

DIGITALNI DOKAZI

Lazar D. Petrović

Policijska akademija, Humska 22, Beograd

petlaki@ptt.yu

Kratak sadržaj: - Digitalni dokaz je svaka informacija koja ima dokazujuću vrednost, a koja može biti uskladištena ili prenesena u digitalnom obliku. Pojam digitalnog dokaza, u digitalnoj forenzičkoj nauci, obuhvata kompjuterski uskladištene i generisane dokaze, digitalni audio i video signal, zapis sa mobilnog telefona, zapis sa digitalne fax mašine ili drugih digitalnih uređaja. Međunarodna organizacija za kompjutersku registraciju, International Organization of Computer Evidence (IOCE), propisala je opšte **principe i procedure**, koje se odnose na digitalne dokaze, za usaglašavanje metoda i praktičnih rešenja među nacijama i koje garantuju međunarodnu razmenu (transnacionalni menadžment) digitalnih dokaza. Nažalost, nigde u svetu još ne postoji verifikacija zvaničnih istražnih organa, forenzičkih analitičara i pravosudnih organa, podjednako kvalifikovanih u svojim oblastima, da objektivno i tačno vode istragu, forenzičku akviziciju, analizu, dokazni postupak i prezentaciju digitalnih dokaza na sudu. Istraga incidentnog kompjuterskog događaja zahteva uvek timski rad. Za poslove akvizicije i forenzičke analize uvek treba angažovati kvalifikovanog eksperta za informacione tehnologije (IT), specijalistu za konkretni operativni sistem (OS), program, platformu, mrežu, itd.

Ključne reči: digitalni dokaz, istraga, forenzička akvizicija, analiza, dokazni postupak, informacione tehnologije

Abstract: - Digital evidence is every information which has proofing value and which can be stored or transmitted in a digital form. The concept of digital evidence in a digital forensic science embodies computer-stored and generic evidence, digital audio and video signals, mobile phone records, digital fax machine records or records of other digital devices. International Organisation of Computer Evidence (IOCE) has prescribed general **principles and procedures** relating to digital evidence, for the purpose of harmonizing methods and practical solutions among nations, aimed at securing international exchange (transnational management) of digital evidence. Unfortunately, the world does not yet register any verification of official investigating bodies, forensic analysts, and judicial bodies – equally qualified in their fields of expertise – which could objectively and correctly carry out the investigation, collection of forensic evidence, analyses, evidentiary procedure and presentation of the digital evidence before the court. The investigation of an incidental computer event always requires a team work. Qualified IT experts, operational system specialists, programme specialists, platform specialists, network specialists and other experts should always be engaged in the process of collection of forensic evidence and conduct of forensic analysis.

Key words: digital evidence, investigation, forensic acquisition, analysis, evidentiary procedure, information technology

1. Uvod

Glavni cilj istrage u kompjuterskoj incidentnoj situaciji je, kao i slučaju klasičnog kriminala, izgraditi za pravosudne organe neoporiv ili čvrst dokaz krivice ili dokaz za oslobađanje osumnjičenog, i/ili pravedno sankcionisanje učinjenog dela. Pojam **digitalni dokaz** je u ovom radu upotrebljen u smislu “*utvrđivanja dokaza zloupotrebe u sistemima u kojima je primenjena digitalna tehnologija*”, u širem smislu te reči.

U slučaju klasičnog kriminala neoporiv dokaz, na primer ubistva, je pištolj koji se dimi u ruci ubice. Takav direktan (neposredan) dokaz u slučaju kompjuterskog kriminala gotovo

je nemoguće obezbediti. Ipak, moguće je izgraditi čvrst digitalni dokaz, bez tzv. pukotina, od niza posrednih dokaza, kakvi su digitalni podaci po svojoj prirodi.

Prema međunarodnoj definiciji 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. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i generisane dokazne informacije, digitalizovani audio i video dokazne signale, signali sa digitalnog mobilnog telefona, informacije na digitalnih fax mašina i signali 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, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije orginalne digitalne informacije koje imaju dokazujuću vrednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije.

Međunarodna organizacija za kompjutersku registraciju, IOCE, Nacionalni institut za standardizaciju i tehnologiju **NIST** (National Institute for Standardization and Technologies) i američko Ministarstvo pravde **USDJ** (US Department of Justice) su propisali marta 1996. godine, opšte **principe i procedure**, koji se odnose na digitalne dokaze, metode za usaglašavanje praktičnih rešenja među nacijama, koje garantuju međunarodnu razmenu, ili tzv. transnacionalni menadžment, digitalnih dokaza, odnosno prihvatljivost digitalnih dokaza u jednoj zemlji iako su isti prikupljeni u nekoj drugoj zemlji.

Na pripremi standarda za definiciju i menadžment digitalnih dokaza u 2001. godini uzelo je učešće 68 različitih agencija i 73 specijalizovanih jedinica iz 19 zemalja sveta. Za tu priliku upućen je upitnik u više od 200 organizacija, a za pitanja je korišćen IOCE usvojen skup pojmova za digitalni dokaz, forenzičku analizu i analizu digitalnih slika.

