

KOMPJUTERSKA FORENZIKA: ODGOVOR NA INCIDENT

Dipl. Ing. Stevanović Boris, Narodna banka Srbije,
sboris@ptt.yu

Abstrakt: *U ovom radu obrađena je problematika prikupljanja digitalnih dokaza pomoću kompjuterske forenzike kao reakcije na incident. Prikazano je nekoliko tehnika prikupljanja digitalnih dokaza i njihovog tretiranja.*

Ključne reči: *digitalni dokaz, povraćaj podataka, logovanje, auditing, toolkit*

COMPUTER FORENSICS: INCIDENT RESPONSE

Abstract: *This paper deals with problems of gathering computer evidences with computer forensics as incident response. Several techniques for collecting and management of digital evidence are reviewed.*

Keywords: *digital evidence, data retrieval, logging, auditing, toolkit*

1. Uvod

Kompjuteri, bez sumnje, čine ljudsku aktivnost bržom, jednostavnijom i interesantnijom. Uz njihovu pomoć stvaraju se novi modeli rada, ali i ostalih tipova aktivnosti koje ljudi preduzimaju. Posledica takvog stanja je kontinualno generisanje novih ideja kao i povećanje broja mogućnosti koje se nude savremenom čoveku. Međutim, u svetlu ovih dobrih stvari koje računari donose postoji i tamna strana koja pruža prilike za nanošenje štete društvu. Sve one tehnologije koje nose informacionu i informatičku revoluciju istovremeno su i nosioci evolucije kompjuterske forenzike, posebnog tipa forenzike, koja nam može pokazati i dokazati kako ljudi, pomoću kompjutera, mogu počiniti neko kriminalno delo.

U samom početku Internet je kao i svaki dimamički sistem nametnuo određena pravila ponašanja kojih su se većina korisnika pridržavala. U početku reč je bila o nekoj vrsti kodeksa (*netiquette*), da bi zatim razvio sistem praćenja, moderacije, a na kraju je došao u sistem kažnjavanja (*ban, black lists* itd). Kako kibernetički prostor (*cyber-space*) nije moguće ograničiti, tako dolazi i do problema u postavljanju zakonske regulative koja bi mogla najbolje da se suprotstavi neprimerenom ponašanju ljuskog faktora. Problem dolazi i sa izvora cele priče. Ma koliko korisnici Interneta želeli da njihovi računari budu sigurni često je takvo stanje u kontra poziciji u odnosu na ekonomski faktor. Administratori, pretežno, komercijalnih sajtova u cilju poboljšanja prodaje i unapređenja njihovih *e-commerce* sistema često primenjuju neke tehnike koje se mogu iskoristiti na maliciozan način. Od svih aktivnosti koje takav sistem može da pruži korisniku nije sve produktivno, niti je sve legalno i samim tim nije društveno poželjno. Zakoni, regulative i etika su često u konfliktu sa ciljevima poslovanja.

Kompjuterska forenzika daje sve potrebne veštine za identifikaciju incidenta, otkrivanje i sklapanje svih dokaza neophodnih za izgradnju čvrstog pravnog slučaja. Veoma važno je da slučaj bude utemeljen i dobro obrazložen u očima prava pa čak iako to nije slučaj sa aspekta sistem administratora ili nekog drugog korisnika. Termin forenzika se može primeniti u informacionoj tehnologiji iako pred društvo postavlja niz problema u konceptualizaciji slučaja. Postavlja se set pitanja kako krivično delo može biti dokazano digitalnim dokazom ? Kako alocirati odgovornost ? Može li kompjuter biti oruđe ? Koji bi bili elementi validni za odbranu ? Možda najgore od svega je pitanje da li kompjuter može izazvati jasan, očevidan, zločin (kriminalni akt) i može li se neopaženo podmetnuti krivica nekome ko je u celoj priči nevin ?

2. POJAM I ULOGA KOMPJUTERSKOG KRIMINALA

Kompjuterska forenzika obuhvata istragu neke zloupotrebe na osnovu kompjuterski zasnovanih odnosno digitalnih dokaza¹. Često je neophodno da odgovorna lica, koja sprovode tu istragu, pored pravnog aspekta, poznaju i tehničku ulogu koju igraju računarski sistemi. Kao što smo već pomenuli neće svaki incident rezultirati jakim slučajem, niti će prestupnik biti krivično gonjen. Prema američkom Ministarstvu pravde kompjuteri mogu odigrati tri različite uloge u kriminalnom slučaju².

