaženje ili osujećivanje tehnoloških mera namenjenih sprečavanju povreda autorskih i srodnih prava, ili ko takve uređaje ili sredstva koristi u cilju povrede autorskog ili srodnog prava,kazniće se novčanom kaznom ili kaznom zatvora do tri godine.

(5) Predmeti iz st. 1. do 4. ovog člana oduzeće se i uništiti.

Neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom i srodnim pravima

Član 200

(1) Ko neovlašćeno ukloni ili izmeni elektronsku informaciju o autorskom ili srodnom pravu, ili stavi u promet, uveze, izveze, emituje ili na drugi način javno saopšti autorsko delo ili predmet srodnopravne zaštite sa kojeg je elektronska informacija o pravima neovlašćeno uklonjena ili izmenjena, kazniće se novčanom kaznom i zatvorom do tri godine.

(2) Predmeti iz stava 1. oduzeće se i uništiti.

Povreda pronalazačkog prava

Član 201

(1) Ko neovlašćeno proizvodi, uvozi, izvozi, nudi radi stavljanja u promet, stavlja u promet, skladišti ili koristi u privrednom prometu proizvod ili postupak zaštićen patentom,kazniće se novčanom kaznom ili zatvorom do tri godine.

(2) Ako je delom iz stava 1. ovog člana pribavljena imovinska korist ili prouzrokovana šteta u iznosu koji prelazi milion dinara,učinilac će se kazniti zatvorom od jedne do osam godina.

(3) Ko neovlašćeno objavi ili na drugi način učini dostupnim suštinu tuđeg prijavljenog pronalaska pre nego što je ovaj pronalazak objavljen na način utvrđen zakonom,kazniće se novčanom kaznom ili zatvorom do dve godine.

(4) Ko neovlašćeno podnese prijavu patenta ili u prijavi ne navede ili lažno navede pronalazača,
kazniće se zatvorom od šest meseci do pet godina.

(5) Predmeti iz st. 1. i 2. oduzeće se i uništiti.

Neovlašćeno korišćenje tuđeg dizajna

Član 202

(1) Ko na svom proizvodu u prometu neovlašćeno upotrebi, u celosti ili delimično, tuđi prijavljeni, odnosno zaštićeni dizajn proizvoda,kazniće se novčanom kaznom ili zatvorom do tri godine.

(2) Ko neovlašćeno objavi ili na drugi način učini dostupnim javnosti predmet prijave tuđeg dizajna pre nego što je objavljen na način utvrđen zakonom,kazniće se novčanom kaznom ili zatvorom do jedne godine.

(3) Proizvodi iz stava 1. ovog člana oduzeće se.

KRIVIČNA DELA PROTIV POLNE SLOBODE PREDVIĐENA KRIVIČNIM ZAKONOM REPUBLIKE SRBIJE

Prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju

Član 185

(1) Ko maloletniku proda, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim tekstove, slike, audio-vizuelne ili druge predmete pornografske sadržine ili mu prikaže pornografsku predstavu,kazniće se novčanom kaznom ili zatvorom do šest meseci.

(2) Ko iskoristi maloletnika za proizvodnju slika, audio-vizuelnih ili drugih predmeta pornografske sadržine ili za pornografsku predstavu,kazniće se zatvorom od šest meseci do pet godina.

(3) Ako je delo iz st. 1. i 2. ovog člana izvršeno prema detetu, učinilac će se kazniti za delo iz stava 1. zatvorom od šest meseci do tri godine, a za delo iz stava 2. zatvorom od jedne do osam godina.

(4) Ko pribavlja za sebe ili drugog, poseduje, prodaje, prikazuje, javno izlaže ili elektronski ili na drugi način čini dostupnim slike, audio-vizuelne ili druge predmete pornografske sadržine nastale iskorišćavanjem maloletnog lica, kazniće se zatvorom od tri meseca do tri godine.

(5) Predmeti iz st. 1. do 4. ovog člana oduzeće se.

KRIVIČNA DELA PROTIV PRIVREDE PREDVIĐENA KRIVIČNIM ZAKONOM REPUBLIKE SRBIJE

Falsifikovanje i zloupotreba platnih kartica

Član 225

(1) Ko napravi lažnu platnu karticu ili ko preinači pravu platnu karticu u nameri da je upotrebi kao pravu ili ko takvu lažnu karticu upotrebi kao pravu,kazniće se zatvorom od šest meseci do pet godina i novčanom kaznom.

(2) Ako je učinilac dela iz stava 1. ovog člana upotrebom kartice pribavio protivpravnu imovinsku korist,kazniće se zatvorom od jedne do osam godina i novčanom kaznom.