U postupku prikupljanja i analize digitalnih dokaza potrebno je pridržavati se određenih principa, koji, između ostalog, određuju menadžment digitalnih dokaza, a to su:

- U postupcima radu sa digitalnim dokaznim materijalima svi generalni forenzički i proceduralni principi moraju biti striktno primenjivani;
- Pre, u toku i posle uzimanja digitalnih dokaza ni jedna preduzeta akcija ne sme da dovede do izmene digitalnog dokaza;
- Samo dobro obučeno lice može pristupi originalnom digitalnom dokazivanju, kada za to postoji potreba;
- Sve aktivnosti koje se odnose na sakupljanje, skladištenje, pristup ili transfer digitalnih dokaza moraju biti potpuno dokumentovane, sačuvane i raspoložive za stavljanje na uvid, bilo kojoj zainteresovanoj strani u sporu;
- Lice koje rukuje digitalnim dokaznim materijalom je odgovorno za sve aktivnosti u odnosu na digitalni dokaz, kada je isti u njegovom posedu;
- Agencija koja je odgovorna za menadžment digitalnih dokaza odgovorna je za usklađenost svih postupnih radnji i aktivnosti u skladu sa ovim principima.

Sudska praksa prihvata kompjuterski generisane i memorisane digitalne dokaze pod adekvatnim uslovima. Transformacija digitalnih podataka, koji se sastoje iz niza kodiranih bita, u sudski dokaz je apstraktan proces koji može navesti sudiju i porotu da dovedu u pitanje autentičnost i integritet kompjuterski generisanog dokaza. U tom smislu, moraju se

na nacionalnom nivou (na nivou zakona ili podzakonskog akta), propisati odgovarajuće procedure, koje obuhvataju: proceduru rukovanja i čuvanja digitalnih dokaza i proceduru za forenzičku akviziciju i analizu digitalnih dokaza [7]. Pojam akvizicije i analize je u ovom radu korišćen u smislu otkrivanja, izvlačenja i dokazivanja digitalnih dokaza u dokaznom postupku.

2. Digitalni kompjuterski dokaz

Digitalni kompjuterski dokaz čini gomila posrednih stvarnih dokaza, od kojih se ni jedan ne sme isključiti iz bilo kog razloga. Dokazi moraju biti potpuni, da se međusobno dopunjuju (da su isprepleteni) i da nemaju tzv. pukotina za donošenje zaključaka, odnosno za utvrđivanje čvrstog dokaza [6].

Najteže je dobiti dokaze bez tzv. pukotina koji potpuno pokrivaju zaključke i objašnjenja. U izgradnji čvrstih (neoborivih) dokaza utvrđuje se: šta se stvarno desilo, šta je izgubljeno, koliki je iznos štete i da li se stvarno dogodio kriminalni akt. Pri tome se mora zadržati potpuna objektivnost. Kada se rekonstruiše hipoteza o događaju, tada počinje prikupljanje dokaza. Dokaze treba prikupljati na mestu kompjuterskog kriminalnog događaja (*sceni zločina*), jer to može biti jedini kontakt sa stvarnim dokazima. Treba raditi metodično, polako i sakupljati ključne stvari. Koristeći zaključke o događaju treba se vratiti na postavljenu hipotezu sa kritičkim pogledom, odnosno postaviti sebi pitanje kako bi lično prihvatio te dokaze ako bi se nalazio na suprotnoj strani. Treba misliti o svakom razlogu: zašto dokaz nije dobar, gde se izgubila neka važna činjenica, kako naći dokaz koji popunjava prazninu, šta uraditi ako se pronađe, itd. U ovoj fazi istrage jednako je važno dokazati kao i opovrgnuti dokaz. Zajednička odbrana u svim kompjuterskim ekscenim situacijama je najčešće teza da se događaj nikada nije dogodio, da je to samo normalna kompjuterska anomalija i.t.d.

Dakle, treba sakupljati sve posredne dokaze sa lica mesta, ne samo što digitalni forenzičar misli da treba, nego i sve ono što može potencijalno indicirati šta se stvarno desilo. U procesu akvizicije digitalnih dokaza, treba generalno snimiti listu datoteka i logova kao dokaze, čak i bez ikakve ideje šta se stvarno dogodilo. Treba imati u dokaznom materijalu svaku datoteku koja potencijalno može sadržavati dokaz, pre nego što ista nestane ili bude promenjen. Nakon inicijalne istrage (bez zaplene računara), treba se okrenuti prvobitnoj hipotezi i dograditi je detaljnije sa prikupljenim dokazima. Velika je verovatnoća da je propušten neki važan dokaz, što je dobar argument da se kompjuter zapleni dok traje istraga (što nije uvek lako). Svaki posredni dokaz, koji zajedno čine dokazni materijal, treba tretirati kao da direktno vodi ka nepobitnom dokazivanju izvršene kriminalne radnje i kao da su svi jednako važni i kritični za konkretni slučaj. Tek tada počinje proces izgradnje dokaza bez tzv. pukotina, odnosno, izgradnja neoborivog dokaza. Potrebno je, dakle, mnogo posrednog dokaznog materijala za jedan mali čvrsti dokaz.

Tri su osnovne kategorije digitalnih podataka koji mogu činiti digitalne dokaze u kompjuterskoj ekscenoj situaciji:

- **Prelazni podaci** ili informacije koje se gube nakon isključivanja računara, kao što su veze sa otvorenom radnom memorijom (RM), rezidentni memorijski programi, itd. Ovi podaci se mogu izgubiti u toku procesa isključivanja računara. Otuda je veoma važno do kraja precizno sprovesti proceduru akvizicije. Pre isključivanja računara treba

odmah ispitati, locirati i izvući osetljive i šifrovane podatke, jer se može desiti da se posle isključivanja ne može doći do njih (npr. vlasnik ključa ili smart kartice za pristup je nekooperativan ili mrtav, itd.).