- Kompjuteri imaju ulogu žrtve,
- Kompjuteri mogu imati indirektnu ulogu u izvršenju prestupa i
- Kompjuteri imaju ulogu prestupnika.

¹ Definicija preuzeta sa internet enciklopedije Wiki

² Mohay G., Anderson A, Collie B., VelRodney D., McKemmish R., Computer and Intrusion Forensics, str 9

3. UPOTREBA KOMPJUTERSKE FORENZIKE

Već je pomenut pojam kompjuterske forenzike i neke od oblika kriminalnih radnji koje kompjuterska forenzika može tretirati. Kompjuterska forenzika predstavlja skupljanje, čuvanje, analizu i prezentaciju kompjuterskih i/ili digitalnih dokaza³. Postavlja se logično pitanje. Kada je potrebno koristiti kompjutersku forenziku? Laici bi rekli da je upotreba kompjuterske forenzike potrebna uvek kada se radi o kompjuterskom kriminalu. Međutim podsetimo se da kompjuterska forenzika nosi velike nedostatke i da je teško napraviti čvrst slučaj samo pomoću forenzike. Upotreba kompjuterske forenzike potrebna u svakoj situaciji kada je jasno da se na nekom kompjuteru nalaze potencijalno važni dokazi za slučaj, ali kako je veoma moguće da do tih dokaza nije lako doći potrebno je da tehnike kompjuterske forenzike primenjuje ekspert iz te oblasti kako ne bi došlo do oštećenja dokaza i smanjenja njihove upotrebljivosti na sudu.

Kada se traži stručnjak iz oblasti kompjuterske forenzike od velikog je značaja da se pronađe iskusna osoba. Kompjuterska forenzika je forenzika kao i svaka druga pa je iskustvo od neprocenjive važnosti. Iako će mnogi reći za sebe da su stručnjaci, pravnici kojima je potrebna usluga nekog forenzičkog stručnjaka posebno moraju da obrate pažnju da reference istog i da pažljivo procene nivo stručnosti.

Kompjuterska forenzika nije samo pronalaženje skivenih i obrisanih podataka ili snimanje stanja memorije. Sposobnost onoga ko sprovodi te tehnike povećava se sa mogućnošću da na pravilan način interpretira rezultate do koji je došao. Te rezultate taj isti stručnjak moraće da brani argumentacijom koja je razumljiva svakom ko bi je slušao. U krajnjem slučaju forenzičar mora da svoju analizu prezentuje i obrazloži na sudu pa i da odgovori na svaka pitanja koja bi mogla da se postave u toku postupka. Neki autori pokušali su da razviju neku vrstu okvira (*framework-a*) koji bi pomogao u upotrebi kompjuterske forenzike u pravosuđu. Iako je vođenje pravnog slučaja primer situacionog menadžmenta, a smeštanje metodologije u neke okvire nije takve prirode iznećemo primer jednog *framework-a*.

- Test eksperitze,
- Test metodologije i
- Test tehnologije.

Kompjuterska forenzika je našla svoju primenu u velikom broju oblasti. Nisu samo pravo i istražni organi zainteresovani za kompjutersku forenziku. Sve je više velikih, privatnih, kompanija koje koriste kompjutersku forenziku kao vid unutrašnje kontrole svojih zaposlenih, pravdajući to prevencijom. Kasnije će biti reči se pozabaviti praktičnim aspektima primene kompjuterske forenzike.

4. USPOSTAVLJANJE SLUČAJA KOMPJUTERSKE FORENZIKE

Na početku ovog rada napravljenja je razlika između forenzike upada i kompjuterske forenzike. Jedna od zajedničkih stvari za oba tipa forenzike jeste priroda dokaza koju koriste. Kompjuterski bazirani digitalni dokazi čine osnovu bez koje nije moguće uspostaviti bilo koji slučaj iz oblasti kompjuterske forenzike.

