
DIGITALANA FORENZIKA
KAO ARHEOLOGIJA
PODATAKA U VISOKO
TEHNOLOŠKOM KRIMINALU
Vanja Korać

ARHEOLOGIJA I
PRIRODNE NAUKE
POSEBNA IZDANJA

Center for New Technology
Archaeological Institute Belgrade

ARCHAEOLOGY AND SCIENCE
SPECIAL EDITION
6

Belgrade 2012

Centar za nove tehnologije
Arheološki institut Beograd

ARHEOLOGIJA I PRIRODNE NAUKE
POSEBNA IZDANJA
6

Beograd 2012.

Published by:
Center for New Technology
Viminacium
Archaeological Institute Belgrade

For the publishers:
Miomir Korać
Slaviša Perić

Editor:
Miomir Korać

Edited by
Dragan Prlja
Gojko Grubor

Cover Design:
Nemanja Milićević

Graphic design by:
Nemanja Milićević

Print:
Digital Art Company Belgrade

Printed in:
500 copies

Izdavači:
Centar za nove tehnologije
Viminacium
Arheološki institut Beograd

Za izdavače:
Miomir Korać
Slaviša Perić

Urednik:
Miomir Korać

Recenzenti:
Dragan Prlja
Gojko Grubor

Dizajn Korica:
Digital Art Company

Dizajn i tehničko uređenje:
Nemanja Milićević

Štampa:
Digital Art Company Beograd

Tiraž:
500 primeraka

ISSN: 1452-7448
ISBN: 978-86-87271-22-7

Vanja Korać

DIGITALNA FORENZIKA KAO ARHEOLOGIJA PODATAKA U VISOKOTEHNOLOŠKOM KRIMINALU

Beograd 2012.

S a ž e t a k

U ovom radu su opisani tipovi visokotehnološkog kriminala, dat je osvrt na zakonsku regulativu i na određene primere iz prakse. Opisani su najznačajniji modeli istražnih metodologija. Detaljno su objašnjeni elementi digitalne forenzike računarskih sistema kroz digitalnu istragu kao i odgovor na forenzički relevantan događaj. U radu je dat i prikaz digitalne forenzike u virtuelnom okruženju iz dva pravca. Jedan pravac definiše virtuelno okruženje kao digitalno mesto protivpravne aktivnosti, a drugi pravac posmatra virtuelno okruženje kao okruženje za digitalno forenzičku analizu. Cilj ovog rada je da se pruži prikaz stanja iz ove oblasti, da se baci svetlo na digitalnu forenziku, odnosno na metode i tehnike digitalne forenzike računarskih sistema. Isto tako vrlo je značajan i inicijalni odgovor za forenzički relevantan događaj, koji može pomoći otkrivanju ovakve vrste kriminala (visokotehnološkog), sprečiti moguću štetu i dati korisne informacije za preventivnu zaštitu od budućih napada.

Abstract

This paper describes the types of cyber crime, gave an overview of the legislation and the specific examples in practice. The most important models of investigative methodologies are also described. Elements of computer forensics through the investigation and incident response for forensics relevant event are explained in details. The paper gives overview of digital forensics in a virtual environment from two directions. From first point of view, a digital virtual environment is defined as a place of crimescene. From second point of view, a digital virtual environment is defined as as an environment for digital forensic analysis. The goal of of this paper is to provide a view of the situation in this field, and also to throw light on digital forensics computer systems and its methods and techniques. In this paper is also considered initial incident response for forensic relevant event, that can help to detect this type of cyber crime, to prevent any possible damage and provide useful information for preventive protection against future attacks.

SADRŽAJ :

1. Uvod

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

Pojavom savremenih računara i široka rasprostranjenost velike količine najrazličitijih korisničkih programa uticalo je na promene života ljudi širom sveta. Ova tehnologija nam pruža ogromne mogućnosti i u velikoj meri nam olakšava naše živote. Današnji računari koji postaju sve manji a istovremeno „snažniji" nalaze primenu gotovo u svi 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, upravljanje uređajima, bezbednosti veštačkoj inteligenciji itd. Međutim, mora se razumeti da ona 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 za jednu sjajnu i pozitivnu ideju koja se odnosi na međusobnu komunikaciju na svetskom nivou. Međutim, 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 je i razvijanje ideje o korišćenju novih tehnologija u protivpravne svrhe [2]. In-

ternet je uvećao lakoću i brzinu kojom se sprovode kriminalne radnje uklanjajući fizička ograničenja i smanjujući fizički napor da bi se neko prevario. Npr iz banke mogu biti ukradene milijarde dolara u online okruženju za nekoliko minuta, za razliku od 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 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 dolazi veka do pojave visokotehnološkog kriminala.

Globalnom ekspanzijom korisnika Interneta[1] (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 [2] imalo je za posledicu i globalni talas krivičnih dela koja su povezana sa računarskim tehnologijama.

Visokotehnološki kriminal je tako postao svakodnevica, 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 [2]. U stvari on podrazumeva korišćenje interneta,

1 Izvor: http://www.internetworldstats.com/stats.htm pristup 16.11.2011

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

računara, mreža i srodnih tehnologija u izvršenju krivičnog dela uključujući kako tehnološki specifična krivična dela tako i tradicionalna krivična dela potpomognute informaciono komunikacionim tehnologijama. Ova rad je usmeren na digitalnu forenziku računarskih 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:

a. gotovo da ne postoji nijedna veća organizacija na svetu koja nije pretrpela kompromitovanje svojih sistema od strane napadača;
b. većina outsourced[3] (eng. outsourced) programa se pravi za backdoor-ovima[4], 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 bavljenjem 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 digitalnu forenziku odnosno metode i tehnike digitalne forenzike računarskih sistema kao i inicijalne odgovore na forenzički relevantne događaje, čime se doprinosi otkrivanju ovakve vrste kriminala (sajber), i preventivno delujući kao vid zaštite računarskih sistema za buduće napade.

3 Outsourced programi su programi koji se prave za ime i račun određene kompanije od strane neke druge kompanije.

4 Backdoor ili zadnja vrata predstavlja metod zaobilaženje normalne autentifikacije, neprimećeno obezbeđivanje daljinskog pristupa računaru.

2. 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 ću u daljem tekstu ovu vrstu kriminala nazivati visokotehnološki kriminal.

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.

Šta je međutim, tačno visokotehnološki kriminal, ili sajber kriminal, kako glasi američki naziv ove vrste 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 shvataju veliki broj Internet enciklopedija i rečnika, pa sajber kriminal definišu kao „kriminalnu aktivnost počinjenu korišćenjem računara i Interneta".[5]

5 Izvor: Internet adresa: http://www.techterms.com/definition/cybercrime, pristupano 21.11.2011.
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.

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.[6] 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 protiv pravne 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[7].

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.

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

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

Takođe izdvojio bih jednu najpotpuniju mada mažda 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[8]:

"*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 ona učinjena sa namerom a ne slučajnošću.

U Konvenciji o sajber kriminalu (Convention on Cybecrime[9]) 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 odnostno eng. umbrella termin – kišobran 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 podrazu-

8 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

9 http://conventions.coe.int/treaty/en/treaties/html/185.htm, 01.03.2012

mevaju krivična dela prema krivičnom zakonu nacionalne države, 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 [8][10] 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 [23][11]:

-**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 raču-

10 Milan Milosavljević, Gojko Grubor, ISTRAGA KOMPJUTERSKOG KRIMINALA - metodološko tehnološke osnove, Singidunum 2009. Strana 4

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

narom su tradicionalni zločine, kao što su krađe, prevare, falsifikovanja, uhođenje ili distribucija dečije pornografije. Razlika je u tome da su ove tradicionalni zločini počinjeni koristeći informaciono komunikacione tehnologije. Novije vrste krivičnih dela koje spadaju u ovu kategoriju spadaju ugrožavanje e-maila, krađu identiteta, spam, fišing (eng. phishing)[12], farming (eng. pharming)[13] kao i sve aktivnosti planiranja, rukovođenja, izvršenja i prikrivanja protivpravnih aktivnosti.

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 informaciono komunikacionih tehnologija (računari, mreže i ostali digitalni uređaji).

12 Fišing na mreži predstavlja način prevare korisnika računara u cilju otkrivanja ličnih ili finansijskih informacija putem lažne eporuke ili Web lokacije. Uobičajena phishing prevara na mreži počinje eporukom koja izgleda kao zvanično obaveštenje iz pouzdanog izvora, kao što je banka, preduzeće koje se bavi kreditnim karticama ili ugledni prodavac na mreži. Primaoce eporuka 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

13 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 email 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 emaila zaraženog virusom) koji služi za farming, ustvari 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

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[14].

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 ustvari sajber kriminal odnosi na bilo koji zločin koji je u vezi sa informaciono komunikacionim tehnologijama.

2.1. 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 B. Standler sajber kriminal prema obliku odnosno vrsti krivičnog dela deli u tri ka-

14 Dragan Prlja, Mario Reljanović, Pravna informatika, Pravni fakultet Univerziteta Union u Beogradu, 2010, strana 54

tegorije [15]: 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. sa pravnog fakulteta 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[16]

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.[17]"

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.[18]

Razlog ne postojanja univerzalne definicije je i taj što se 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

15 http://www.rbs2.com/ccrime.htm

16 Škulić Milan, AleksićŽivojin (2002.) — Kriminalistika-Dosije, Beograd, str.*396*

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

18 Zakon o organizaciji i nadrežnosti državnih organa za borbu protiv visokotehnološkog kriminaliteta, „Сл.гласник Р.Ц. бр.61/2005, 23. 10. 2011.

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 [9]

Profesor Predrag Dimitrijević kada govori ovom obliku kriminala podrazumeva je 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)[19]. 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 su navedeni su kroz definicije u užem i širem smislu [18]:

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) 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[20]. 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 [19] i listom OECD-a [20] iz 1989., odnosno 1985. godine. To su :

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

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

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

Evropska konvencija o sajber kriminalu [21] 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).

Profesor na Ročesterovom Tehnološkom institutu Samuel McQuade u Enciklopediji Sajber kriminala čiji je on uređivač, 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 [22]:

Upade 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 [17] :

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 [17]:

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
i) povrede sajber privatnosti (nadgledanje e-pošte; spam, phishing prisluškivanje, njuškanje lozinki tj. sniffing praćenje e-konferencija, prikačinjanje i analiza "cookies") [55].
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 "indiskretnom zlonamernom ponašanju"

kombinovane – kod kojih izvršenje krivičnog dela kao posledicu stvaraju i materijalnu i nematerijalna 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 dru-

gim 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 Draganu 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% delinkvenata 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[21], koji ko-

21 Napomenuio bih 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. npr ukoliko pronađu neki sigurnosni propust neće nanositi štetu već će ostaviti 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 napravi 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.

riste 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.