- **Osetljivi podaci** ili podaci uskladišteni na hard disku (HD) koji se lako mogu izmeniti, kao što je, npr. poslednje vreme pristupa login datoteci itd.
- **Privremeno pristupačni podaci** ili podaci uskladišteni na HD kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

2.1. Pravosudni aspekt digitalnih kompjuterskih dokaza

Podsetimo se kako istražni organi, pravnici i sudije definišu dokazni materijal. Postoje formalna pravila sakupljanja dokaznog materijala, što treba da definiše normativni akt (priručnik ili uputstvo). Međutim, postoji i zakon slučaja (*case law*) koji pokriva definicije i očekivane ishode bazirane na iskustvima i odlukama drugih sudova, a govori kako druge sudije i porote interpretiraju isti zakon.

Kompjuterski kriminal je uneo poseban problem u oblast sudskog veštačenja i svedočenja. Pravilo klasičnog svedočenja kaže da svedok može svedočiti samo ako je očevidac, odnosno samo o onome što je lično iskusio (čuo, video, zna), a ne iz druge ruke, što se smatra posrednim dokazom, poznat u žargonu kao “rekla – kazala” [8].

Međutim, kod računara imamo upravo slučaj da se, sve što se nalazi u njemu, može svesti pod kategoriju “rekla – kazala” dokaze. Naime, ništa direktno vezano za događaj se ne vidi u računaru, jer se login datoteka može naknadno izmeniti, promeniti datum datoteke, izbrisati ili izmeniti dokument, što praktično znači da samo osoba koja je izazvala kompjuterski incident (kompjuterski kriminalac) ima direktno saznanje o tome i jedini je očevidac, odnosno neposredan svedok. Dakle, kompjuterski podaci se mogu koristiti kao dokazi za svedočenje samo ako su veoma pažljivo preuzeti i ako zadovoljavaju neke specifične kriterijume u sudskom veštačenju (forenzičkoj akviziciji i analizi). Ovi su kriterijumi kritični u pogledu sposobnosti forenzičkog analitičara da sakupi što više posrednih dokaza pomoću kojih se dolazi do neoporivog dokaza. Praktično, posredni su svi dokazi u kompjuterskom kriminalnom aktu koji se sakupe analizom samog softvera, računara i/ili računarske mreže. Da bi posredni dokaz bio prihvatljiv za sud mora biti takav da potvrđuje hipotezu o čvrstom dokazu, ili da je pobija. Drugo, mora postojati dokaz da je login datoteka, kao posredni dokaz, nastala u normalnom radnom procesu, pa je, npr. potrebno imati čvrste dokaze da je počinilac bio logovan kada je server pao. Ovo je dovoljno čvrst dokaz i opravdava postupak da nadležni organ istrage službeno zahteva prisluškivanje linije osumnjičenog te da se snimi vreme pristupa serveru, koje se kasnije upoređuje sa login podacima u log datotekama računara i aktivnostima drugih mrežnih uređaja i utvrđuje kao neoporiv dokaz pristupa serveru.

Kompjuterski dokaz mora biti autentičan. Sudski veštak za informacione tehnologije (IT veštak), mora potvrditi da je dokaz nepromenjen u odnosu na originalno stanje. Ovo je od kritičnog značaja za prihvatanje dokaza na sudu (*forensic evidence*). Kako su dokazi pribavljeni, čuvani, prenošeni, zaštićeni od izmena i kako se sa njima manipuliralo, ključni su elementi da li će biti na sudu prihvaćeni ili odbačeni. Prethodno, originalno, stanje digitalnih dokaza moraju utvrditi sudski veštaci za IT svojim svedočenjem, kao i forenzički analitičari i organi istrage koji su te dokaze sakupili, čuvali, analizirali i rukovali njima.

Digitalni kompjuterski dokazi moraju zadovoljiti i sve ostale zahteve pravosudnih organa, koji se odnose na sudske dokaze i to:

- ako je potrebno koristiti kopiju, ona mora biti najbolja,
- ako je original na raspolaganju onda kopija ne važi,
- kopija može zadovoljiti sve zahteve za izvođenje dokaza (npr. printing login datoteka), ako postoji originalna datoteka u kompjuteru za upoređenje,
- sudski veštak za IT mora posvedočiti kako je kopija (npr. printing login datoteke) napravljena, kao i druge detalje rukovanja sa datotekom i kopijom (printingom).

2.2. Menadžment digitalnih kompjuterskih dokaza

Menadžment digitalnih kompjuterskih dokaza koji obuhvata sakupljanje, prenos, analizu i čuvanje, zahteva posebnu diskusiju. Dokazi se čuvaju tokom čitavog lanca istrage (*chain of custody*), lanca dokaznog postupka i suđenja, što znači da je dokaz u posedu suda od trenutka akvizicije do završetka suđenja. Prikupljeni dokaz se mora čuvati od štetnih uticaja koji mogu dovesti do oštećenja: toplote, hladnoće, vode, dejstva magneta, itd.). Svaku datoteku treba "bekapovati" i uskladištiti sa digitalnim potpisom (DS), npr. CRCMD5¹, koji kreira siguran heš (*hash*). Sud može prihvatiti digitalno potpisan (heširan) dokaz kao originalan, jer svaka izmena datoteke uništava heš koji je digitalni pečat potpisa, što se lako utvrđuje poređenjem. Dobro bi bilo memorisati digitalni potpis u tekst podataka dokaza, sve šifrovati sa PGP² ključem i tako uskladištiti i čuvati.