(3) Ako je učinilac dela iz stava 1. ovog člana pribavio protivpravnu imovinsku korist u iznosu koji prelazi milion i petsto hiljada dinara,kazniće se zatvorom od dve do dvanaest godina i novčanom kaznom.

(4) Kaznom iz st. 2. i 3. ovog člana kazniće se i učinilac koji to delo učini neovlašćenom upotrebom tuđe kartice ili poverljivih podataka koji jedinstveno uređuju tu karticu u platnom prometu.

(5) Ko nabavi lažnu platnu karticu u nameri da je upotrebi kao pravu ili ko pribavlja podatke u nameri da ih iskoristi za pravljenje lažne platne kartice,kazniće se novčanom kaznom ili zatvorom do tri godine.

(6) Lažne platne kartice oduzeće se.

PRILOG 5 EVENT ID KOJI SE ODNOSE NA SISTEMSKU BEZBEDNOST

U ovom prilogu prikazani će biti bezbednosni Event ID-ovi koji digitalnom forenzičaru mogu pružiti uvid u dešavanje na ispitivanom računaru, odnosno administratoru sistema mogu ukazati na potencijalni problem. Prikazana lista odnosi sa na Windows operativne sisteme Windows 2000 i Windows XP (pre Windows Viste). Zbog promenjenog načina logovanja kod Windows Viste i Windows 7 kod većine bezbednosnih Event ID-a dodaje se broj 4096 na event ID[592].

- Type 2 : Konzolno logovanje sa lokalnog računara.
- Type 3 : Logovanje preko mreže ili mrežno mapiranje (net use/net view)
- Type 4 : batch logovanje i upotreba scheduler-a
- Type 5 : servisno logovanje uz pomoć naloga
- Type 7 : otključavanje radne stanice
- Event ID 528 : Uspešno logovanje na lokalni računar
- Event ID 529 : nepoznat korisnik ili upotreba pogrešne šifre
- Event ID 530 : Prekoračenje vremenskog ograničenja za logovanje
- Event ID 531 : Nalog je onemogućen (eng. disabled)
- Event ID 532 : Nalog je istekao (eng. expired)
- Event ID 533 : Ograničenje na randnoj stanici, korisniku nije dozvoljeno logovanje na računar.
- Event ID 534 : Neodgovarajuča prava za konzolno logovanje.
- Event ID 535 : Šifra je istekla expired
- Event ID 536 : Net Logon servis je nedostupan
- Event ID 537 : Neočekivana greška pri logovanju. Moguća je upotreba blanko korisničkog naloga ili nesinhronizovano vreme između lokalnog računara i domenskog kontrolera[593]. Da bi se tačno odredio razlogo konsultovati opis Status Code i Substatus Code.
- Event ID 538 : Korisnik se odjavio sa sistema (interaktivno, mrežno ili nekim drugim načinom)
- Event ID 539 : Greška logovanja: Nalog je zaključan
- Event ID 540 : Uspešno mrežno logovanje. Korisnik koristi deljene resurse.
- Event ID 627 : NT AUTHORITY\ANONYMOUS pokušava da promeni šifru
- Event ID 644 : Korisnički nalog je zaključan
- Event ID 541 : Uspostavljanje IPSec security sesije
- Event ID 542 : Kraj IPSec security sesije (mod zaštite podataka)
- Event ID 543 : Kraj IPSec security (razmene ključeva)
- Event ID 544 : Uspostavaljanje IPSec security sesije nije uspelo zbog nemogućnosti autentifikacije peer-a
- Event ID 545 : Autentifikacija IPSec peer-a nije uspela
- Event ID 546 : Uspostavaljanje IPSec security sesije nije uspelo zbog nevažećeg odgovora od strane peer-a.
- Event ID 547 : IPSec security sesija neuspela u pregovaranjima
- Event ID 551 : Korisnik je inicirao odjavu sa sistema.
- Event ID 560 : Otvaranje obejkta od strane programa koji su omogućeni za auditing.
- Event ID 567 : Pokušaj pristupanju objektu od strane korisnika ili programa.
- Event ID 624 : Kreiran je korisnički nalog

[592] http://blogs.msdn.com/b/ericfitz/archive/2007/04/18/vista-security-events-get-noticed.aspx
[593] http://www.ultimateWindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=537