Kompjuterska forenzika kako u širem (korišćenje svih kompjuterski zasnovanih dokaza) tako i u užem smislu (korišćenje samo dokaza prihvatljivih za sud) sastoji se od aktivnosti prilično različitih od onih aktivnosti koje se sprovede u nekim tradicionalnim forenzičkim disciplinama. Materijal koji kompjuterska forenzika obrađuje, kao i alati i tehnike, nisu prirodnog porekla niti se proizvodi u nekim laboratorijama. Često je mes-

³ Definicija preuzeta sa internet enciklopedije Wiki

to događaja komercijalne prirode, a kompjuterska forenzika pokušava da sastavi divergentne dokaze kako bi se dobio prihvatljiv scenario slučaja.

Jasno je da je centralna uloga u uspostavljanju slučaja kompjuterske forenzike namenjena dokazu. Po prirodi stvari digitalni dokaz je potreban uslov za izgradnju slučaja kompjuterke forenzike, ali ne i dovoljan. Pravo i istražni organi se susreću sa problemom nedovoljnog broja obučenih ljudi koji bi se mogli pozabaviti ovom problematikom. Do skora je i zakonska regulativa bila prepreka u izgradnji slučaja baziranog na kompjuterskoj forenzici jer u postojećim zakonima većine zemalja nisu se mogli objasniti pojmovi poput kompjuterski upad, *download*, *logging* i sl. Problem koji je bio podjednako ozbiljan kao i ovaj prvi je to što digitalni dokaz nije imao fizičku, materijalnu, komponentu poput otisaka prstiju, mrlja od krvi ili rane od oružja pa je težina dokaza uvek bila dovođena u pitanje od suprotne strane u slučaju.

5. DIGITALNI DOKAZ

Dokaz je ono što razdvaja hipotezu od neosnovane tvrdnje. Dokazi mogu potvrditi ili oboriti hipotezu pa je njihov integritet ključna stvar u njihovom prihvatanju odnosno odbacivanju pred sudom. Postoji nekoliko specijalnih karakteristika digitalnog dokaza koje ih čine posebno izazovnim. Pre svega potrebno je jasno i precizno definisati digitalni dokaz.

Digitalni dokaz je informacija uskladištena ili prenošena u digitalnoj formi koja učestuje u sudskom slučaju i može se koristiti na suđenju⁴. Digitalna forma po svojoj prirodi podrazumeva da se radi o nekom elektronskom ili magnetnom uređaju pa to mogu biti podaci u operativnoj memoriji, na hard disku, flash karticama, ali i podaci koji se nalaze u transmisiji npr. radio talasi. Digitalni dokaz nije nešto što ljudi mogu na prvi pogled protumačiti. U bukvalnom smislu digitalni dokaz predstavlja niz nula i jedinica koje neki elektronski uređaj prevodi u ljudima razumljivu formu koju oni mogu koristiti kao potkrepljenje svojoj hipotezi u okviru nekog sudskog slučaja.

Treba se osvrnuti na karakteristike i prirodu digitalnih dokaza⁵.

- 1 *Veliki broj potencijalno inkriminiranih*: Kod tradicionalnih prestupa često se pojavljuje nešto što isti manifestuje – postoji leš, otisci prstiju, vlasi kose – materijalni tragovi. Sa takvom početnom tačkom istražiteljima je lako da započnu pretragu jer postoji neko usmerenje i početna lista osumnjičenih. Proverava se ko je poznao žrtvu, čiji su otisci, radi se DNK test i sl. Internet, zbog svoje anonimnosti i nepostojanja standarda indentifikacije može ponuditi veliki broj potencijalno osumnjičenih.
- 2 *Identifikacija prestupa*: Kod kompjuterskog kriminala priroda prestupa je manje očigledna i neposredna. Na primer ako haker ukrade poverljive informacije, žrtva može da ne primeti da je oštećena sve dok ne bude obaveštena od strane sistem administratora, a to je obično kasno nakon samog upada. Krađa identiteta je jedan od prestupa koji ima najveći faktor rasta u oblasti kompjuterskog kriminala, a može biti otkrivena tek nakon nekoliko godina.
- 3 *Suviše potencijalnih dokaza*: Kod kompjuterske forenzike nekad je neophodno pokušati dati postojanu hipotezu koja je mnogo šira od finalne, da bise zatim ta ista hipoteza sužavala tokom istrage. Naravno da nije sve digitalni dokaz. Čak šta više o odnosu na ono na šta se sve nailazi tokom istrage dokazi su u malom procentu. Istražitelj mora znati šta od toga da iskoristi za sužavanje početne hipoteze, a da bi to uradio mora znati prirodu prestupa. Kako je identifikacija prestupa teška sama po sebi jasno je o kakvom se problemu radi.