U oblasti korporacijske i zvanične istrage kompjuterskog ekscenog događaja, ne samo da svedoci i eksperti moraju biti pouzdani, nego i softverski i hardverski alati za forenzičku akviziciju i analizu digitalnih dokaza. Načelno, softverski i hardverski forenzički alati, programi za praćenje saobraćaja i detekciju upada u radnu memoriju treba da budu namenski, komercijalno dostupni proizvodi sa sertifikatom o pouzdanosti za ovu vrstu poslova. Tako npr. digitalni dokazi sakupljeni na ilegalan način (npr. bez upotrebe pouzdanih i sertifikovanih forenzičkih alata) mogu biti problematični ili odbačeni od strane suda. Zato treba dokazati da stavljanje *snifera*³ na mrežu nije namenjeno za prisluškivanje privatnih lica i ugrožavanje njihovih ljudskih prava, nego za dokazivanje upada osumnjičenog lica u informacioni sistem.

Digitalni dokaz podrazumeva da postoji pravo vlasništva nad informacionim sistemom, datotekama i softverima koji su oštećeni. Drugim rečima, ako se ne može dokazati da je nešto lično (privatno), onda se ne može ni optužiti neko da je to ukrao, ošteti i/ili izmenio. Prava vlasništva u informacionim sistemima uspostavljaju, tajne lozinke, mehanizmi kriptozastite i drugi mehanizmi kontrole pristupa, skrivene datoteke, razna upozorenja, koja sugerišu da je to vlasništvo i da bez eksplicitne dozvole vlasnika nema pristupa.

U dokazivanju kompjuterskog ekscenog događaja najbolje je doći do računara osumnjičenog, a kako to često nije moguće onda barem do fizičke (miror) slike njegovih

¹ CRCMD5 – NTI standardna hash funkcija za digitalni potpis

² PGP – *Prity Good Privacy*, kriptozastitni sistem sa javnom distribucijom ključa i asimetričnim algoritmom

³ *snifer* – uređaj za praćenje rada osumnjičenog u informacionom sistemu

hard diska (HD). Na osnovu te slike treba formirati HD na forenzičkom (ispitnom) računaru, koji mora biti pouzdan fizički duplikat HD računara osumnjičenog.

Ako inicijalna istraga unutar funkcionalnog sistema (zatvorene računarske mreže) utvrdi da je napad došao izvan tog IS, i ako menadžer ili vlasnik IS donesu takvu odluku, onda se u toj tački moraju angažovati zvanični organi istrage, da bi se dobio nalog suda za pretres i zaplenu osumnjičenog računara, radi akvizicije digitalnih dokaza. Ako je napad došao iz druge organizacije (u istoj državi), treba doći do lokalnog administratora IS te organizacije i sa njim nastaviti istražni postupak. Osumnjičeni računar obavezno treba zaštititi od kompromitacije (izmene), kad god se dođe do njega.

2.3. Procedura sakupljanja posrednih kompjuterskih dokaza

U procesu akvizicije koja obuhvata otkrivanje, identifikaciju, izvlačenje i sakupljanje digitalnih kompjuterskih dokaza, samo prikupljanje digitalnih dokaza zaokružuje se kroz nekoliko faza akvizicije:

1. Sakupljati sve podatke koji podržavaju prvu hipotezu o tome kako je došlo do kompjuterskog ekscesnog događaja, odakle je napad potekao i šta je urađeno na napadnutom računaru.
2. Sakupiti sve podatke koji su kontradiktorni postavljenoj hipotezi, da bi se podržalo dato objašnjenje ili lakše suprotstavilo napadu druge strane u sporu. U većini slučajeva, posebno u kriminalističkoj proceduri, treba imati na umu da obe strane žele da otkriju i podnesu *neoborive dokaze*.
3. Sakupiti sve flopi diskove otkrivene na lokaciji osumnjičenog računara i analizirati ih. Ta analiza se može vršiti programom za analizu flopi diskova (npr. alatom tipa **Sydex Anadisk**). Takođe se moraju sakupiti svi štampani materijali, rukopisi, zabeleške, trake, CD ROM – ovi ili drugi materijali, koji mogu ukazati na rasvetljavanje spornog događaja.
4. Napraviti skice ili fotografije osumnjičenog računara i svih perifernih uređaja, sačuvati i označiti sve periferne uređaje i kablove za ponovnu montažu u forenzičkoj laboratoriji.
5. Ako postoji matrični ili impakt printer, ukloniti ribon i staviti novi. Originalni ribon ispitati kao dokazni materijal. Ako postoji displej na kompjuterskom ekranu, fotografisati ga.
6. Isključivanje osumnjičenog računara je posebno osetljiva operacija. Zavisno od operativnog sistema (OS), postoje dve mogućnosti. Napadnuti računar se može isključiti na klasičan način bez straha da će se izbrisati dokazi o upadu, ili se osumnjičeni računar ne sme isključivati, jer bi se isključivanjem mogu uništiti dokazi o upadu. Ako se **Unix** mašine ne isključe propisno može doći do oštećenja datoteka. Međutim, u ovim sistemima se pak lako kreiraju *boby zamke* za uništavanje datoteka sa dokazima, ako se računar isključuje po propisu. Zato uvek postoji dilema da li računar isključiti propisno i sprečiti uništavanje nekih datoteka, ili ga isključiti nepropisno čime se omogućava aktiviranje *boby* zamke koja može da uništi dokaze. Kako će postupiti u konkretnom slučaju, to sam istražni organ mora proceniti. U ovom slučaju najbolje je koristiti pomoć sudskog veštaka, eksperta za IT, odnosno specijaliste za dati OS i platformu, kome se mora dobro objasniti legalni aspekt zahteva za zaštitu integriteta digitalnih dokaza.