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 [22]: 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

Pavel Dugal, 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[23] :

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

22 Izvor :http://www.crime.hku.hk/cybercrime.htm, 22.11.2011
23 http://www.crime-research.org/analytics/702, 27.10.2011

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[24] 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 manipulacijom 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 [25] [24];
- **sajber uznemiravanje**, **uhođenje** (eng. cyber stalking) primer 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[26][25];
- **sajber nasilje – maltretiranje** (eng. cyber bullying). Dok se tradicionalno maltretiranje može izraziti kroz fizičke ili psihičke napade, cyber bullying se odvija na mentalnom planu kao vrsta psihološkog šikaniranja koja se manifestuje kroz slanje uznemirujućih, ponižavajućih, uvredljivih i neprikladnih poruka ili sadržaja. Napadi ovog tipa mogu

24 Izvor http://www.aic.gov.au/events/aic%20upcoming%20events/2011/~/media/conferences/2011-studentforum/alice_hutchings.pdf, pristupano 22.11.2011

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

26 **Kamil Kopecký**, S**talking a kyberstalking nebezpečné pronásledování**, studie Olomouc, 2010 Izvor: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=9%3Astudie-o-stalkingu-a-kyberstalkingu 22.11.2011

biti toliko intenzivni i ponavljajući da žrtva može da doživi mentalni slom, a posledice mogu da dovedu i do samoubistva[27] [26]. I ovaj oblik krivičnih dela takođe se realizuje putem informaciono komunikacionih tehnologija na već opisan način;

Realizacija ove vrste kriminala vezane za dela protiv ličnosti uglavnom prolazi kroz 4 faze prema sledećem scenariju:

„*Prvo se **identifikuje i locira** žrtva, sledeći korak je **uspostavljanje kontakta** sa žrtvom što za cilj ima **prikupljanje svih relevantnih informacija** potrebnih napadaču da bi sproveo **uznemiravanje** odnosno krivičnu radnju.*"

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[28] prevare kroz sajtove za upoznavanje[29]

27 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

28 Clickjacking predstavlja tehniku prevare web korisnika iskorišćavajući neki sigurnosni propust na sistemu ili iskorišćavajući ranjivost nekog web pretraživača sa ciljem otkrivanja poverljivih informacija ili prezuzimanja 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 omogućivalo 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).

29 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

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 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 zlonamerne programe (npr. programski kod, skripta, aktivni sadržaj[30]) 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[31]: logičke

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.

30 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. Izvor : http://windows.microsoft.com/sr-Latn-CS/windows-vista/What-is-active-content-and-why-does-Internet-Explorer-restrict-it, 01.03.2012

31 John Aycock, Computer Viruses, and Malware , Springer , Canada, 2006, Strana 11-18

bombe[32] (eng. logic bomb), trojanski konji[33] (eng. trojan horse), zadnja vrata[34] (eng. backdoor), virusi[35] (eng. virus),

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

33 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 da se kradu 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.

34 *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).*

35 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. briše sve podatke sa neke particije, ali oni nisu virusi. Činjenica 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*

crvi[36] (eng. worm), zečevi[37] (eng. rabbit), spajveri[38] (eng.

virusi mogu biti detektovani i uklonjeni antivirusnim ili antimalware programima.

36 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 email 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.

37 Rabbit predstavljaju posebnu podgrupa crva. Naziv je dobijen po tome što mu je glavna osobina neverovatno brzo umnožavanja. Postoje dve vrste ovih rabbita. Prva zapravo predstavlja program koji pokušava do potroši sve sistemske resurse kao naprimer 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).

38 *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 primer 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 gra-

spyware), adveri[39] (eng. adware), hibridi[40], kapalice (eng. droppers) i zamke[41] i zombiji[42] (eng. zombies) [28].

fički 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.*

39 Adware ili oglašivački softver ima velike slličnosti sa spajverom iz razloga što obe vrste programa se 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 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 podatka 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 uslovim što prouzrokuje instaliranje i adware programa. Često dolazi sa integrisanim spajverom ili drugom 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.

40 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 malvare 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.

41 Dropper ili kapalica je program koji sadrži neku zlonamernu komponentu koji je dizajniran da »instalira« neka vrstu malvare-a (virusa, spajvera, backdoora, itd) na određenom sistemu. Dropper može biti samostalan ili izveden iz dve faze. Kod samostalan dropperera 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.

42 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

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*.[26][43]" 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 [27]. 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 bio reči u prethodnom delu

izblokirati računar sa kog se to pokušava prostim prekidom konekcije sa tim računarom. 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 istakao bih i činjenicu da je veliki broj instalacija operativnih sistema ostala na onoj osnovnoj formi (sveža instalacija) bez instaliranja sigurnosnih zakrpa (eng. patch) i kao takva postaje podložna napadima crva, što govori o ozbiljnosti ovog problema. Koliko je jedan takav operativni sistem, bez instaliranih sigurnosnih zakrpa ranjiv, biće prikazano u PRAKTIČNOM DELU RADA U POGLAVLJU $$$. 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.

43 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

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 da ima nanošenje velike štete kako kompaniji tako i pojedincu, ali i državi.

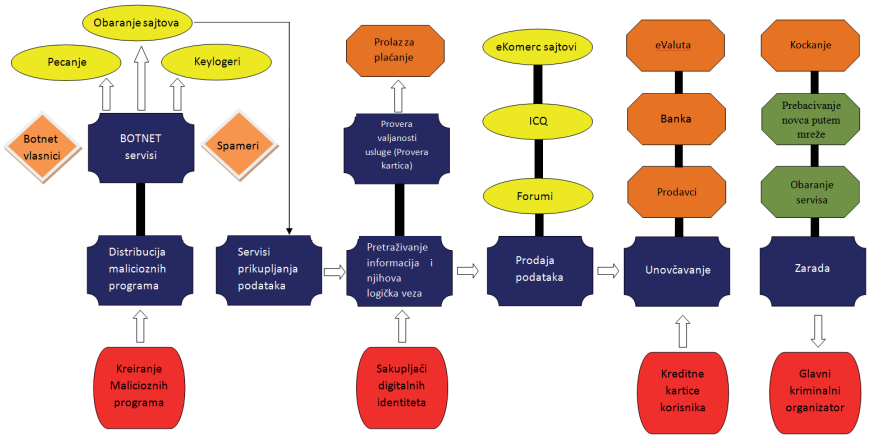
Kada je reč o visokotehnološkom kriminalu u Srbiji reč, on uglavnom obuhvata široku lepezu pojavnih oblika i najčešći slučajevi su neovlašćen pristup računarima, računarskoj mreži ili bazama podataka, pravljenje i unošenje (širenje) računarskih virusa (kako bi se prikupili podaci o platnim karticama), 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 onemogućivanje 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 bavi 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 biti VIP korisnik da biste našli 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[44].

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 zemlje 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 postoji više servera nego stanovnika, i onda odatle deluju ti kriminalci 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

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

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, ali i reorganizacijom državnih organa (Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[45]). 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. [12]. U Okružnom javnom tužilaštvu u Beogradu 2005. godine je osnovano **posebno odeljenje za borbu protiv visokotehnološkog kriminala ali je od** 1. januara 2010. godine ovo odeljenje ukinuto. Procesuiranjem dela visokotehnološkog kriminala bave se dva zamenika višeg javnog tužioca u Beogradu koji su specijalizovani za ovu oblast.

Prethodno navedene informacije o visoko tehnološkom kriminalu su veoma važne i moraju se shvatiti krajnje ozbiljno ukoliko

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

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 produžuju postupci, zbog same prirode digitalnih dokaza, koji iziskuju brzinu i sposobnost, da se za veoma kratko vreme spasu digitalni dokazi i identifikuju 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.

2.2 Zakonska regulativa visokotehnološkog 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[46]), sa svojim izmenama i dopunama u 1986, 1988, 1989 i 1990. godine. 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 pravnu komponenta i mogućnost vođenja građanskog parničnog postupka[47].

U Australiji je 1989 godine je izmenjen i dopunjen „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. [48] Takođe u Holandiji 1993. Godine usvojen je Zakon o računarskom kriminalu. Mnoge međunarodne organizacije su takođe donele preporuke u vezi sa izmenama zakonodavstava u vezi sa sprečavanjem računarskog kriminala. Na primer, Ujedinjene nacije su se bavile ovim problemom na VIII kongresu UN o sprečavanju zločina i postupanju sa delinkventima, 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 te obrazovanja i stručnog usavršavanja službenika državnih organa koji se

46 Izvor: http://www.panix.com/~eck/computer-fraud-act.html

47 Građansko pravo daje oštećenoj strani priliku da podnese tužbu protiv prekršioca, kako bi dobili nadoknadu za učinjenu štetu.

48 Eoghan Casey, Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet, Second Edition, Academic Press 2004, poglavlje 2, strana 19.

s njim susreću, razrada pravila profesionalne etike o postupanju sa kompjuterizovanim informacionim sistemima, te unapređenje svih oblika zaštite računarskih delatnosti.[49]"

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 Enforcement Center (FLETC), and National White Collar Crime Center (NW3C)", pokrenuli su inicijativu za sprovođenje programa treninga za agencije reda i zakona [7].

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 [50].Prema tom zakonu za krivično delo se smatra svako slanje komercijalnog e-maila sa lažnim ili obmanjujućim zaglavljima poruke ili obmanjujućim naslovom poruke. U Americi, Ministarstvo pravde je obrazovalo posebno odeljenje nadležnoe za krivično gonjenje digitalnih zločina počinjenih od računarskih i internet korisnika pod nazivom "Odeljenje za Internet zločine i intelektualnu svojinu"[51].

Kada je reč o Evropi, prema profesorima Mirjani Drakulić i Ratomiru Drakulić možda najznačajnija aktivnost kojom se pokušava operacionalizovati saradnja u borbi protv visoko tehnološkog kriminala je formiranje EU Foruma [75] 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[52].

49 Vladica Babić, Kompjuterski kriminal, RABIC, Sarajevo, 2009, str. 71

50 htpp://www.spamlaws.com/federal/can-spam.shtml

51 The Computer Crime and Intellectual Property Section (CCIPS). Videti na http://www.cybercrime.gov/crimes.html

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

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 je 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 a 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.

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 vi-

sikotehnološkim 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 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 podatke 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.

Znači zakonodavni okvir u zakonodavstvu Republike Srbije koji se odnosi na obezbeđivanje i pružanje krivično pravne 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.

2.3 Visokotehnološkog kriminal - primeri iz prakse

Da bi se stekao bolji uvid u razmere specifičnosti i težinu 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 sistema 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 krađa programa i 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. 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 koji je ovaj crv izazvao na oko 1.2 milijarde dolara[53].

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[54].

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.[55] Organizovani kriminal, odnosno terorističke grupe, pornografske i pedofilske mreže, grupe za ilegalna trgovina oružija, 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.

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 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 koji se dešavaju kod nas i u okruženju.

53 http://malware.wikia.com/wiki/Slammer, 12.9.2011

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

55 Koliko je „moderni" visokotehnološki kriminal opasan, može se videti iz napada koji se desio u februaru 2007. godine, kada su 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.).

Primer 1 [12]

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 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 [12] 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 ona odabira parametri iz menija bankomata oni joj neprimetno podmetnu neku novčanicu ili papir da izgleda kao da joj je nešto ispalo. Paralelno prate šta on kuca i fokusiraju se da zapamte pin tj. taj

četvorocifreni broj. Čim ga ukuca obraćaju joj se da joj kažu da joj je nešto ispalo. U momentu kada se ona savije da podigne tu podmetnutu novčanicu oni za to vreme izvlače karticu i beže. U tom momentu on 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 bankomati 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) (za sada nije bilo primera u Srbiji), predstavlja redirekciju sa nekog sajta. Ukoliko ste pristupali 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 tv 42" samo 100 evra). Oni daju primamljivu ponudu i 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 [56].

56 Socijalni inženjeringa 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.

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 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 poboljšanje 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 koja god 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 kancela-

rija 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 je moguće naći i Bluetothova 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 100 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 100 evra. Sledeći korak je da dobijate mail u kome se kaže da ste slučajnim izborom sistema dobili nagradu od 100 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 Mađarsku u Budimpeštu, uzeli mu pasoš, i rekli mu da će ubuduće raditit 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. Tipična manifestacija protivpravne imovinske koristi. To su uglavnom lica mlađeg starosnog doba 20-30 godina. Pripada jednom organizovanom obliku kriminala na internetu i mimo interneta gde svako ima određenu ulogu.

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 $[57]

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[58].

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 počinjena preko interneta na zatvorsku kaznu od 6 meseci uslovno, zato što su od januara 2007 do jula 2007.g. 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[59].