⁴ Definicija preuzeta sa internet enciklopedije Wiki

⁵ Mohay G., Anderson A., Collie B., VelRodney D., McKemmish R., op. cit., str 44.

- 4 *Podložnost kontaminaciji*: Tradicionalni dokazi, uglavnom, bivaju poslani sa scene događaja na neko drugo mesto na kojima se vrši njihova obrada i na kome se čekaju rezultati. Kod kompjuterske forenzike ne postoji takva neosetljivost na promenu stanja. Svi koraci u procesu istrage moraju preduzeti što pre sve potrebne mere za očuvanje početnog stanja. Sprovođenje takve metodologije moguće je samo ako se prati striktno određena procedura. Niko ne želi da dođe do kontaminiranja dokaza, a koliko je to moguće govori činjenica da se restartom kompjutera drastično menja početno stanje, a da dokazi mogu biti ne samo kontaminirani već i zauvek izgubljeni.
- 5 *Lakoća gubitka dokaza*: Upravo poslednja rečenica prethodne karakteristike otvara novo pitanje. Da li bez dokaza koji je izgubljen slučaj može da opstane. Naravno da je gubitak dokaza kardinalna greška koja ne bi smela da se dogodi ni početnicima, a kamoli nekome ko je iskusan u poslu kompjuterske forenzike. Međutim nekada je gubitak dokaza posledica neznanja da je dokaz zaista prisutan. Kasnije će se govoriti o koracima koji se preduzimaju kao reakcija na incident i videćemo na koji način se ovakve greške mogu smanjiti na minimum.

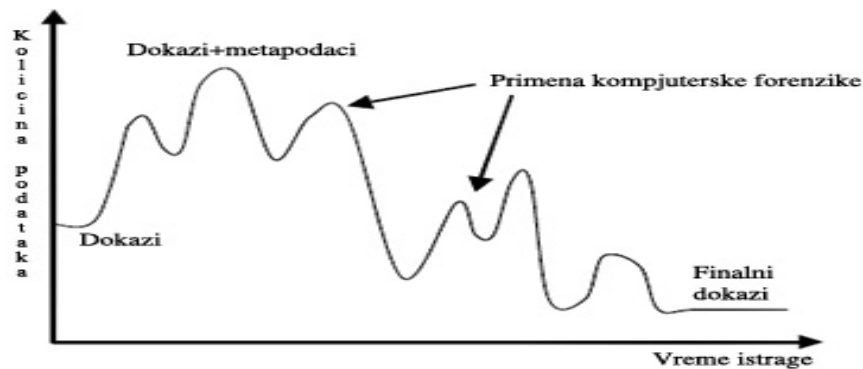
5.1 Pribavljanje digitalnih dokaza

Kako je kompjuterska forenzika više zainteresovana za formu nego za funkciju izvora digitalnog dokaza izvori digitalnih dokaza su klasifikovani prema skladištenju podataka na:

1. **Privremenu formu digitalnog dokaza**. Tipičan predstavnik ove forme je RAM memorija koja bez eksternog izvora napajanja prestaje da postoji.
2. **Nestalnu formu**. Kod ove forme postoji neki interni izvor napajanja poput baterije. Kao i kad privremene forme ukoliko bismo izvadili bateriju informacije bi bile izgubljenje. Primer ove forme je CMOS ili RAM na laptopu koji ima napajanje na bateriju.
3. **Semipermanentna (polustalna) forma**. Reč je o perzistentnom medijumu koji se može promeniti npr. hard disk, disketa, CD, DVD, MMC i sl.
4. **Permanentna (stalna) forma**. ROM memorija⁶.