7. Ako je sigurno da postoji ugrađena zamka, najbolje je računar jednostavno isključiti iz mreže, uz rizik da će biti uništene neke datoteke. Naravno, neki računari tako ne mogu da se isključe (mainframe i mikrokompjuteri). Zato je potrebno angažovanje eksperta za IT, koji treba da onesposobi svaku logičku bombu sakrivenu u napadnutom računaru.
8. Za rebutiranje ispitivanog računara nikada ne treba koristiti njegov OS i interpretator komandi (tastaturu). Računar treba butirati sa butabilnog flopi diska, koji je fizički zaštićen od upisivanja, čime se sprečava unošenje virusa ili sa CD ROM – a koji je fizička slika operativnog sistema.
9. Kada se završi rebutiranje sistema, prvo se uzima fizička slika OS i HD – a (alatom tipa **Drivespay** ili **Image**), zatim se sakupljaju drugi dokazi i preliminarno analiziraju. Najbolji način za skladištenje mirror slike HD je optički disk (CD), jer je otporan na oštećenja usled elektromagnetnih zračenja iz okruženja, tj. ne može se brisati (osim ako je CD tipa *rewritable*), a može se lako kopirati.
10. Zaplenjeni osumnjičeni računar sa svim magnetnim medijima, uskladištiti na bezbedno mesto, zaštićeno od uticaja okoline, posebno elektromagnetnih polja i obezbediti ga od neovlašćenog pristupa, jer se veštak mora zakleti na sudu da dokazni materijal nije bio dostupan neovlašćenim osobama.
11. Za razliku od pisanog dokaza, elektronski digitalni dokaz često može egzistirati u različitim formama ranijih verzija, koje su još dostupne na HD. Poznavanjem lokacija njihovog postojanja i korišćenjem adekvatnih alata za forenzičku akviziciju, čak i izmenjeni formati istih podataka mogu se lako otkriti. Proces akvizicije najbolje poznaje iskusni ekspert za IT, koji brže otkriva moguće dokaze. Osim toga, u slučaju preliminarnog ispitivanja i identifikacije digitalnih dokaza na licu mesta, kada se računar iz nekog razloga ne zaplenjuje u cilju istrage, niti se pravi forenzična kopija HD, ekspert za IT brže identifikuje skrivena, nelocirana i izbrisana mesta koja treba gledati, znake koje treba tražiti i dodatne izvore informacija za relevantne dokaze. Dodatni izvori informacija mogu biti ranije forme datoteka podataka (npr. u *Memos*, *Spreadsheets*, ...) koje postoje na HD, ili u bekap mediju, ili različito formatirane verzije podataka (npr. *.templates*, *.doc*, *.pdf* i sl.), bilo da su tako namerno formirane ili tretirane drugim aplikativnim programima (npr. *Word processing*, *spreadsheet*, *e-mail*, *timeline*, *scheduling*, *graphic*).
12. Zaštita integriteta dokaza je kritična faza. Iskusan ekspert za IT mora obezbediti:
 - da ni jedan mogući dokaz ne bude oštećen, uništen ili kompromitovan na neki način sa procedurom forenzičke akvizicije i analize računara,
 - da se ni jedan mogući kompjuterski virus ne sme ubaciti u ispitivani računar u toku procesa akvizicije i analize,
 - da se sa izuzetom i potencijalno relevantnim dokazima propisno manipuliše i da se isti štite od eventualnih mehaničkih ili EM oštećenja,
 - da se uspostavi neprekidni lanac menadžmenta (čuvanja i održavanja integriteta dokaza),
 - da funkcionalni aspekt bude ugrožen ograničeno kratko vreme ili nikako,
 - da se dobije bilo koja potrebna informacija u toku forenzičke akvizicije i analize, od kljijenta ili advokata koji su prema etičkom kodeksu dužni pružiti sve neophodne informacije forenzičkom ekspertu za IT.

2.4. Korisnici kompjuterskih digitalnih dokaza

U procesu vođenja postupka mnogi organi i institucije mogu zahtevati i koristiti kompjuterske digitalne dokaze, kao što su:

- tužilaštvo,
- pravosudni organi u privatnom parničkom postupku (pronevera, razvod, diskriminacija, uznemiravanje, i sl.),
- osiguravajući zavodi, za moguću prevaru u slučajevima kompenzacije oštećenih lica i sl.
- organizacije (vlasnici napadnutog informacionog sistema),
- zvanični istražni organi (MUP, BIA, VBA),
- pojedinci (vlasnici napadnutog IS),
- udrženja IT veštaka.