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

57 Izvor : http://www.justice.gov/criminal/cybercrime/ferrisPlea.pdf

58 Dr Dragan Prlja, Sajber criminal, Pravni fakultet Univerzitet Union, http://www.prlja.info/sajberkriminal.pdf, 30.04.2012

59 Dr Dragan Prlja, Sajber criminal, Pravni fakultet Univerzitet Union, http://www.prlja.info/sajberkriminal.pdf, 30.04.2012

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 računar neovlašćeno preledao sadržaj njihove elektronske pošte [60].

Kada je u pitanju visokotehnološki kriminal digitalna forenzika je jedan od najznačajnih faktora u procesu otkrivanja istine o protiv pravnim aktivnostima na osnovu svojih otkrića i rezultata. Jer upravo njeni rezultati su ti koji pokazuju kako se neka protivpravna aktivnost desila npr 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 i novih tehnologija i njenih primena u zlonamernu svrhu na drugoj strani i dalje traje.

60 Dr Dragan Prlja, Sajber criminal, Pravni fakultet Univerzitet Union, http://www.prlja.info/sajberkriminal.pdf, 30.04.2012

3. ISTRAŽNE METODOLOGIJE

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 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 [33].

Cilj metodologije i tehnologije računarske forenzičke analize ja da obezbede pouzdano čuvanje digitalnih podataka, oporavak izbrisanih podataka, rekonstrukciju računarskih događaja , odvraćanje napadača, generisanje dobrih forenzičkih alata i procedura[61].

Svrha definisanja modela digitalne istrage je da informiše, oblikuje, i standardizuje proces digitalne istrage[62]. 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 u radu prilaze digitalnoj istrazi sa naučno-tehničkog aspekta, a neki sa ne-tehničkog aspekta. Takođe neki od prikazanih modela su detaljniji u odnosu na druge po pitanju korespodencije 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.

61 Slobodan Trivić, Virtuelni zločin i njegovo sankcionisanje, Strani pravni život, br 3/2011, str. 300-311

62 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

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. Kao rezultat istraživanja u nastavku bih izložio 10 najvažnijih tipova modela :

3.1 The DFRWS model

DFRWS model razvijen je između 2001 i 2003[63] pri digitalnoj forenzičkoj istraživačkoj radionici (eng. Digital Forensics Research Workshop) razvijena od strane grupe istraživača i stručnjaka iz digitalno forenzičkih oblasti [31]. Ovim modelom su obuhvaćene digitalno istražne radnje definisane klasama. Te klase ustvari 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 elementa predstavljeni su u tabeli 1. [64]:

63 http://www.dfrws.org/2001/dfrws-rm-final.pdf, 18.12.2011
64 http://www.dfrws.org/2001/dfrws-rm-final.pdf, strana 17, 18.12.2011

1	2	3	4	5	6	7
IDENTIFICA-TION	**PRESERVA-TION**	**COLLEC-TION**	**EXAMINA-TION**	**ANALYSIS**	**PRESENTA-TION**	**Decision**
Event/Crime Detection	**Case Manage-ment**	**Preserva-tion**	**Preservation**	**Preserva-tion**	Documen-tation	
Resolve Signature	Imaging Technologies	**Approved Methods**	**Traceability**	**Traceability**	Expert Testimony	
Profile Detection	**Chain of Custody**	Approved Software	Validation Techniques	Statistical	Clarification	
Anomalous Detection	**Time Synch.**	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement	
Complaints		**Legal Aut-hority**	Pattern Matching	Data Mining	Recommen-ded Coun-termeasure	
System Moni-toring		Lossless Compre-ssion	Hidden Data Discovery	Timeline	Statistical Interpreta-tion	
Audit Analysis		Sampling	Hidden Data Extraction	Link		
		Data Reduc-tion		Spatial		
		Recovery Techniques				

Tabela 1. DFRWS model digitalne istrage

3.2 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 [65][33]:

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.

65 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 [32]. Ovaj model predstavlja jedan apstraktni model koji može da se primeni na bilo koju tehnologiju ili vrstu visokotenološkog kriminala za različite tipove incidenata. Ustvari njegov značaj je da se on iskorisiti kao osnova za razvoj detaljnijih metode 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 digithnologije
- 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 kategoriju mogu biti previše uopštene za praktičnu primenu
- nema lakog načina za testiranje ovog modela
- svako dodavanja podkategorija ovom modelu učiniće ga težim za korišćenje.

Model nije isticao značaj lanca očuvanja (eng. chain of custody) već se u njemu samo navodi da ukoliko je lanac očuvanja jak, on će se održati tokom trajanja istrage.

3.3 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[66]. Koraci ili faze u ovom

66 Vodopad način istrage podrazumeva da aktivnosti prate jedna drugu u nizu.

modelu definisani su kao aktivnosti. Ovaj model se realizuje kroz sledećih 13 koraka tj. aktivnosti[67] [34]:

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 drugim 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.

67 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

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 i 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.

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 formalna izveštaj koji je namenjen menadžmentu kompanije.

11. **prezentovanje hipoteze** - hipoteza biti prezentovana i trećim licima odnosno nadležnim organima osim istražiteljima. Kada je u pitanju policijska istraga hipoteza se predstavlja sudu, a u slučaju kompanijske istrage predstavalja 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"[68] [36] 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 [35] 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.

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

3.4 The Beebe i Clark model

Model Bebbe i Klark[37] 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 koje utiču na povećanje dostupnosti digitalnih dokaza kao podrška detekciji, odgovoru na incident i krivičnoj istrazi visokotehnološkog kriminala. Cilj ove faze je postavljanje organizacije u forenzički spreman položaj [38].

2. **Odgovor na incid**ent - 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 opovrgnu sumnje u vezi sa protivpravnim aktivnostima. Takođe može dati odgovore na pitanja u vezi sa rekonstrukcijom događaja (ko, šta, gde, kada i kako).

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.

3.5 Kruse i Heiser model

Kruse i Heiser u svom modelu predstavljenom 2002, navode da se proces forenzičke istrage sastoji iz 3 koraka [39]:

1. dobijanje dokaza (eng. acquiring)- podrazumeva rukovanje dokazima, prikupljanje dokaza, identifikovanje i označavanje dokaza, transport dokaza, skladištenje dokaza, uz poštovanje lanca očuvanja dokaza i 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 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 (bit stream) programima čime se dobija forenzički bekap odnosno klon originalnog diska. Ovo je jako važno napomenuti jer

normalan bekup ne kopira obirsane fajlove i određene delove hard diska koji mogu sadržati informacije od velike važnosti za digitalnu istragu. Sa analizom početi nakon pravljenja hash vrednosti image-a hard diska koji će se analizirati, i izvršiti dokumentovanje. Obavezno je nad svim pronađenim digitalnim dokazima održati lanac očuvanje digitalnih dokaza (eng. chain of custody) kao i očuvanje njihovog integriteta. 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.

3.6 America's department of justice - DOJ model

Ovaj model (DOJ model[69])je predložilo američko pravosuđe 2001. godine u "Vodiču za istragu digitalnog mesta krivičnog dela" (eng. Electronic Crime Scene Investigation Guide)[40] 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 – ovoj fazi vrši se pretraga i prikupljanje elektronskih dokaza koje se realizuje kroz sledeće podaktivnosti : obezbeđenje mesta krivinog dela[70], dokumentacija mesta krivičnog dela[71] i sakupljanje dokaza[72];

ispitivanje - obezbeđuje prepoznavanje dokaza objašnjavajući njegovo poreklo i značaj kao i pregled skrivenih i nejasnih informa-

69 https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

70 Obezbediti mesto krivičnog dela radi bezbednosti lica i integriteta podataka kao i zbog identifikacija potencijalnih dokaza.

71 Podrazumeva se dokumentovanje fizičkog opisa mesta krivičnog dela, kao na primer fotografisanje računara

72 Podrazumeva konfiskovanje računarskog sistema ili pravljenje kopije podataka na forenzičkom sistemu

cija 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 da 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.

3.7 Lee model

Henry Lee zajedno sa svojim kolegama je 2001 godine predstavio model koji sistematično i metodično fokusiran samo na jedan deo forenzičke istrage (što predstavlja ograničenje ovog modela), odnosno ne dotiče se radnji kao što je sticanje, priprema i prezentovanje dokaza i orijentisan je ka fizičkom mestu krivičnog dela. Sastoji se od 4 faze [29][73]:

-**prepoznavanje** - prepoznavanje potencijalnih dokaza i njihovo selekcija na one koji imaju dokaznu vrednost i na one koji to nemaju. Ovde postoje dve podfaze: prikupljanje sa dokumentovanjem i očuvanje fizičkog mesta krivičnog dela, a pristup je omogućen samo ovlašćenim licima (istražnim organima, forenzičarima). Mesto zločina se dokumentuje fotografisanjem, skiciranjem i snimanjem video snimaka. Sobzirom da se dokazi prikupljaju za kasniju analizu treba ih dokumentovati jasno i potpuno .

-**identifikacija** - u ovoj fazi vrši se identifikacija očiglednih delova dokaza i dokaza koji su prolazni - kratkotrajni (pljuvačka, krv, sluz) od strane istražitelja. Takođe identifikovanje različitih vrsta dokaza podrazumeva i njihovu klasifikaciju . Kao podfaza pojavljuje se poređenje odnosno proces upoređivanja pribavljenih dokaza sa poznatim klasnim karakterisitkama objekta tj. standardnim.

-**individualizacija** - je svojstvena forenzičkoj nauci i odnosi se na dokazivanje jedinstvenosti određenog uzorka (predmetnog doka-

73 Henry Lee, Timothy Palmbach, and Marilyn Miller. Henry Lee's Crime Scene Handbook, Academic Press, 2001, strana 272-277

za) tako da može biti povezan sa pojedincem ili događajem. Objekti ili materijali pored klasnih karakteristika poseduju i individualne karakteristike. Individualne karakteristike objekata ili materijala su upravo one jedinstvene osobine na osnovu kojih se razlikuju članovi koji pripadaju istim klasama.

-**rekonstrukcija** - predstavlja proces objedinjavanja kako informacija iz prethodnih faza procesa tako i sve druge relevantne informacije koje su istražitelji dobili da bi se obezbedio detaljan opis događaja i radnji koje su u vezi sa protipravnom aktivnošću. Podrazumeva sledeće korake koji će postaviti bazu za rekonstrukciju izvršenja protivpravnog akta: prikupljanje podataka, pretpostavka, formulisanje hipoteze, testiranje hipoteze, formiranje teorije. Sve ovo vodi ka izveštavanju i prezentaciji.

Ovaj model omogućava kompletnu dokumentaciju mesta zločina i koristi iskustvo istraživačkog organa da bi se došlo do relevantnih dokaza.

3.8 Model "Odgovor na incident"

Prosise i Mandia su 2001. godine predstavili digitalno istražni model "Odgovor na incident" [45][46]. Ova metodologija je adekvatna za korporacijski model istrage i fokusirana je na incidenti odgovor kada su u pitanju kritični sistemi koji mogu biti kompromitovani. Model se sastoji od sledećih 11 faza :

-**priprema za incident** - podrazumeva organizovanje obuke IT kadra u okviru organizacije i nabavka neophodne infrastrukture

-**detektovanje incidentne radnje** - identifikacija sumnjive radnje

-**inicijalni odgovor na incident** - u ovoj fazi se vrši potvrđivanje da se desila incidentna radnja i skupljaju se nestabilni dokazi tj. lako promenljivi dokazi (dokazi, odnosno podaci koji mogu lako da se izgube na primer podaci i RAM memorije)

-**izrada strategije za odgovor na incident** - određivanje odgovora na incidentnu radnju u skladu sa poznatim činjenicama

-**duplikacija** - pravljenje bekapa, odnosno mirror postojećeg sistema

-**istraga** - istraživanje sistema da se identifikuje ko, zašto i na koji način se realizovala incidentna situacija

- **realizacija sigurnosnih mera** - ova faza podrazumeva izolovanje sumnjivog sistema.