Kompjuterski forenzičar mora dobro da poznaje svaku od gore navedenih formi kako bi izbegao probleme koje smo naveli, a koji karakterišu digitalne dokaze. Već je pominjana inicijalna obimnost digitalnih dokaza. Istražitelj mora sa takvim podacima da postupa iterativno-dekrementativno i da početnu veliku količinu podataka svede na optimalnu veličinu. Svaka iteracija u forenzičkoj istrazi rezultira za slučaj vrednim podacima, a istovremeno smanjuje inicijalnu količinu podataka. Rezultujući skup podataka se u sledećoj iteraciji koristi za dublju analizu i tako se dolazi do neke optimalne veličine podataka. Finalni set dokaza bi trebao da bude od velike koristi pravnicima u sudskom procesu protiv počinioca prestupa. Na sledećoj slici možete videti kako se grafički predstavlja ovaj iterativno-dekrementativni proces pronalaženja rezultujućeg skupa digitalnih dokaza.

⁶ Mohay G., Anderson A., Collie B., VelRodney D., McKemmish R., op. cit., str 25.



Slika 1. Proces pronalaženja dokaza

5.2 Odgovor na incident

U informacionoj tehnologiji termin incident odnosi se na ne-prijateljski događaj u informacionom sistemu i/ili mreži ili pretnju takvim događajem. Događaji poput čupanja kablova koje rezultira padom sistema ili namernog izazivanje nestanka električne energije nisu incidenti ovog tipa pošto se pod incidentom smatra samo ono što je u opsegu bezbednosti informacija (informacione sigurnosti). Navedimo neke primere: pad sistema, *flooding*, incidenti nastali ljudskom greškom poput brisanja kritičnih podataka itd.

6. FORENZIČKA PRIPREMA I PRVI ODGOVOR

6.1. Značaj log fajlova

Log fajlovi (logovi-dnevnici rada) su tradicionalni izvor informacija i dokumentacija aktivnosti koje su se desile ili koje se i dalje dešavaju u operativnom sistemu. Svrha logovanja (*logginga*) je da se sačuvaju značajni događaji npr. nakon dešavanja incidenta administrator sistema želi da dođe do neke ideje o tome šta se zaista desilo. Logovi mogu biti različitog tipa. Sistemski logovi, aplikacioni logovi, mrežni logovi su samo najčešći od brojnih tipova logova. Moderni operativni sistemi ponekad spajaju tipove logova kako bi se povećala mogućnost sinhronizacije vremenske linije logovanja i praćenja aktivnosti na kompjuterskom sistemu.

Važna aplikacija koja se može pronaći u Windows XP i 2000 sistemima je tzv. *Event viewer*. Ova aplikacija nakon nadziranja, dokumentuje sve važne informacije na jednom mestu npr. Podatke o punom hard disku, hardversku koliziju, ali i one događaja koji se u prvi mah čine nevažnim. Logovanje događaja počinje odmah nakon podizanja operativnog sistema i traje sve do završetka rada. *Event viewer* dokumentuje logove raznih formata. Tri formata su bazična:

1. **System log:** Sistem logovi sadrže podatke o događajima i aktivnostima koji izazivaju komponente sistema. Na primer greške u drajveru ili nekog drugog sistemskog servisa biće zabeležene u logu ovog tipa. Tipovi događaja koji odgovaraju svakom od ovih logova predefinisani su od strane samog sistema.
2. **Security log:** Logovi ovog tipa sadrže informacije o validnim i ne validnim pokušajima logovanja kao i događaje koji regulišu korišćenje resursa. Pod ovim se podrazumeva kreiranje i brisanje fajlova ili drugih objekata, kao i menjanje statusa nekih sistemskih komponenti. Logovi ovog tipa dostupni su samo administratoru sistema i adminisitrator određuje koje će aktivnosti nadzirati.