Nažalost, nigde u svetu još ne postoji generacija zvaničnih istražnih organa, forenzičkih analitičara i predstavnika pravosudnih organa (tužilaštva i sudstva), koji su podjednako kvalifikovani u svojim oblastima da objektivno i tačno vode, istragu, forenzičku akviziciju i analizu, dokazni postupak i prezentaciju digitalnih dokaza na sudu.

3. Priprema digitalnih dokaza za prezentaciju pred sudom

Nezavisni ekspert za IT koji pomaže istražnom organu u otkrivanju i akviziciji podataka treba da ima iskustvo iz široke oblasti informacionih tehnologija. Takav ekspert je uvek od velike koristi kada se vrši istraga konkretnog kompjuterskog ekscesnog događaja. Međutim, iako je osnovni dizajn računara i aplikativnog softvera često sasvim sličan kod većine OS, pa se znanja iz jednog sistema lako prenose na drugi sistem, ipak za poslove akvizicije i forenzičke analize uvek treba angažovati kvalifikovanog eksperta za IT, specijalistu za konkretni OS, program, platformu, mrežu, itd.

Digitalne dokaze od trenutka otkrivanja do zaključno sa forenzičkom analizom, treba uvek tretirati kao da će biti prezentirani na sudu. Na sudu u parničkom ili krivičnom postupku, zavisno od težine ekscesnog kompjuterskog događaja, digitalne dokaze prezentira sudski veštak za IT, zakleti sudski svedok, kvalifikovan za predmetni hardver i softver, krajnje objektivno, tačno, uverljivo i razumljivo. U najvećem broju slučajeva digitalne dokaze na sudu prezentira ekspert za IT koji je u toku istrage vršio akviziciju i forenzičku analizu digitalnih dokaza. Naravno, obe strane mogu zahtevati i druge, nezavisne veštace za IT, što neminovno podrazumeva unakrsno ispitivanje i sučeljavanje mišljenja dva veštaka za IT podjednako istih znanja i iskustava. To je u praksi često faktor odvratanja, jer istaknuti eksperti za IT odbijaju sudsko veštačenje i sučeljavanje mišljenja sa drugim podjednako dobrim sudskim ekspertom i radije prihvataju ulogu neutralnog stručnog konsultanta tužioca ili samog sudijske.

U pripremi za prezentaciju digitalnih dokaza na sudu veštaci za IT moraju obaviti mnogobrojne konsultacije sa advokatom stranke koja ih angažuje (tužilaštva ili odbrane), za izbor metode prezentacije (korišćenje pomoćnih audio – vizuelnih sredstava, strategiju nastupa, i sl.), a sami se psihički pripremaju za unakrsno ispitivanje i eventualno suočavanje sa svedočenjem drugog veštaka za informacione tehnologije.

4. Preopruke IOCE za menadžment digitalnih dokaza

Danas u svetu postoji čitav niz preporuka, između ostalih i preporuke IOCE, kojima se definišu postupci sa prikupljenim i obrađenim dokaznim materijalom. Preporuke IOCE se sastoje u sledećem [6], [10] :

- a. Za čuvanje originalnih (miror) snimaka digitalnih dokaza **nisu prihvatljivi** sledeći medijumi: instant film paket, inject printeri, ink printeri, termalni voštano – papirni printeri, *dye* sublimacioni printeri, suvo srebreni printeri, laserski printeri i elektrostatički printeri.
- b. Za čuvanje originalnih snimaka digitalnih dokaza **prihvatljivi su**, zbog kvaliteta, trajnosti i pouzdanosti sledeći medijumi: klasični filmovi na bazi srebro – oksida, izuzev instant fotografije, CD ROM za jedno upisivanje (*non RW*), digitalni CD ROM za upisivanje (*RW CD ROM*).
- c. Za čuvanje originalnih snimaka digitalnih dokaza **mogu se koristiti**, uz kontrolu eventualnih gubitaka podataka, sledeći medijumi: odvojeno razvijen instant film, fotografski print, diskete, magnetske trake, fiksni HD, prenosni magnetni medij, kompakt fleš medij, PC kartice, smart kartice, prenosni magnetno – optički drajvovi i magnetno – optički drajvovi za jedno upisivanje.
- d. Za čuvanja originala i procesiranje nakon akvizicije mogu se koristiti: **film** na kome se može procesirati original (ako proces nije destruktivan), **analogni video** se preporučuje za minimalno procesiranje originala, (da bi se izbegla degradacija signala. Ako za procesiranje treba koristiti original, mora se napraviti kopija pre procesiranja i analize), **digitalni format** za koji je potrebno za procesiranje napraviti miror duplikat (fizičku sliku) i koristi ga kao radnu verziju.
- e. **Dokumentacija za procesiranja slike** mora biti precizna, detaljna, neporeciva i napravljena na poverljivom sistemu.
- f. **Verifikacija originala i procesiranih slika** mora biti obavezna i da nepobitno potvrđuje da nije bilo povrede integriteta originalnih digitalnih dokaza.
- g. **Čuvanje originala u lancu istrage** je stroga obaveza u celom lancu od pokretanja istrage i otkrivanja dokaza do svedočenja na sudu. Ova procedura se mora administrativno propisati u svakom pravosudnom sistemu. Takođe mora postojati zakonska obaveza svakog pojedinca koji dođe u kontakt sa originalnim digitalnim dokazom u istražnom, dokaznom i pretresnom postupku, da čuva dokaz od izmene, oštećenja ili brisanja (nestanka).