- Event ID 626 : Korisnički nalog je omogućen (eng. enabled). Kod Windwos 2000 se ne loguje ali se kod Windows 2003 loguje.
- Event ID 627 : Pokušaj promene šifre od strane korisnika
- Event ID 628 : Postavljanje šifre od strane korisnika
- Event ID 629 : Korisnički nalog je onemogućen.
- Event ID 630 : Korisnički nalog je obrisan
- Event ID 642 : Korisnički nalog je izmenjen
- Event ID 672 : Odobren Autentifikacioni tiket
- Event ID 673 : Odobren Servisni tiket
- Event ID 674 : Odobren tiket za obnovu
- Event ID 675 : Neuspela pre-autentifikacija
- Event ID 676 : Zahtev za Autentifikacionim tiketom neuspešan
- Event ID 677 : Zahtev sa servisnim tiketom neuspešan
- Event ID 678 : Nalog je mapiran za logovanje
- Event ID 679 : Nalog ne može biti mapiran za logovanje
- Event ID 680 : Nalog se koristi za logovanje
- Event ID 681 : Neuspelo logovanje. Kodna greška je :
- Event ID 682 : Sesija je obnovljena sa Windows radnom stanicom
- Event ID 683 : Sesija je prekinuta sa Windwos radne stanice
- Event ID 4625 : Neuspešno logovanje naloga (primer za *Windows Vista/2008/Windows 7*)
- Event ID 4634 : Korisnički nalog je izlogovan (primer za *Windows Vista/2008/Windows 7*)
- Event ID 4647 : Korisnik je inicirao logoff (primer za *Windows Vista/2008/Windows 7*)
- Event ID 7035 : Odnosi se na pokretanje i stanje servisa (primer za *Windows Vista/2008/Windows 7*)
- Event ID 7036 : Odnosi se na pokretanje i stanje servisa (primer za *Windows Vista/2008/Windows 7*)

PRILOG 6 IZJAVA O AUTORSTVU

Potpisani : VANJA KORAĆ

Broj indeksa : _____

Izjavljujem

da je doktorska disertacija pod naslovom :

"DIGITALNA FORENZIKA U FUNKCIJI ZAŠTITE INFORMACIONOG SISTEMA BAZIRANOG NA LINUX I WINDOWS PLATFORMAMA"

- rezultat sopstvenog istraživačkog rada,
- da predložena disertacija u celini ni u delovima nije bila predložena za dobijanje bilo koje diplome prema studijskim programima drugih visokoškolskih ustanova,
- da su rezultati korektno navedeni i
- da nisam kršio/la autorska prava i koristio intelektualnu svojinu drugih lica.

Potpis doktoranda

U Beogradu, _____ _____

PRILOG 7 IZJAVA O ISTOVETNOSTI ŠTAMPANE I ELEKTRONSKE VERZIJE DOKTORSKOG RADA

Ime i prezime autora : VANJA KORAĆ

Broj indeksa : _____

Studijski program : STARI STUDIJSKI PROGRAM

Naslov rada : "DIGITALNA FORENZIKA U FUNKCIJI ZAŠTITE INFORMACIONOG SISTEMA BAZIRANOG NA LINUX I WINDOWS PLATFORMAMA"

Mentor : prof. dr. Žarko Mijajlović, redovni profesor, PMF, Univerzitet u Beogradu

Potpisani : VANJA KORAĆ

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao za objavljivanje na portalu Digitalnog repozitorijuma Univerziteta u Beogradu.

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog zvanja doktora nauka, kao što su ime i prezime, godina i mesto rođenja i datum odbrane rada.

Ovi lični podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Univerziteta u Beogradu.

Potpis doktoranda

U Beogradu, _____ _____

PRILOG 8 IZJAVA O KORIŠĆENJU

Ovlašćujem Univerzitetsku biblioteku „Svetozar Marković“ da u Digitalni repozitorijum Univerziteta u Beogradu unese moju doktorsku disertaciju pod naslovom :

“DIGITALNA FORENZIKA U FUNKCIJI ZAŠTITE INFORMACIONOG SISTEMA BAZIRANOG NA LINUX I WINDOWS PLATFORMAMA“, koja je moje autorsko delo.

Disertaciju sa svim prilozima predao sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalni repozitorijum Univerziteta u Beogradu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio/la.

1. Autorstvo

2. Autorstvo - nekomercijalno

3. Autorstvo - nekomercijalno – bez prerade

4. Autorstvo - nekomercijalno – deliti pod istim uslovima

5. Autorstvo - bez prerade

6. Autorstvo - deliti pod istim uslovima

(Molimo da zaokružite samo jednu od šest ponuđenih licenci, kratak opis licenci dat je na poleđini lista).

Potpis doktoranda

U Beogradu, _____ _____

1. Autorstvo - Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. Autorstvo – nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. Autorstvo - nekomercijalno – bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. Autorstvo - nekomercijalno – deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. Autorstvo – bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. Autorstvo - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.

PRILOG 9 BIOGRAFIJA AUTORA

Kandidat Vanja Korać rođen je 13.10.1976. godine u Beogradu. Osnovnu i srednju školu završio je u Beogradu. Visoko obrazovanje stekao je na Fakultetu za poslovnu informatiku Univerziteta "Singidunum" 2005. godine u Beogradu, na smeru programiranje i projektovanje, gde dobija zvanje diplomirani inženjer informatike.