- **posmatranje mreže** - ova faza podrazumeva posmatranje mreže radi potencijalne detekcije novih odnosno ponovljenih napada

- **oporavak** - vraćanje sistema u njegovo originalno stanje sa pridodatim merama zaštite

- **izveštavanje** - podrazumeva izradu dokumentacije u vezi sa odgovorom na incidentnu radnju

- **revizija** - razmatranje odgovora i prema potrebi adekvatno prilagodjavanje

3.9 Eoghan Casey model

Casey model je predstavljen 2000. godine [41][44] 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 istraživačima principe na osnovu kojih može da se formira argumentovana hipoteza koja je zasnovana na činjenicama uzimajući u obzir pravni kriterijum za prihvatljivost. Ti pricipi su sledeći [42]:

-**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 potrepljena

-**ponovljivost**- postupak je nezavistan prostorno i vremenski i može se ponoviti

-**integritet** – postojanje mogućnosti provere neporemenjenosti stanja dokaza

-**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 [42]:

- **optužbe 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 aktiivnosti 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 kompromitovanje 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 je 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 detaljno detaljno dokumentovanje i obrazloženje svake sprovedene aktivnosti. Dokumentacija je prisutna u svim fazama istražnog postupka ali je pri konfiskovanju digitalnih dokaza najvažnija zbog uspostavljanja lanca nadležnosti i autentičnosti samih zaplenjenih dokaza. Na primer, fotografisanje i snimanje serijskih brojeva, predmeta, dokumentovanje ko je rukovao dokazima, pomaže da se prati kretanje dokaza nakon prikupljanja. U tu svrhu postoje obrasci i definisane procedure koje pomažu da se u 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"[74] koja mogu da se izgube nakon zaplene ili nestabilnosti elektronskih uređaje (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 saobraćaj, 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

74 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.

nimalo lak zatadat. Da bi se proces zaplene što efikasnije sproveo publikovani su i vodiči u kojima su dati praktično saveti i principe koju su od koristi onima koji se bave digitalnim dokazima. Jedan od njih je "*Electronic Crime Scene Investigation: A Guide for First Responders*"[75] publikovan od strane US *Department of Justice 2001. godine u USA*. Drugi 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 [76]. Dokumenti su veoma korisni u smislu razvijanja standradnih operativnih procedura[77] i može da omogući izvođenje jednostavnijeg tipa istrage sa manjim brojem računara (do 5). Što je bolje utrenirano i obučeno osoblje koje prvo odgovara na incident veće su šanse da se pronađe veliki broj dokaza i da se konfiskuju predmeti koji sadrže veliki broj relevantnih informacija.

-čuvanje - 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 krivčnom 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 prave 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.

75 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 osobllju koje prvo odgovara na incident, dostupno na adresi https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

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

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

-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. Isključivo raditi na forenzičkim kopijama originalnih digialnih dokaza dobijene iz faze čuvanja[78]. 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 od strane počinioca ukoliko je konkretan dokaz pronađen ili snimljen.

- 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 ili izgledaju da su u vezi sa relevatnim činjenicama iz slučaja. Ovo je faza gde konkretne činjenice dobijaju oblik koji potvrđuje ili opovrgava hipotezu izgrađenju od strane istražnog tima. Na primer ukoliko se radi o optužbi koja ima 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 rootkit alatima, 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.

78 Osim u izuzetnim slučajevima kada su u pitanju ugrađeni sistemi (eng. embedded systems).

- **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 (hash ili checksum vrednosti) ili tipova podataka, ne uzimajući u obzir sadržaj ili kontekst. Kriterijum na osnovu kog se vrši eliminisanje određenih podataka izuzetno je 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 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 - analizi

-analiza - ova faza podrazumeva vrlo detaljnju pretragu padataka koji su identifitikovani 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 padfaze :

-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 - 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) su prikupljeni iz mnogih izvora (digitalni i nedigitalnih). Sami za sebe podaci (informacije) ne mogu da prenesu priču o istraživanom događaju, već moraju da se fuzionišu da bi se sklopila celan priča. Primer fuzije može predstavljati vremenski okvir nekog događaja ili radnje koji se odnosi na određeni slučaj odnosno incident. Svaki zločin 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. 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 protokolaekojih su se istražitelji pridržavali, metode prilikom konfiskacije, dokumentacija, kolekcija, čuvanje, oporavak, rekonstrukcija, organizovanje i pretraga ključnih dokaza. U izveštaju potrebno je pokloniti 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.

3.10 Carrier i Spafford model

Carrier i Spafford model je predstavljen 2003. godine [47]. Ovaj model posmatra računar kao mesto zločina i naziva ga digitalno mesto krivičnog dela u kojoj 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 intervetnog ili forenzičkog tima. Ovaj model sastoji se iz 17 podfaza organizovanih u pet faza :

- **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, 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 mogu da 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.

-**razvojna faza** - je odgovorna 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 incidentu radnju i preduzima potrebne aktivnosti kako bi proverili da li je sistem kompromitovan (nadgledanje mreže u potrazi za sumnjivim aktivnostima, pretraživanje po sistemu radi pronalaženje

rootkit programa ili drugih exploit alata). Bitno je naglasiti da ukoliko se analiza sprovodi "uživo", prema sistemu 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[79].

Faza istrage fizičkog mesta krivičnog dela [80] - u ovoj fazi se vrši prikupljanje i analiza fizičkih dokaza i vrše se rekonstrukcija događaja koji su doveli do incidentne radnje. Kao najvažniji cilj digitalno 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 veći broj 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 :

-**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 vezana 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 ustvari 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

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

80 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.

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 faza podrazumeva pretragu za dodatnim medijima i

digitalnim uređajima na mestu zločina. Ova podfaza 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, se šalju 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.

- **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. Napomenuo bih 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 da budu organizovane u primarna i sekundarna mesta, što omogućava analizu različitih tipova uređaja na različitim mestima [29]. 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 očuva-

nje 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 jedno 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 podiži 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 njegovu istoriju. U zavisnosti od veštine osumnjičenog za protivpravne aktivnosti istražitelji će izvršiti procenu potrebnih tehnika koje će primeniti istrazi. Moguće je i dodatno konsultovanje ili angažovanje eksperata iz kriptografskih oblasti, eksperte za oporavak podataka (ukoliko su određeni podaci obrisani ili nestali), eksperte 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 [48]. 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 hash funkcije kao na primer MD5 ili SHA-1, nad dokazima da se dobije heš vrednost koja dokazuje integritet [49]. Da bi dokazi mogli da se koriste na sudu u ovoj fazi vrši se kreiranje lanca neprekidnog očuvanja i nadzora dokaza (eng. chain of custody).

-**podfaza akvizicija** - predstavlja vremenski najzahtevniju fazu, podrazumeva detaljnu digitalno forenzičku analizu sistema radi pretrage i prikupljanja digitalnih dokaza. Koristi rezultate iz faze Pretraga da bi tipski fokusirala analizu. Na primer pretraga se može vršiti prema ključnoj reči ukoliko su one identifikovane iz drugih dokaza. Nealocirani prostor na fajl sistemu je 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).

-**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 koje 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.

-**kontrolna faza** - predstavlja fazu pregleda stanja istrage sa ciljem identifikovanja oblasti koja bi mogla 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 drugi 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 [43][81]. 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.

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

4. DIGITALNA FORENZIKA RAČUNARSKIH SISTEMA

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 istraga predstavlja proces gde se razvijaju i testiraju hipoteze koje odgovaraju na pitanja o digitalnim događajima. Digitalna istraga se vrši upotrebom naučne metode uz pomoć koje se razvija hipoteza i to korišćenjem dokaza koji su otkriveni. Zatim se testira hipoteza pretraživanjem dodatnih dokaza koji su u kontradiktorni u odnosu na hipotezu. Digitalni dokaz je digitalni objekat koji sadrži pouzdane informacije koje podržavaju hipotezu ili je opovrgavaju[5][82].

Veliki broj literature u svetu bavi se temom digitalnih dokaza, odnosno izjednačavanja pravne snage elektreonskih dokaza (uključujući e-mail poruke) i papirnih dokaza i dokaza u drugim formama. Mišljenja su različita kod zapisa koje računari generišu bez uticaja čoveka, ali su jedinstvena kada su u pitanju zapisi koji se samo arhiviraju na računaru, a proizvodi ih čovek. Ova druga vrsta zapisa faktički sadrži "rukopis" jedne ili više osoba koji je u elektronskoj formi i ima se smatrati orginalom. Primeri takvih zapisa su e-mail poruke, poruke u internet diskusionim grupama [59].

Kada je reč o elementima računarskog i Internet kriminala, njih predstavljaju protivpravne aktivnosti počinilaca zajedno sa okolnostima pod kojima je to delo počinjeno.

Digitalna forenzička istraga predstavlja proces koji korišćenjem naučnih metoda i tehnologije analizira digitalne uređaje, razvija i testira teorije, koje predstavljaju relevantan dokaz u sudskom postupku. Cilj takve istrage je utvrđenje istine i svih okolnosti u vezi sa počiniocem i načinom izvršenja krivičnog (prekršajnog dela).

82 Ugljesa Georgijevic, ISTRAzNE METODOLOGIJE, TEHNIKE I ALATI ZA DIGITALNU FORENZIčKU ISTRAGU, singidunum 2010. Strana 9

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 **o**bezbeđuje jedini pouzdani alat za istragu računarskog kriminala, akviziciju i analizu digitalnih podataka i pripremu i prezentaciju digitalnih dokaza pred sudom. 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 [1].

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.

I upravo ta brzina tehnološkog razvoja utiče 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, uslovili su i specijalizovanje stručnjaka za različite oblasti. U najširem smislu digitalnu forenziku možemo podeliti na forenziku raču-

narskih sistema, forenziku mobilnih uređaja, forenziku baza podataka i forenziku računarske mreže uključujući i Internet ili kibernetička forenzika[83]. 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).

Digitalna forenzika ima široku primenu i to od policijsko-sudskih i vojno-obaveštajnih aktivnosti, civilnog i bankarskog sektora i osiguravajućih društava i 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[84].

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 [3][4].

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

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

84 Dragan Prlja, Sajberkriminal, predavanje održano na Pravnom fakultetu Univerziteta u Beogradu, 28.12.2008: http//www.prlja.info/sk2008.pdf

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.

U literaturi neretko 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.

4.1 Digitalna istraga

Digitalna istraga podrazumeva prikupljanje činjenica i njihovu proveru, zatim 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 predstavlja 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 [85](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 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 kojima se pričinila protivpravna aktivnost, utvrđuje motiv protivnpravne aktivnosti, definiše tip kriminala i procesuira ga.

korporativna istraga (zaposleni koji koriste resurse kompanije za ličnu upotrebu osim što troše vreme organizaciji i njene resurse već i krše politiku organizacije. Takvi zaposleni treba da budu prona-

85 Pod uslovom da su isti usklađeni sa pozitivnim propisima.

đeni i edukovani o politici orkganizacije. Ukoliko se problem nastavi preduzeti određene disciplinske mere)

Potrebno je istaći i značaj informacije o cilju napada ali i utvrditi eventualno postojanje uzročno-posledične veze (direktne ili indirektne) sa ostalim kumulativno 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. 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. Takođe biće opisani najvažnije metodologije odnosno modeli forenzičke istrage. U literaturi modele, koje možemo pronaći 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 koristi da bi pronašla digitalne dokaze [47].