5. Predlog elemenata za

“Uputstvo za čuvanje i rukovanje sa digitalnim dokazima”

Uputstva za menadžment (čuvanje i rukovanje) digitalnim dokazima (u daljem tekstu: **Uputstvo**) propisuje Ministar pravde podzakonskim aktom.

1. Uputstvo primenjivati za slučajeve kada je došlo do zloupotrebe u korišćenju informacionih tehnologija ili nekog drugog oblika kompjuterskog kriminala, u parničkom i krivičnom postupku.
2. Zvanični organi istrage (Odeljenje za suzbijanje kompjuterskog kriminala MUP) od trenutka zaplene osumnjičenog računara, radi utvrđivanja dokaza, treba da znaju sva zakonska i tehnička pitanja, neophodna za otkrivanje, utvrđivanje i prezentaciju digitalnih kompjuterskih dokaza pred sudom, u skladu sa ovim Uputstvom.
3. Pravosudni organi treba da uvažavaju specifičnost digitalnih kompjuterskih dokaza, pošto se mogu formirati, menjati, skladištiti, kopirati i prenositi sa neverovatnom lakoćom, što za pravnike i pravosudni sistem predstavlja veliki problem u procesu utvrđivanja činjenica.
4. Digitalni kompjuterski dokazi se u mnogo čemu mogu tretirati i ispitivati kao i svi ostali klasični dokazi kriminalnog akta. Zato sa pravnog aspekta treba postavljati pitanja generalne verodostojnosti i pouzdanosti kompjuterskih dokaza, a ne da li su oni pouzdani i verodostojni u svim svojim aspektima. Svakako, ispitivanje kompjuterskih digitalnih dokaza zahteva i jednu vrstu interne autentifikacije ispitivača i vremena pristupa, što povećava pravnu pouzdanost dokaza.
5. Pravosudni organi treba da razumeju suštinu stvarne prirode digitalnih kompjuterskih dokaza, za koju namenu i sa kojim humanim i tehnološkim procesom su dokazi formirani.
6. Osnovno pravilo najboljeg dokaza u zakonskoj regulativi dokazivanja dela klasičnog kriminala, navodi da je direktan, originalan dokaz – najbolji dokaz, odnosno da se dokaže sadržaj rukopisa, tonskog snimka ili fotografije, treba posedovati orginale ovih dokumenata.
7. U slučaju digitalnih kompjuterskih dokaza zahtev za «originalom» ili direktnim dokazom mora se preispitati i revidirati. Upisivanje i snimanje u računaru podrazumeva mehaničke, magnetne i elektronske metode upisivanja slova, reči, brojeva ili njihovih ekvivalenata. Na taj način, digitalni dokument formiran na hard disku sadrži ekvivalentne elektronske podatke, koji su prihvatljiv zapis za pravosudne organe.
8. Ako su dokazni podaci memorisani u računaru ili sličnom uređaju, svaka štampana kopija ili drugi izlazni dokument, vizuelno čitljiv ili prikazan tako da tačno reflektuje podatke sa HD, takođe se smatra originalnim digitalnim dokazom.
9. Svaki duplikat ili fizička (mirror) slika originalnih digitalnih podataka prihvataju se kao original, sve dok se ne pokrene suštinsko pitanje o autentičnosti istog, ili ne postane neophodno da se pred pravosudnim organima prezentuju originalni podaci.
10. Ako je kopija proizvedena istim otiskom kao i original, mehaničkim ili elektronskim ponovljenim snimanjem ili drugom ekvivalentnom tehnikom, koja tačno reprodukuje original, onda je duplikat prihvatljiv kao originalni dokument.
11. Forenzičke agencija za ispitivanje digitalnih dokaza treba da koriste podatke sa preciznih elektronskih kopija tzv. «fizičkih ili mirror kopija niza bitova» koje se dobiju odgovarajućim forenzičkim softverskim alatima. Sve dok je takva kopija propisno generisana, čuvana i korišćena, za sud je prihvatljiva kao i originalni elektronski dokument. Drugim rečima, i originalni elektronski dokument i njihove kopije svake vrste i na svakom nosiocu prihvatljive su za sud. Pitanje koje pravosudni organi treba da postavljaju su: da li su originalni podaci autentični i da li je napravljena tačna kopija, a ne na kojem se nosiocu (HD, flopi, papirna kopija i sl.) dokazni dokument nalazi.
12. U sudskom procesu, kod prezentacije svakog elektronskog digitalnog dokaza mora se biti spreman za autentifikaciju, odnosno verifikaciju identiteta predmetnog digitalnog dokaza. Najčešći metod autentifikacije elektronskih digitalnih dokaza je prikazivanje identiteta dokaza kroz neke njegove osobine, koje mogu biti standardizovane i

propisane, pomoću nekih karakteristika ili elemenata kvaliteta, kao što su: posebnosti u izgledu, sadržaju, materiji, internom formatu ili drugim karakteristikama, uzetim zavisno od konkretnih okolnosti. Na primer, identifikacija digitalne fotografije od strane svedoka često se dovodi u pitanje baš iz razloga što se radi o fotografiji koja se može lako promeniti bez vidljivih tragova. Zato je potrebno da svaka digitalna fotografija, posebno za forenzičku analizu, ima neizbrisiv (kriptozaštićen) digitalni vođeni pečat (DVP), ili elektronski digitalni potpis (DS), koji evidentira vreme snimanja, kratak sadržaj snimka, mesto snimanja i sl. U tom slučaju DS ili DVP je taj posebni element za autentifikaciju dokumenta (fotografije), pošto je digitalni potpis inače priznat od strane pravosudnog sistema.