3. **Application log:** Aplikacioni logovi su najbrojniji logovi i beleže aktivnosti aplikacija. Kao primer izdvojimo logove sistema za upravljanje bazama podataka koji svaku transakciju nad bazom beleže u jedan log ovakvog tipa. Tvorci aplikacija određuju šta će se nadzirati i logovati

6.2 Povraćaj podataka

Povraćaj (oporavak) podataka⁷ predstavlja vrlo važan deo svake forenzičke istrage. U uvodnim razmatranjima pomenuli smo da je esencija svake forenzičke istrage i odgovora na incident skupljanje digitalnih dokaza. Digitalni dokazi su najčešće u obliku nekih fajlova, ali kako nije svaki fajl dokaz treba razgraničiti ove dve stvari. Prestupnik će, vrlo verovatno, pokušati da uništi sve dokaze koji bi govorili o njegovim aktivnostima na mestu zločina pa tako neki podaci predstavljaju objekat brisanja. Cilj forenzičara je da povрати takve podatke i da njihovom analizom ustanovi da li su dovoljno dobar dokaz za upotrebu u pravnom postupku protiv počinica krivičnog dela.

Znači postoje dva koraka u povraćaju podataka:

1. Hardeverski i
2. Softverski

Hardverski aspekt nije obavezan i sprovodi se samo u slučaju oštećenja medijuma na kojem se nalaze podaci. Važno je istaknuti da se svaka od operacija zamene defektnog hardvera mora izvršiti u potpuno sterilnom okruženju i da i najmanja kontaminacija može rezultirati trajnim gubitkom podataka. Postoje specijalne tzv. čiste sobe u kojima stručnjaci za hardver izvršavaju ove popravke.

Softverski deo je dosta lakši. Softver, nakon pokretanja, traži podatke i u zavisnosti od njihovog stanja na medijumu uspeva da ih rekonstruiše i povрати. Na tržištu je moguće naći veliki broj softverskih paketa koji su namenjeni povraćaju podataka, a na istražitelju je da odabere onaj koji mu najviše odgovara.

7. SASTAVLJANJE FORENZIČKOG TOOLKITA

Krucijalna komponenta svake istrage nekog kompjuterskog zločina je skup specijalizovanih alata (*toolkit*) koji mogu ekstrahovati i pružiti detaljne informacije o kompjuteru ili mreži koju ispitujemo. *Toolkit* može imati dva tipa. Prvi, najčešće komercijalni, predefinisani *toolkit* izrađen od strane nekog softverskog proizvođača i drugi tip, šire rasprostranjen kod početnika, *toolkit* koji korisnik sastavlja po želji, od alata koje želi da koristi. Svaki *toolkit*, bez obzira na tip mora da obuhvati veliki broj alata kako bi mogao da pravilno odgovori na bilo koji tip incidenta. Tu je velika prednost *toolkitova* koji prave specijalizovane forenzičke laboratorije, jer se smanjuje mogućnost da se prilikom sprovođenja istrage neće raspologati odgovarajućim alatima.

Svi alati koje smo do sada predstavili trebali bi da bude deo manuelno napravljenog *toolkita*. Za one koji žele da naprave svoj *toolkit* trebalo bi da imaju u vidu da su sledeće kategorije alata neophodne:

⁷ Data recovery – eng

- Alat za analizu mrežnog saobraćaja,
- Alat za kreiranje fizičke slike hard diska i celog sistema,
- Alat za razbijanje lozinki,
- Alat za skeniranje i rad sa portovima,
- Alat za povratak obrisanih i izgubljenih podataka,
- Alat za rad sa *Registry*-jem,
- Alat za *real time* monitoring aktivnosti sistema,
- Alat za analizu fajlova,
- Antivirusni alati.