Kada je u pitanju istraga fizičkog mesta krivičnog dela dominantna teorija je Lokardov zakon razmene [16]: Kada dva objekta

dođu u interakciju (kontakt) doći će do razmene materije između njih. Primer dlake sa zločinca vrlo često se zadrže na fizičkoj 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 sitema 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 bih izneo 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 [29].

-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 sekukndarna 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 o potencijalnih napada i špijunaže (kao jedan od pojavnih oblika visokotehnolokog 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 računasrkog 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 razvoja 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 razvoj tehnologije i sajber kriminala. Prikupljanjem 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 su 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. Skrenuo bih pažnju 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[86]) je objavila vodiče za trening "Najbolje prakse računarske forenzike"[87] [65]. Američko udruženje direktora laboratorije za zločine - ASCLD (eng. American Society of Crime Laboratory Directors) je predložila 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 više nivoiska sertifikacija [5]:

1. Ispit opšteg znanja (koji svi moraju da prođu, uključujući i osoblje koje prvo odgovara na incident, a koje rukuje digitalnim dokazima)

86 Working Group for Digital Evidence

87 Best practices for Computer Forensics

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.

4.2 Digitalni dokazi

Veoma važan datum za digitalnu forenziku kao mladu naučnu disciplinu je 1991. godina. Naime u Portlandu (država Oregon) te godine održano je zasedanje Međunarodne asocijacije računarskih naučnika IACIS[88]gde konstatovano i odlučeno da su „digitalni dokazi" ravnopravni sa dokazima prikupljenim na tradicionalan način, odnosno fizičkim predmetima [10].

Prema SWGDE/IOCE[8990] standardu dokazi su klasifikovani u tri osnovne kategorije[11][91]:

-**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.

88 IACIS – International Association of Computer Specialist

89 Scientific Working Group on Digital Evidence (SWGDE) http://www.swgde.org/

90 International Organization on Digital Evidence (IOCE) http://www.ioce.org/core.php?ID=1

91 Michael cross, Scene of the Cybercrime, Second Edition, syngress, 2008, strana 628.

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 [14].

Naveo bih 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.

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 ROMu, FD, mempriji, itd.).

Kopija digitalnog dokaza je precizna reprodukcija informacija koje su sadržane na originalnom fizičkom predmetu, nezavisno od originalnog fizičkog predmeta.[92]

-Analiza uživo - predstavlja analizu koja se sprovodi nad originalnim dokazima

-Off-line analiza - analiza koja se sprovodi nad forenzičkom slikom originalnog dokaza

-dokazni tragovi - fragmenti informacija koji se mogu naći u slobodnom ili slek prostoru.

Postoji nekoliko načina izrade kopija i duplikata digitalnog dokaza korišćenjem specijalnih programa za te namene:

- Kopija (eng. *Copy*): uključuje samo informacije o datotekama iz fajl sistema, ne i o *slack* ili neiskorišćenom prostoru i nisu očuvane vremenske oznake.- KLASIČNA COPY Funkcija koja ne zadovoljava zahteve DF istrage
- Rezervna kopija (eng. *Backup*): datoteke kopirane za buduću restauraciju, služe kao sigurnosna kopija – **Takođe ne** zadovoljava sve zahteve DF istrage. To je miror kopija.

Mirror kopija: ovaj način očuvanja dokaza zasniva se se na metodi kopiranja svih podataka na disk (eng. *capture*), kako bi se stvorila neinvazivna kopija (eng. *mirror image)* kopiranog diska. *Mirror image* može, ali i ne mora predstavljati identičnu kopiju originala zbog toga što se ona najčešće koristi kao sigurnosna kopija (eng. *backup*), a u složenijim situacijama *mirror image* ne tretira se kao forenzička kopija.

- Slika (eng. *Image*): npr. *ISO image* kopija datoteka kompletnog diska kreirana zbog dupliciranja ili restauracije sistemskih i aplikativnih programa
- Forenzička kopija bit-po-bit ili *Bitstream* kopija: Egzaktna replika svih sektora

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

- (TO je forenzički duplikat originalnog HD i rad na njemu se smatra kao rad na originalnom računaru. Uzimaju se obavezno 2 forenzičke kopije – jedna radna i jedna refrentna za dokazivanje integriteta ispitivanog HD pred sudom)

Sektor-po-sektor kopija ili *bitstream kopija* predstavlja napredniju metodu reprodukcije podataka kopirajući svaki bit, jedince i nule, od početka do kraja, bez brisanja ili bilo kakve izmene nad podacima. Takođe se kopiraju i neiskorišćeni i nealocirani prostori na disku, zbog toga što se na njima često nalaze izbrisani podaci.

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.

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 koji 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. Ti digitalni dokazi su izuzetno nestabilni (osetljivi, lako promenljivi eng. volatile), jer mogu da se lako uklone ili izmene, što u dokaznom postupku može predstavljati veliki problem. Međutim ti dokazi 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 javi prilikom prikupljanja podataka su sledeće :

-izmena datumskih i vremenskih pečata (time and data stamps) (ZA GRUBORA kako bi to preveli lepše)

-zaustavljanje zlonamernih procesa na računarskom sistemu

-instaliranje zakrpa na sistemu (eng. patching) pre izvršene istrage nad sistemom.

-ne evidentiranje 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.

Ovde bih spomenuo i termin "lanac očuvanja nadležnosti" COC (eng. chain of custody - COC), a u literaturi se još može se naći i termin „kontinuitet dokaznog materijala", 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. 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 medja na drugi 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 načinu na koji je način dokazni materijal skladišten i zaštićen u laboratoriji za vreme ispitivanja.

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 fo-

renzički 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 nanete 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.

Istakao bih 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[93]-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*[94] (FBI[95], SAD), *X-Way Forensic*[96] (NPIA[97], Engleska) , *Paraben*[98] (BKA[99], Nemačka), kao brojni alati na Linux platformama otvorenog koda. Brayan Carrier je promovisao priznavanje alata otvorenog koda u svojim radovima. Mi nemamo zakon o digitalnom dokazu posebno, niti u sklopu nekog dugog zakona

Dakle, kod nas se preuzima ono što se u svetu prizna. Naše službe koje se bave digitalnom forenzikom koriste EnCase (prvi je naučno verifikovan sa preciznim brojem grešaka koje unosi u isipitivani

93 http://www.nist.gov/index.html, 30.04.2012
94 http://www.perlustro.com/, 30.04.2012
95 Federal Bureau of Investigation, http://www.fbi.gov/, 30.04.2012
96 http://www.x-ways.net/forensics/, 30.04.2012
97 National Policing Improvement Agency,http://www.npia.police.uk/, 30.04.2012
98 http://www.paraben.com/, 30.04.2012
99 BKA odnosno , Federal Criminal Police Office, http://www.bka.de/, 30.04.2012

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. Inače, isto bi pitanje bilo - koji tip detektora metala koristi kriminalistički tehničar za otkrivanje čaure sa mesta ubistva- što se nikada ne postavlja.

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.

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 pravno prihvatljiva iako 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[100][15].

Neophodno je permanentno praćenje noviteta na polju računarskih sistema što ujedno predstavlja i preduslov valjane akvizicije dokaza sa njih. Takođe bih primetio da je sa jedne strane primetan 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 [6].

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, 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).

Da bi se prikupile sve relevantne informacije i dokazi, bilo da su oni digitalni ili fizički, neophodno je izvršiti analizu ne samo ciljnog

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

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.

Kada računar postaje deo istrage ? Računar postaje deo istrage kada se na njemu ili sa njim izvrši neka protivpravna radnja. U prethodnom poglavlju pomenuo sam Lokardov zakon čiji je tvorac Edmond Lokard koji govori od tome da prilikom svakog kontakta dva objekta, postoji neka razmena materije, tj. svaki kontakt ostavlja trag [16]. 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 određenje dokaze u vezu sa izvršiocem.

Na osnovu pomenutog prinicipa razmene mogu se mogu biti proizvedeni digitalni dokazi koje možemo da svrstati sledeće dve kategorije [7] :

a. 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 [30] .

b. dokazi sa atributima koji pripadaju grupi individualnih karakteristika - pojedinačne karakteristike su jedinstvene i mogu povezati izvršioca ili aktivnost sa većom sigurnošću

Ustvari preko ovih 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, digital-

ni 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 je više odgovarajuće procesiranjem 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 fajl 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 hash vrednosti.

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 primenjije heširanje sa MD5 ili SHA algoritmom da bi sačuvao integritet (nepromenjivost) digitalnog dokaza. 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 može 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 (ZA GRUBORA), treba da radi u okviru svojih stručnih znanja i ovlašćenja i da dokumentuje bilo kakvu promenu na dokazu.

4.3 Uloga računara u kriminalnim aktivnostima

U periodu od 1994. godine do 1998. godine Ministarstvo pravde Sjedinjenih američkih država (eng. *US Department of Justice* - USDOJ) kreiralo je skup kategorija i na osnovu njih niz 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. (Pitati GRUBORA !!!!) 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. Te kategorije su sledeće [101]:

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

Ministarstvo pravde Sjedinjenih američkih država je 2002 godine je ažuriralo dokument tako da je u skladu sa današnjom tehnologijom i zakonom i 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"[102]. 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 [7]. Uputstvo ukazuje na to da čak i ako je sama informacija bila meta kriminalne aktivnosti može biti neophodno da se zapleni

101 http://www.irational.org/APD/CCIPS/toc1.htm#IV, 15.12.2011

102 http://www.justice.gov/criminal/cybercrime/searching.html, 15.12.2011

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 [29]. 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 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 protivpravne aktivnosti

U slučaju da je hardver odigrao značajnu ulogu u protivpravne 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 po-

sebno dizajniran da prisluškuje mrežu. Ovaj tip uređaja se koristi za prikupljanje šifri i drugih osetljivh informacija, koje se posle mogu zloupotrebiti (kao na primer neovlašćen pristup serveru, mrežnim resursima itd...).

Svrha zaplene instrumenta protivpravne aktivnosti je da se spreče buduće protivpravne. Ukoliko se ne može dati argument da je hardver imao "značajnu" ulogu instrumenta u kriminalnoj aktivnosti onda se ne bi trebala 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. [103])

b. U Virdžiniji istočni okružni sud odlučio je da je računar bio instrument protivpravne aktivnosti zato što je posedovao fajl koji je detaljno opisivao uzgajanje biljke marihuane. (United States v. Real Property 783 F.Supp. 253, 1991. [104])

Hardver kao zabranjeni materijal ili plod protivpravne aktivnosti

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[105]. 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 protivpravnih aktivnosti. Drugi primer bi bio oprema za kloniranje

103 http://securitylaw.info/pdf/945_F_Supp_441.pdf, 16.12.2011

104 http://www.leagle.com/xmlResult.aspx?xmldoc=19911036783FSupp253_11003.xml&docbase=CSLWAR2-1986-2006

105 Primer se odnosi na Sjedinjene Američke države 18 USCS 2512, 16.12.2011

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

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 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 protivpravne aktivnosti

Informacija može da bude instrument kojim je izvršena protivpravna 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 protivpravne 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[106] (eng. vulnerabi-

106 Ranjivost se definiše kao postojanje slabosti usled projektovane ili implementirane greške koja može dovesti do neočekivanog i/ili neželjenog događaja odnosno do ugražavanja bezbednosti sistema, izvor http://en.wikipedia.org/wiki/Vulnerability_%28computing%29,

lity) nekog operativnog sistema (servisa, programa ili programskog koda), a time i omogući sprovođenje neke protivpravne aktivnosti. Samo u slučaju da se prikaže da je informacija imala značajnu ulogu u protivpravnoj aktivnosti može da se zapleni kao instrument protivpravne aktivnosti, u suprotnom se ne konfiskuje.