Nakon uspešno završenih osnovnih studija, pohađao je specijalističke studije na Fakultetu za poslovnu informatiku Univerziteta “Singidunum” u Beogradu, smer bezbednost informacionih sistema i elektronskog poslovanja i 2006. godine stekao diplomu specijaliste za bezbednost informacionih sistema i elektronskog poslovanja, sa zvanjem specijalista za bezbednost elektronskih komunikacija i elektronskog poslovanja.

Magistarske studije na fakultetu za poslovnu informatiku Univerziteta "Singidunum" završio je 2008. godine odbranom magistarskog rada sa temom "Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja", gde dobija zvanje magistra informatike.

2011. godine odobrena mu je tema za izradu doktorske disertacije od strane Centra za multidisciplinarne studije Univerziteta u Beogradu pod naslovom : "**Digitalna forenzika u funkciji zaštite informacionog sistema baziranog na Linux i Windows platformama** ".

U stalnom je radnom odnosu na radnom mestu Rukovodilac računarskog centra i administrator sistema i mreže Matematičkog instituta SANU.

Takođe, kao saradnik Arheološkog instituta SANU zadužen je za administriranje mreže i sistema.

Bio je angažovan na projektima :

- 2008. FP6 projekat: ADHOCSYS (Wireless Ad-Hoc Broadband Monitoring System);

- 2008-2010 Projekat 144018 pri Ministarstvu za nauku Republike Srbije (Napredne metode u kriptologiji i procesiranju informacija).

Trenutno je angažovan na projektu Ministarstva za nauku Republike Srbije:

- 2010- III 47018 - IRS - Viminacium, rimski grad i legijski vojni logor - istraživanje materijalne i duhovne kulture, stanovništva, primenom najsavremenijih tehnologija daljinske detekcije, geofizike, GIS-a, digitalizacije i 3D vizuelizacije.

Objavljeni radovi

Radovi međunarodnog značaja (M20):

Rad objavljen u međunarodnom časopisu

M23

1. Korać V., Kratica J., Savić A., *An Improved Genetic Algorithm for the Multi Level Uncapacitated Facility Location Problem,* International Journal Of Computers Communications & Control 8 (6):845-853, ISSN 1841-9836, Oradea, 2013.

Monografije nacionalnog značaja (M40)

Istaknuta monografija nacionalnog značaja

M41

1. Korać V., *Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja*, Monografija, Arheologija i prirodne nauke, specijalna izdanja, Centar za nove tehnologije Viminacium, Arheološki institut, ISSN 1820, -6492, ISBN 978-86-87271-21-0, Beograd, 2010.
2. Korać V., *Digitalna forenzika kao arheologija podataka u visokotehnološkom kriminalu,* Monografija, časopis Arheologija i prirodne nauke, specijalna izdanja 6, Centar za nove tehnologije Viminacium, Arheološki institut, ISBN 978-86-87271-22-7, Beograd, 2013.

Radovi nacionalnog značaja (M50):

Rad objavljen u časopisu nacionalnog značaja

M52

1. Korać V., *SPAM*, Arheologija i prirodne nauke, br.1, str. 137-150, ISSN 1452-7448, COBISS.SR-ID 136747788; Beograd, 2006.
2. Korać V., *Mobilni E-komerc*, Arheologija i prirodne nauke, br. 2, str. 129-144, ISSN 1452-7448, COBISS.SR-ID 136747788; Beograd, 2006.
3. Korać V., *Prevencija širenja virusa kroz autorun funkciju operativnog sistema*, Arheologija i prirodne nauke br.4, str. 103-107, UDK 004.056.57, ISSN 1452-7448, Beograd, 2008.
4. Korać V., *Uputstvo za povećanje sigurnosti bežičnih mreža implementacija*, Arheologija i prirodne nauke, br.5 , str. 111-122, UDK 004.7.056.5; 004.056; 621.39:004.7, ISSN 1452-7448, Beograd, 2009.
5. Davidovac Z., Korać V., *Vulnerability management and patching it systems*, Arheologija i prirodne nauke, br. 6, str. 129-144, UDK 007:004.056.5 005.21:004.49, ISSN 1452-7448, Beograd, 2011.
6. Korać V., *Digital archaeology in a virtual environment,* Arheologija i prirodne nauke, br. 8, str. 129-141, UDK BROJEVI: 902/904:004; 572:004, Beograd, 2013.
7. Korać V., *Digital archaeology of volatile data on Linux platform,* Arheologija i prirodne nauke, br. 9, 2014. (u štampi)

Istraživački rad i interesovanja vezana su za oblasti IT bezbednosti, kao i za oblast administracije i razvoj sistema i mreža. Odlično govori engleski jezik.