8. ZAKLJUČAK

Nema sumnje da će kompjuterska forenzika nastaviti da se razvija i da će postati moćna tehnika za otkrivanje digitalnih dokaza. Da bi taj razvoj bio nesmetan potrebno je da ga prati zadovoljavajuća pravna regulativa i da država ne predstavlja usporavajući faktor. Zemlje zapadne Evrope i SAD su odavno uočile ovu konstataciju i čine sve da pruže pravnu podršku kompjuterskoj forenzici. Naša zemlja kasni u regulisanju ovog pitanja, ali nadu budi predlog zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehničkog kriminala kojim je predviđeno obrazovanje posebnih organizacionih jedinica koje bi se bavile krivičnim delima predviđenim tim zakonom.⁸ Verovatno kao posledica ovog predloga zakona, postoje informacije da će biti formirano posebno odeljenje policije koje bi se bavilo kompjuterskim kriminalom i kompjuterskom forenzikom. Dok se to sve ne ozvaniči ostaje konstatacija da naša zemlja kasni za razvijenim informatičkim zemljama i da bi trebalo unaprediti postojeće stanje. Moguće je da celokupna ekonomska i politička situacija usmerava pažnju relevantnih faktora u državi na neke druge oblasti, međutim ne bismo smeli da dozvolimo da se ovaj problem skloni u stranu. Informaciono društvo omogućava njegovim manje razvijenim delovima da preskoči neke, uglavnom loše, evolucione korake i da implementira dobra rešenja.

Dok se ne donesu pravni mehanizmi nama ostaje da radimo na unapređenju postojeće metodologije i tehnika. Setimo se pitanja sa početka ovog rada. Zakon je jasno definisao dela kompjuterskog kriminala i ulogu kompjutera u svakom od prestupa. U takvom stanju stvari digitalnom dokazu se mora posvetiti velika pažnja. Nije jednostavan zadatak dokazati krivicu pomoću nematerijalnog dokaza. Kompjuterski forenzičari bi morali da se strogo pridržavaju osnovnih koraka u tretiranju digitalnih dokaza. Konsultantsku ulogu bi trebalo da imaju pravnici jer istražitelji ne mogu da znaju vrednost nekog od dokaza na sudu. Ovakva saradnja daje sinergijski efekat jer se pored pribavljanja dokaza dolazi i do povećanja brzine rada. Zato nije neobično što velike advokatske kancelarije imaju u svom sastavu sopstvene forenzičke laboratorije.

Jasnost i očevidnost prestupa je, kad se radi o kompjuterskoj forenzici, u zavisnosti od subjektivnih osobina i iskustva istražitelja. Početnik i iskusan forenzičar neće jednakom dinamikom doći do ispravnog zaključka. Brzina je u pojedinim incidentima imanenta pa je važno odabrati prave nosioce istrage. U direktnoj povezanosti sa ovim pitanjem je alociranje odgovornosti. Brza reakcija pomaže, kod ove oblasti kriminaliteta više nego kod nekih drugih, pronalazak počinioca. Zato je na kompjuterskim forenzičarima zadatak da vrše edukaciju svih oni koji bi mogli biti mete napada nekog malicioznog korisnika.

Kada su tragovi digitalni, kompjuterski, u *cyberspace*-u gotovo da su nevidljivi. Ipak moguće je povezati trag sa pojedincem, ma koliko to bilo teško. Podmetanje zloči-

⁸Član 1. predloga zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehničkog kriminala

na je lako i zapanjuje inventivnost prestupnika. Na istražiteljima je da pažljivo analiziraju dokaze kako ne bi došlo do greške u utvrđivanju odgovornosti. I prestupnici i žrtve bi trebalo da imaju u vidu da ne postoji savršen zločin i da uvek postoje tragovi, a da je na kompjuterskoj forenzici da ih pravilno: otkriju, sačuvaju, analiziraju i prezentuju.

9. LITERATURA

1. Drakulić M (1996), *Osnovi Komjuterskog prava*, Dopis, Beograd,
2. Drakulić M., Drakulić R. (2003), Fakultet organizacionih nauka, Beograd
3. Đurić-Lulić A., Stamenković B. (2003), *Kompjuterski kriminalitet - opasnost na našem pragu*, www.2ojt.sr.gov.yu
4. Marcella I., Greenfield A. (2002), *Computer crimes--Investigation--Handbooks, manuals etc.*, Auerbach publications a crc, Boston
5. Mohay G., Anderson A, Collie B., Vel Rodney D., McKemmish R (2003), *Computer and Intrusion Forensics*, Artech, Boston
6. Potaczala M. (2004), *Computer Forensics*, www.forensics.com
7. Schweitzer D (2003)., *Incident Response: Computer Forensics Toolkit*, Wiley Publishing, Inc., London
8. Vacca J.(2005), *Computer Forensics: Computer Crime Scene Investigation 3rd Edition*, Charles River Media, London