Informacija kao zabranjeni materijal ili plod protivpravne aktivnosti

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 omogućilo im veliku privatnost. To za posledicu može 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 informacije kao plod protivpravnih aktivnosti su slike dečje pornografije, nelegalne kopije računarskih programa, ukradene poslovne tajne (industrijske, trgovačke), šifre ili bilo koje druge informacije dobijene iz protivpravnih aktivnosti.

Informacija kao dokaz

Ovo je najbogatija kategorija od svih pomenutih. Mnoge naš dnevne aktivnosti ostavljaju digitalne tragove. Svi pružaoci usluga (na primer Internet servis provajderi, telefonske kompanije, banke, kreditne institucije) vode 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 idenfitkatori uređaja kao naprimer 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 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[107].

U Americi aktom Computer Assistance Law Enforcement (CALEA)[108] 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[109]) države članice su u obavezi da čuvaju specifične telekomunikacione podatke definisane Direktivom, od 6 meseci do 2 godine[110]. U Srbije je 2010. godine usvojen Zakon o elektronskim komunikacijama, prema kojem pružaoc komunikacionih usluga (operator) mora da čuva podatke o elektronskim komunikacijama 12 meseci[111]. 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. S tim u vezi, naglasio bih da se u velikom broju zemalja još uvek vode velike polemike vezane za ovu vrstu čuvanja informacija

107 Odnosno dokaz može biti optužujući ili oslobađajući.

108 http://www.justice.gov/criminal/cybercrime/usamay2001_4.htm

109 http://en.wikipedia.org/wiki/Directive_2006/24/EC, 17.12.2011

110 Mada u praksi ima odstupanja. Ne pridržavaju se sve članice striktno te direktive, neki od primera su Nemačka Švedska.

111 http://www.paragraf.rs/propisi/zakon_o_elektronskim_komunikacijama.html, 17.12.2011

po pitanju vremena i vrste podataka zbog ugrožavanja privatnosti (u ovom slučaju privatni život i privatna komunikacija) koje 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.

4.4 Digitalna forenzika računarskih sistema - odgovor na incident

Pre svake istrage podrazumeva se ispitivanje potrebnih preduslova kao što su : postojanje dovoljnog broja obučenih profesionalaca, forenzičku radnu stanicu i forenzičku laboratoriju za oporavak podataka, saradnja sa javnim tužilaštvom i definisanu metodologiju. U zavisnosti od tipa istrage zavisi i ko će odgovarati na incidnentnu radnju/protivpravnu aktivnost.

Treba istaći da čak i najspremnije zaštitne organizacije mogu biti suočene sa krivičnim delima kao što su dela prevare, krađe, upada u računarske sisteme, finansijske prevare, krađa intelektualne svojine, ddos napada, podmetanje virusa i crva kao i druge računarske incidente i protivpravne aktivnosti. Na primer odgovor na incident u okviru orgranizacije uglavnom se odnosi na sledeće probleme :

-gubitak ili curenje osetljivih (poverljivih) podataka

-neprihvatljivo korišćenje računarskih resursa od strane zaposlenih

-računarski zlonamerni programi (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

-istraga nad drugim zaposlenim licima u IKT sistemu

U odgovoru na incident mogu da učestviju lica iz različitih oblasti na primer, menadžeri poslovnih organizacija, advokati i tužioci kao predstavnici prava, IT osoblje i nadležni državni organi, kadar tehničke podrške, sistem administratori, stračnjaci za bezbednost informacija, korporativni istražitelji, i krajnji korisnici.

Iz prethodih poglavlja koja su se odnosila na visokotehnološki kriminal i digitalnu istragu mogu se uočiti određene specifičnosti:

-protivopravne 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 počinjeni iz inostranstva

-velike razlike između sofictičiranih alata za napad i onih koji se koriste za njihovu detekciju i analizu

-mora postojati mehanizam za detektovanje incidente radnje koji aktivira odgovor na incident

Istakao bih da odgovor na incidentu radnju podrazumeva ispunjavanje različitih ciljeva kao što su :

-koordinisan i solidaran odgovor na incident (svih timova koji rade na istrazi)

.sprečava nepovezane i neusaglašene odgovore na incidentne radnje

-daje odgovor na pitanje da li se incidenet dogovio ili ne

-potpomaže prikupljanje tačnih informacija

-uspostava kontrole za pronalaženje i pravilno rukovanje digitalnim dokazima

-vodi računa pravu na privatnost utvrđenim zakonom

-minimizira ometanje tekućeg poslovanja u mrežnom okruženju.

-omogućava krivični, građanaski ili korporativni postupak protiv učinioca

-obezbeđuje tačne izveštaje i korsnike preporuke
-obezbeđuje brzo detektovanje i suzbijanje protivpravnih aktivnosti
-minimizira izloženost tj ugroženost vlasničkih podataka
-štiti imovinu i ugled organizacije
-edukuje viša rukovodstva
-potpomaže bržem detektovanju i ili sprečavanju protivpravnih incidenata u budućnosti (učenjem kroz iskustva, izmenama politika i procedura u samim organizacijama)

Kategorije incidenata

Nije svaka incidentna aktivnost i protiv pravna aktivnost. Postoje različiti pojavni oblici incidentnih radnji i neke od njih predstavljaju i protivpravna aktivnosti što za sobom povlači i zvaničnu istragu. Na osnovu pojavnih oblika incidentnih radnji i protiv pravnih 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) [67]. Detaljnija klasifikacija sa više kategorija definisana je u Federal Incident Reporting Guidelines od strane US-Cert-a[112].

Incidenti niskog nivo 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. Neki od primera bi bili neovlašće-

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

no skladištenje i obrada podataka, ilegalan pristup kancelarijama, uništavanje imovine pričinjena računarskim incidentom manja od 850.000 dinara, krađa ličnih podataka u vrednosti do 850.000, širenje računarskog virusa ili crva većeg inteziteta, neovlašćeno dobijanje privilegovanog pristupa računaru ili serveru. Incidenti visokog nivoa značajnosti za najozbiljniji incidenti i takođe su inkriminisani propisanim odredbama zakona određene države na osnovu visine pričinjene štete. Treba ih 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 inteziteta, trojanski konji ili zadnja vrata (eng. backdoor), neovlašćenja izmena hardverskih komponenti na računaru, neovlašćeno instaliranje firmware-a na računarskom sistemu ili neovlašćeno instaliranje programa na serveru. Takođe ovde spada i uništavanje imovine veće od 850.000, krađa u vrednosti preko 850.000 dinara ili je broj primeraka autorskih dela prešao 500. ilegalno prenošenje novca ili njegovo preuzimanje, ilegalni download zaštićenih materijala kao na primer muzički fajlovi video ili programi ili druge fajlove zakonom zabranjeni, upotreba računara za čuvanje slanje i primanje dečije pornografije, kockanje ili kršenje bilo kog zakona određene države, i tumačiće se kao protivpravna aktivnost.

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 dato je u tabeli US-CERT-a[113].

Postupak odgovora na incidentnu radnju

Proces ogovora na incidentu radnju sastoji se od nekoliko faza :

-pripremanje za incidentnu radnju/protivpravnu aktivnost

-detektovanje protivpravne aktivnosti

-inicijalni odgovor

-definisanje strategije za odgovor na incidentu radnju

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

-istraga samog incideneta (prikupljanje i analiza podataka)
-izveštavanje

Pripremanje za incidentnu radnju/protivpravnu aktivnost

Podrazumeva sve one radnje koje će potpomoći da se forenzički relevantan događaj spremno dočeka. Omogućava se jednostavnija koordinacija između kadra zaduženog za odgovaranje na incidentnu radnju. Pripremam 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 incidente radnje. 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. Ulaganje u razvoj kapaciteta za incidentne odgovore u okviru organizacije zavisi od procenjenog rizika.

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 kapacitetomdiktafon

-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 kao na primer Victorinox cybertool. Slika Victorinox sajbertool[114]

114 http://www.rarst.net/hardware/victorinox-cybertool/, 07.03.2012

-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

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 : Quickview plus,

Detektovanje protivpravne aktivnosti

U ovoj fazi bitno je ustanoviti inicijalnu procenu odnosno sve simptome incidentne radnje odnosno protivpravne aktivnosti, da bi se dobio odgovor na pitanje da li je u pitanju sistemski problem ili incidentna odnosno protivpravna aktivnost. To podrazumeva potvrđivanje da se radi o incidentu identifikaciju incidenta i prijavljivanje incidentne radnje odnosno protivpravne aktivnosti.

U tu svrhu potrebno je vrštiti edukaciju krajnjih korisnika i sistem administratora da mogu da prepoznaju protivpravne aktivnosti kako bi bili u mogućnosti da ih razlikuju od sistemskih problema kao na primer nestanak struje, neispravan program, problemi u komunikacionog infrastrukturi i ostali probelimi koji mogu biti izazvani lošim hardverom odnosno programom.

Jako je važno da se identikuje priroda incidentne radnje, događaji da bi se zaštitili svi potencijalni dokazi.

Prilikom detekcije i identifikovanja incidentne radnje u praksi se spovode sledeće aktivnosti :
-provera logova IDS-a (eng. intrusion detection systems)

-ispitati da li postoje procedure koje ukazuju na proveru pokazatelja protivpravnih aktivnosti na računaru putem sistema za proaktivnu zaštitu računara.

-proaktivnost podrazumeva pretraživanje neuobičejenih aktivnosti kako na mreži tako i na računarima odnosno serverima u okviru njihovih logova.

-edukovati osoblje koje radi kao tehnčka podrška da razume na koji način napadači napadaju računarske sisteme i kako da uoče napade putem nadzora mrežnih aktivnosti.

Odgovor na protivpravnu aktivnost može da postoji samo ako se ona uspešno detektuje.

Prema tome detekcija može da se uoči ručno (eng. manual) putem pregledanja log fajlova, automatska ili kombinovana. Upozorenje na incident može doći od strane IPS-a, IDS-a, krajnjih korisnika, tehničke podrške, sistem administratora, kao i od strane drugh sistema za zaštitu.

Usko je povezana sa nadgledanjem računarskih sistema i mreže (eng. monitoring) u okviru organizacije. Radno mesto za nadgledanje ima za cilj da se obezbedi kvalitet i procenjuju performanse delatnosti kojim se organizacija bavi.

Mora se istaći da se rana detekcija upada može detektovati kroz pregledanje sistemskih logova i sigurnosnih logova (eng. audit log). Koji sve procesi mogu biti praćeni zavisi od sistema. Audit log može sadržati sledeće informacije :

-specijalne operacija kao na primer promene šifre

-administrativne aktivnosti

-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 fajla

-upis ili izmana fajla

-korisnik koji je inicirao događaj

Praćenjem sistemskih logova

Kontrolisanje kroz praćenje sigurnosnih fajlova ima za cilj sledeće:

- kreiranje bezbednijeg funkcionisanja mreže i operacija na računarima

-mogućnost rane detekcije pokušaja upada na računar ili u mrežu

-brza detekcija kompromitovang računarskog sistema ili podataka koji su oštećeni ili uništeni u toku incidentne radnje odnosno protivpravne aktivnosti.

-sprečavanje daljeg širenja štete na računarskim sistemima ili u mreži nakon nastanka incidentne radnje (na primer nakon upada hakera na server).

U zavisnosti od potrebnog nivo bezbednosti podešava se i nivo Auditinga. Potreban 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. Bitno je istaći da se vreme zaštite izračunava na osnovu vremena potrebnog za detekciju i vremena reakcije na incidentnu odnosno protivpravnu aktivnost.

LINUX logovi

Na linux sistemima postoji sistem za kontrolisanje logova koji se zove Syslog koji predstavlja centralni syslog server. Može se pokrenuti komandom s#yslogd -r (gde parametar r podrazumeva mogućnost dobijanja poruka i sa mreže). Svaki program na sistemu može generisati syslog poruke koji se prosleđuju syslogd programu koji skladišti na određenim lokacijama koje definisane u konfiguracionom fajlu syslog programa - /etc/syslog.conf. U daljem tekstu biće navedeni neki od najvažnih log fajlova koje sadrže bitne informacije o dešavanjima na samom sistemu [115] :

syslog[116] - Lokacijski može da se nalazi u /var/log/ folderu i sa-

115 Lokacija i nazivi sistemskih logova mogu da varira u zavisnosti od korišćene distribucije Linuxa ali se po defaultu uglavnom nalaze u /var/log direktorijumu

116 Syslog se kao samostalan fajl ne nalazi u svim distribucijama, ali on kao sistem za kontrolisanje logova postoji u svim Linux distribucijama i upravalja se kroz njegov konfigu-

drži sistemskih logova

sulog – u ovom fajlu su evidentirane pokušaji na sistemu da se izvrši su komanda (eng. Switch user).

Utmp – vodi evidenciju trenutno prijavljenih korisnika na sistemu

Wtmp – čuva podatke iz prošlosti o prijavljivanju na sistem, odjavljivanju sa sistema, gašenju sistema I restartovanju sistema.

Lastlog- evidentira poslednje vreme I datum prijavaljivanja na sistem za svakog korisnika na sistemu, kao i adresa sa koje se logovao korisnik.

Messages – evidentira informacije definisane u syslog konfiguracionom fajlu

Xferlog- čuva podatke o ftp sesiji na sistemu

Access.log – čuva podatke http saobraćaju na web serveru

Sudolog- vodi evidenciju o tome ko je izda zahtev za korišćenje sudo komande

Btmp –beleže se podaci o greškama na sistemu

pokretanje accton servisa- Nakon upada na sistem zlonamerni napadač će pokušati da ukloni dokaze izvršenja komandi i to uglavnom brisanjem bash histori 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 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 servisa za praćenje komandi), i sa (su-

racioni fajl u kome se definiše šta će biti logovano i gde će se ti logovi na sistemu smeštati. Kao samostalan fajl može se naći na određenim Linux distribucijama kao što je Slackware ili se može kao takav definisati u okviru syslog.conf fajla u nekim drugim distribucijama kao na primeru u Red hatu.

mira informacije o prethodno izvršenim komandama podrazmeva se da je omogućen accton servis). Acct servis je na Debianu i Ubuntu Linux sistemima se startuje automatski po dofiltu, dok je kod Red Hata, Fedore i Centos sistema potrebno ručno pokrenuti servis.

Windows 2000, XP, Vista, 2003, 7 logovi

Logovi se u windowsu nalaze pod **C:\WINDows\System32\Config** folderom**.**

Pod windowsom NT I 2000 security auditing nije omogućen po defaultu.

Pregled događaja omogućen je preko Control Panel – Administrative tools-Computer management – Windows Logs

Da bi se omogućio ili onemogućio auditing na sistemu to se radi iz dva koraka. Prvi korak određuje šta je da se kontroliše i šta će da se snima To se uređuje grupnom polisom Audit Policy. Drugim korakom se određuje koji objekti, korisnici i grupe će da se kontrolišu. 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. Nako omogućavanja auditinga na sistemu u event vieweru pod Security opcijom mogu da se vide stanja praćenih aktivnosti.

Event vieweru 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). Svi ovi log fajlovi imaju svoje vremenske pečate (eng. timestamp)

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 sistemu, pomaže da se razume šta se desilo nakon upada u sistem i može poslužiti za dokazivanje protivpravne aktivnosti na sudu"[66].

5. 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 bih istakao da postoji izvesne razlike u istražnom pristupu digitalnog forenzičara kada su u pitanju fizičke odnosno virtuelne mašine[117]. 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.

Ono što je specifično za virtuelne mašine je to što one koriste u potpunosti hardver fizičkog servera. Na primer, jedan fizički server može predstavljati virtuelno okruženje sa preko 20 virtuelnih mašina. Komunikacija između fizičkog servera i virtuelnih mašina se realizuje preko hypervisor-a (program koji obezbeđuje virtuelizaciju) ili **virtual machine manager-a** putem hiper poziva. Hypervisor može da ozbezbeđuje virtuelizaciju direktno na hardveru (native VM) ili na operativnom sistemu (host VM) [13]. 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

117 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.

virtuelnim mašinama u odnosu na fizičke mašine. Postoje različiti tipovi virutelnog ogruženja a najpoznatiji su *Microsoft Hyper-V* [50], *VMWare Vsphere ESXi* [51], *QEMU* [52], *Citrix XenServer* [53]. U daljem tesktu bih naveo 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.

5.1 Virtuelno okruženje kao digitalno mesto protivpravne aktivnosti

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 fajlove koji se u tom okruženju nalaze.

Dobra informisanost i poznavanje načina rada u virtuelnom okruženju su veoma bitne 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 (ka 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 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, 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 (zvanična) i korporacijska, u zavisnosti 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 spremnih za izveštaj odnosno prezentovanje rekonstruisanog zločina ili incidenta.

Istakao bih 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. Virtualna 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 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 virtualno mogu biti gde (jedan takav primer je

Cloud computing[118]). 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 izvšene 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

Naveo bih kroz jedan slikovit opis važnih servisa koji realizuju virtuelno okruženje, a njihovo upoznavanje može biti od koristi digitalnim forenzičarima [119] [54]:

-servis za upravljanje virtuelnih mašina (Virtual machine management service, VMMS) - upravlja odnosno određuje koj operacije mogu da se izvršavaju u nekom od mogućih stanja vrituelnih mašina.

118 Kako funkcioniše Cloud computing kao tip virtuelnog okruženja. Korisnik je dobio pristup računara 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 održavanju tog računara, a u zavistnosti 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.

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

VMMS upravlja sledećim stanjima virtualnih 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 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 virtuelnih 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 upravljanjem virtuelnim procesorom i memorijom ;

-**windows Hypervisor Interface biblioteka (eng. The Windows Hypervisor Interface Library)** – predstavlja komponentu

kernela kao dinamička bibliotka (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[120] 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 [61] ca ciljem da se smanji rizik od izmene nad dokazima tokom njihovog ispitivanja. Takođe ovaj alat omogućava analizu uživo nad Xen virutelnoj mašini[121]. 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 ovom alatom je mapiranje memorije osumnjičene mašine i dodeljivanje mapiranog dela virtuelnoj forenzičkoj mašini.

120 http://www.uaf.edu/, 03.01.2012

121 http://assert.uaf.edu/papers/forensicsVMI_SIGOPS08.pdf, 03.01.2012

Mreže u virtuelnom okruženju

Kada je reč o mrežama u virtuelnom okruženju postoje tri vrste virtuelnih mreža [54] :

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 virtualna 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 sami 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. 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[122] i AMD-V[123]. Zašto je značajno da se digitalni forenzičar ustavnovi 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 može biti od koristi u slučaju potrebe monitoring-a i upoznavanje sa virtuelnim mašinama na živo (eng. live). Na taj način mogu se otkriti značajne informacije : imena virtuelnih mašina, stanje u kom se nalaze virtuelne mašine (da li su aktivne ili nisu), u kom režimu rada se one nalaze, iskorišćenost resursa od strane virtuelnih mašina, i podatke o vremenu i vremenskim zonama. Na primer to mogu biti „last logon" log fajlovi ili „configuration log" fajlovi, a njihove putanje zavise od vrste programa koji realizu-

122 Ovde se nalazi lista Intelovih procesora koji imaju podršku za virtuelizacije : http://ark.intel.com/VTList.aspx, 10.02.2012

123 AMD platforma za virtuelizaciju :http://sites.amd.com/uk/business/it-solutions/virtualization/Pages/amd-v.aspx, 10.02.2012

ju 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 diretktorijum 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. Evidentirati da li se vremena poklapaju i kolika su odstupanja ?[124]

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 512gb do 4 GB Ram memorije u zavisnosti od OS-a koji je odgovoran za realizovanje virtuelizacije.

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

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.*

Virtuelni hard disk

Svaka virtuelna mašina upisuje svoje podatke na virtuelnom hard disku. Za digitalnog forezičara 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[125] (eng. Storage area network) ili NAS[126] (eng. Network Attached Storage) uređaje ili na lokalne hard diskove. Informacija o veličini je bitna zbog organizova-

125 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.

126 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.

nja 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 samo particije za koju se sumnja da sadrži digitalne dokaze. Te informacije se mogu naći u konfiguracionim fajlovima same virtuelne mašine. Određene ekstenzije[127] 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 koja 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.

127 Ekstenzije ovih fajlova razlikuju se u zavisnosti od progama koji realizuje virtuelno okruženje.

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 [63]. 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 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 jako su važne, jer bi se na osnovu (sa)znanja trenutka učinjenja protivpravne aktivnosti, preko pokretanja slika stanja (od poslednje ka prvoj) na forenzičkoj mašini, 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.

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 koje se numeriše, izračunavala se hash 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 pred-

stavlja 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. 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 sa 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 i postoje čak 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 i okviru istog fizičkog severa ili na neki drugi fizički sever). To sa druge strane može da omogući učiniocu protivpravne aktivnosti prikrivanje dokaza o ne zakonitom 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 sli-

ka stanja sistema (eng. snapshots), podatke o perifernim virtuelnim uređajim, podatke iz RAM 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 ne praktične 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. Dodao bih i to da kada je istraga usmerena ka virtuelnom okruženju u kojoj se jedna virtuelna mašina dovodi u vezu sa protivpravnom aktivnošću, 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.

5.2 Virtuelno okruženje kao okruženje za digitalno forenzičku analizu

Koncept virtuelizacije i specifičnosti digitalne forenzike virtuelnog okruženja su objašnjene na početku ovog poglavlja , a ovaj deo 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 digitalno forenzičke analize. Ideja kod ovog pristupa je da se proces digitalno forenzičke analize sprovodi istovremeno pod konvencionalnim i virtuelnim okruženjem nezavisno jedno od drugog, što kao benefit može da ima skraćenje trajanja digitalno forenzičke analize. Fokus

ovog poglavlja je jedna faza procesa digitalne istrage odnosno digitalna forenzička analiza. Proces digitalno forenzičke analize može se obuhvatiti u 3 ključne faze kao što su to prikazali Kruse i Heiser u svom modelu [39]: dobijanje dokaza, utvrđivanje autentičnosti i analiza.

Christopher Brown, osnivač jedne od vodećih kompanija koja se bavi digitalnom forenzikom (CTO of Technology Pathways LLC[128]) 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[129]) svih uređaja za skladištenje podataka tj. hard diskova. Većina autora ističe da se pravljenje forenzičke kopije odnosno slike (eng. image) osumnjičenog hard diska realizuje sa programima koji su bazirani na „dd alatu" [130] kao i da se dobijena forezнička kopija čuva u dd formatu ili nekom koji je baziran na dd-u [56][57][58]. 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. Postoje priličan broj adekvatnih formata slike originalnog hard diska koji se najčešće koriste a koji nisu identični originalnom čvrstom disku, jer mogu sadržati dodatne meta podatke ka na primer imena istraživača, beleške istraživača ili hash vrednosti. Primer za jedan takav forenzički adekvatan foramat je popularni napredni forenzički format (eng. Advanced forenisc format - AFF) [60] razvijen od strane profeosra Simsona Garfinkela i kompanije Basis Technology[131]. 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.

128 http://www.techpathways.com/DesktopDefault.aspx, 31.02.2012

129 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 [56][58][59].

130 http://en.wikipedia.org/wiki/Dd_%28Unix%29, 31.02.2012

131 http://www.basistech.com/e-discovery/ , 13.02.2012

Sa druge strane alat dd daje sliku identičnu originalu i 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, 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 potrebnih 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 [132] i Technology Pathways-ov Prodiscover[133]. Od besplatnih alata to je Live View[134] 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 pri-

132 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

133 http://www.techpathways.com/prodiscoverdft.htm, 16.02.2012

134 http://liveview.sourceforge.net/, 16.02.2012

mene u forenzičkoj analizi [62]. Međutim ukoliko se virtuelno okruženje u ulozi digitalno forenzičkog alata primenjuje u kombinaciji sa klasičnim digitalnom 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 [64]. Ovaj tip modela podrazumeva dva nivoa digitalno forenzičkog kadra. Prvi nivo predstavlja digitalno forenzičke istražitelje - profesionalce (DFIP) potpuno obučeni sa velikim isktustvom koji striktno poštuju metode pravila i procedure digitalno forenzičke istrage. Drugi nivo predstavljaju digitalno 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.

Ilustrativan primer bi bio sledeći : računarski tehničari pokreću kopiju prikupljene slike u virtuelnom okruženju (kao virtuelnu mašinu), tretirajući ga 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 forenzičkim znanja mogu primenjivati računarske forenzičke tehnike i u fazama bez ugrožavanja digitalnih dokaza.

Podrazumeva se, da se nad jednom kopijom primenila funkcija hashiranja 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.

Na osnovu dobijenih informacija od strane računarskih tehničara, DFIP mogu potvrditi sve rezultate koristeći odgovarajuće fo-

renzičke 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 je postoji manjak kadra forenzičkih profesionalaca).

6. LITERATURA

[1] Milan Milosavljević, Gojko Grubor, *Digitalna forenzika računarskog sistema*, Univerzitet Singidunum, Beograd 2009.

[2] Dragan Prlja, Mario Reljanović, *Pravna informatika*, Pravni fakultet Univerziteta Union, Beograd, 2010.

[3] National Policing Improvement Agency, *Core Skills in Data Recovery & AnalysisCourse Reference Book V2.01*, Bradford, UK, maj 2007.

[4] Nelson B., Phillips A., Enfinger F., Christopher S., *Guide To Computer Forensics And Investigations*, Second Edition, Published by Course Technology, 25 Thompson Learning, lnc., Printed in Canada, 2006.

[5] Georgijević Uglješa, *Istražne metodologije, tehnike i alati za digitalnu forenzičku istragu*, , master rad, Fakultet za informatiku i menadžment, Univerzitet Singidunum 2010.

[6] Aleksandar Tasić, *Forenzika usb i compact flash memorijskih uređaja*, master rad, Univerzitet Singidunum 2010.

[7] Eoghan Casey, *Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet*, Second Edition, Academic Press 2004.

[8] Milan Milosavljević, Gojko Grubor, *Istraga kompjuterskog kriminala - metodološko tehnološke osnove*, Univerzitet Singidunum 2009.

[9] Lidija Komlen Nikolić, *Suzbijanje visokotehnološkog kriminala*, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd 2010 strana 13

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

[11] Michael Cross, *Scene of the Cybercrime*, Second Edition, syngress, 2008

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

[13] Nebojša Ivaniš, *Digitalna forenzicka istraga u virtuelnom okruženju*, master rad, Univerzitet Singidunum 2011.

[14] Gojko Grubor, *Funkcionalni model istrage kompjuterskog kriminala*, Ziteh 2010.

[15] Douglas Schweitzer, *Incident Response - Computer Forensics Toolkit*, Wiley Publishing, Inc, Indianapolis, 2003.

[16] John I. Thornton, "*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*)*

[17] Drakulić M, Drakulić R, *Cyber kriminal*, Fakultet organizacionih nauka u Beogradu, http://www.bos.rs/cepit/idrustvo/sk/cyberkriminal.pdf

[18] 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. http://www.un.org/events/10thcongress/2088h.htm

[19] Council of Europe, Recommendation No. R (95) 13, http://www.justice.gov/criminal/cybercrime/crycoe.htm

[20] http://www.justice.gov/criminal/cybercrime/intl.html

[21] CONVENTION ON CYBERCRIME, Council of Europe, Budapest novembar 2001,

http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc

[22] Samuel C. McQuade III, *Encyclopedia of Cybercrime*, Greenwood Publishing group, USA 2009.

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

[24] Kamil Kopecký, *Cyber grooming danger of cyberspace*, study, Olomouc, 2010.

[25] Kamil Kopecký, *Stalking a kyberstalking nebezpečné pronásledování*, study Olomouc, 2010 Izvor: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd

[26] Clay Wilson, *Computer attack and cyber terrorism : Vul-*

nerabilities and policy issues for Congress. Us Congressional Research Report RL32114, strana 4. Izvor: http://www.fas.org/irp/crs/RL32114.pdf. October 17 2003

[27] Marie-Hellen Maras, *Computer forensics, cybercriminals, laws and evidence*, Jones &Bartlett learning, USA 2012

[28] John Ay cock, *Computer Viruses, and Malware* , Springer , Canada, 2006.

[29] Henry Lee, Timothy Palmbach, and Marilyn Miller, *Henry Lee's Crime Scene Handbook*, San Diego: Academic Press, 2001.

[30] Richard Saferstein, *Criminalistics: An Introduction to Forensic Science*, Pearson, 7 edition, 2000.

[31] Digital Forensics Research Workshop, *A road map for digital forensics research*, Technical report, Digital Forensics Research Workshop, 2001.

[32] Daniel A. Ray, Phillip G. Bradford, *Models of Models: Digital Forensics and Domain-Specific Languages* (Extended Abstract), 2008. http://www.ioc.ornl.gov/csiirw/07/abstracts/Bradford-Abstract.pdf, strana 1., 18.12.2011

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

[34] 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

[35] 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, Online: http://www.ijde.org/docs/02_fall_art2.html

[36] Hauck, R. V., 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.

[37] N.L. Beebe and J.G. Clark. *A hierarchical, objective-based*

framework for the digital investigations process, In Proceedings of the 2005 Digital Forensics Research Workshop, 2005 pp 146-166, 2005.

[38] Rowlingson, Robert "A Ten Step Process for Forensic Readiness," *International Journal of Digital Evidence* (2:3), Winter 2004, pp 1-28

[39] Warren G. Kruse II, Jay G. Heiser, *Computer Forensics Incidend response essentials*, 14th printing, New York: Addison Wesley, March 2010

[40] National Institute of Justice. (July 2001) *Electronic Crime Scene Investigation. A Guide for First Responder,* Dostupno na https://www.ncjrs.gov/pdffiles1/nij/187736.pdf

[41] Casey Eoghan, *Digital Evidence and Computer crime*, Academic press, San Diego 2000.

[42] Casey Eoghan, *Digital Evidence and Computer Crime*, 2nd Edition, Elsevier Academic Press, 2004.

[43] Michael Kohn, Jhp Eloff, Ms Olivier, *Framework for Digital Forensic Investigation: Information and Computer Security Architectures Research Group (ICSA)*, University of Pretoria, 2006. Dostupno na adresei http://mo.co.za/open/dfframe.pdf

[44] Casey Eoghan, *Handbook of Digital forensics and investigation*, Elsevier Academic Press, Burlington, 2010.

[45] Chris Prosise and Kevin Mandia, *Incident Response: Investigating Computer Crime*, McGrawHill Osborne Media, 2001.

[46] Chris Prosise, Kevin Mandia, *Incident response and computer forensics*, second edition, The McGraw-Hill Companies 2003.

[47] Brian Carrier, Eugene H. Spafford, *Getting Physical with the Digital Investigation Process*, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2, 2003

[48] Brian Carrier, *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers,* International Journal of Digital Evidence, Winter 2003

[49] National Institute of Standards and Technology, *Secure Hash Standard*, FIPS PUB 180, May 1993.

[50] Microsoft Hyper-V, http://www.microsoft.com/en-us/ser-

ver-cloud/hyper-v-server/ , *Pristupljeno 09.02.2012*

[51] *VMWare Vsphere ESXi,* http://www.vmware.com/products/vsphere-hypervisor/overview.html , Pristupljeno 09.02.2012

[52] *QEMU*, http://wiki.qemu.org/Main_Page , Pristupljeno 09.02.2012

[53] Citrix Xenserver http://www.citrix.com/English/ps2/products/product.asp?contentID=683148

[54] Mitch Tulloch, *Understanding Microsoft Virtualization Solutions from desktop to the datacentar*, second edition, Microsoft Press A Division of Microsoft Corporation One Microsoft Way Redmond, 2010.

-----[55] Christopher Brown, *Computer Evidence - Collection and Preservation*, Thomson Delmar Learning, Charles River Media, Inc, Hingham, Massachusetts, 2006 pages 213-218

[55] Dragan Prlja, Mario Reljanović, "Visokotehnološki kriminal - uporedna iskustva", u Strani pravni život, br.3/2009, str.161-184.

[56] Nelson, B., Phillips, A., Enfinger, F., & Steuart, C, *Guide to Computer Forensics and Investigations, Second Edition*, Thomson Course Technology, Boston, 2006

[57] Rude, T. (2000). *DD and Computer Forensics,* Retrieved October 23, 2003, http://www.crazytrain.com/dd.html , 13.02.2012

[58] Steve Bunting, William Wei, *EnCase Computer Forensics: The Official EnCE: EnCase Certified Examiner Study Guide,* Indianapolis, IN: Wiley Publishing, 2006

---[59] Scott, Mark, *Independent Review of Common Forensics Imaging Tools*, Memphis Technology Group, SANS GIAC Paper Submission, 2004.

[59] Dragan Prlja, Miodrag Savović, "E-mail kao dokazno sredstvo u uporednom pravu", u Strani pravni život, br. 2/2009, str. 71-85.

[60] Garfinkel, S., *The Advanced Forensic Format 1.0*. 2005. http://stuff.mit.edu/afs/sipb/user/simsong/afflib/affdoc.doc, 13.02.2012

[61] Brian Hay Kara Nance**,** *Forensics Examination of Volatile System Data Using Virtual Introspection***,** SIGOPS Operating Systems Review , Volume 42 Issue 3, ACM, 2008.

[62] Seth Fogie, *VOOM vs The Virus (CIH)*, http://voomtech.com/downloads/Shadow%20Eval%20-%20Fogie.pdf, 2004, 16.02.2012

[63] Christiaan Beek, *Virtual Forensics*, TenICT proffesionals, http://securitybananas.com/wp-content/uploads/2010/04/Virtual-Forensics_BlackHatEurope2010_CB.pdf, 16.02.2012

[64] Derek Bem i Eva Huebner, *Computer Forensic Analysis in a Virtual Environment*, International Journal of Digital Evidence Fall 2007, Volume 6, Issue 2, 2007.

[65] 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/

[66] Bruce Schneier , *Secrets & Lies*, Digital Security in a Networked World, John Wiley & Sons, 2000

[67] Ec-Council Press, Computer Forensics: Investigation procedures and response, Course Technology Cengage learning, USA, 2010

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343.983:004

КОРАЋ, Вања, 1976-
Digitalna forenzika kao arheologija podataka u visokotehnološkom kriminalu / Vanja Korać. - Beograd : Centar za nove tehologije Viminacium : Arheološki institut = Belgrade : Center for new technology Viminacium : Archaeological Institute, 2013 (Beograd : Digital Art). - 139 str. : ilustr. ; 23 cm. - (Arheologija i prirodne nauke = Archaeology and Science, ISSN 1820-6492. Posebna izdanja = Special Edition ; 6)

Tiraž 500. - Napomene i bibliografske reference uz tekst. - Abstract. - Bibliografija: str. 134-139.

ISBN 978-86-87271-22-7 (CNTV)

a) Вештачење - Рачунарски системи
COBISS.SR-ID 196127244