13. Za sud je prihvatljiv i onaj digitalni dokaz, za koji sud zna relevantne detalje o dokazu (dokumentu, fotografiji) i ako svedok koji se smatra najpouzdanijim, verifikuje sve relevantne detalje iz dokumenta. Ključno pitanje ostaje koliko se tačno svedok seća svih detalja iz stvarne scene prikazane na običnoj ili digitalnoj fotografiji (dokumentu) u sudu, jer se ključni markeri zločina mogu lako, neznatno ili bitno, izmeniti, pogotovu na digitalnoj fotografiji (dokumentu), tako da mogu potpuno da zbune svedoka i dovedu ga u nedoumicu. Zato pravosudni organi moraju znati da posebne karakteristike autentifikacije elektronskog dokumenta ne moraju zadovoljiti sud, jer se lako mogu menjati.
14. Čuvanje elektronskih digitalnih dokaza mora biti striktna obaveza, i to od trenutka njegovog uzimanja do prezentacije pred pravosudnim ili drugim organima u neizmenjenoj, autentičnoj formi i da za to snose odgovornost sva lica koja koriste dokaze u celokupnom lancu, od procesa istrage do suđenja.
15. U slučaju digitalnog kompjuterskog dokumenta ili fotografije, odnosno video snimka sud može zahtevati ekspertsko svedočenje (tzv. IT veštačenje). Mora se uspostaviti neprekidnost lanca čuvanja integriteta digitalnih dokaza od forenzičara za IT ili kriminalističkog tehničara (fotografa) do forenzičkog analitičara koji je proizveo kopiju dokaza i prezentira je na suđenju. Svedočenje je lakše ako se kopija digitalnog dokumenta (npr. fotografija) napravi u istom trenutku kada je izvršeno snimanje. U protivnom, veštak za IT mora razjasniti kako je, od izmena u međuvremenu, čuvan originalni dokument (snimak).
16. U slučaju elektronskih procesiranja dokumenta u računaru koja menjaju barem formu informacija, a ponekad i sadržaj (komparacija, računanje, evaluacija, pregrupisavanje ili selektivno izvlačenje), ne znači da je dobijeni dokument neprihvatljiv, nego samo da treba preduzeti drugi analitički korak. Pored toga, svi kompjuterski programi unose neizbežno određene gerške (*bagove*) koje takođe menjaju digitalna dokumenta. Čak iako nema grešaka u izvornom kodu programa, operater može aktivirati program na takav način koji će stvoriti lažne rezultate. Na primer, posebni kompjuterski programi za pretraživanje (*search file*) mogu biti osetljivi na veličinu slova (*case sensitive*), što znači da velika i mala slova bilo kojeg datog slova nisu međusobno zamenjiva. Recimo u WordPerfectu traženje reči "evidence" nije moguće, jer *e* nije veliko slovo *E*.
17. Pitanje pod kojim okolnostima sud može prihvatiti dokaz ako računar na komandu traženja neke reči (*search*) odgovori da je ne može naći (*not found*). Na primer, ako tužilac traži od ispitivanog računarskog sistema da proveri da li je klijent platio porez za prošlu godinu, računarski sistem može dati originalni dokument (*printing*) ili prihvatljivu elektronsku kopiju. Ali, ako ispitivani računarski sistem pretražuje bazu podataka i ne pronade odgovor, zbog takvog procesiranja računara, prema Pravilniku sud treba da dopušta takvu mogućnost, a takav dokaz (da nema dokaza), da se prihvata nakon što «uporno pretraživanje nije uspeo otkriti dokaz u računaru». Pitanje je kakvo IT veštačenje može biti u ovom slučaju ispravno i prihvatljivo? Da li veštak za IT treba

da svedoči koja je slova otkucao za traženje, ili da li je imao programsku logiku bez bagova, da li program traži i za velika i za mala slova imena poreskog obveznika, i slično.

18. U meri u kojoj pravnici i sudije više saznaju o svim ranjivostima i teškoćama u stvaranju dokaza kroz kompjutersko procesiranje, oblast IT veštačenja će biti sve manje usko grlo za eksperte za informacionu tehnologiju.
19. Iz osnovnog pravila o neprihvatanju posrednih dokaza tipa "rekla – kazala" (*Hear say rule*), izuzimaju se poslovni dokumenti u sledećem slučaju: "Svaki memorandum, izveštaj, snimak ili kompilacija poslovnih podataka, sačinjena u vreme ili oko događaja od strane ili na osnovu informacije koju je prenela osoba koja to zna, privatljiv je ako je snimak čuvan u toku regularno vođenog posla i ako je bila regularna praksa da se pravi snimak (izveštaj)".
20. Digitalne informacije se procesiraju i rearanžiraju u računaru, što je prihvatljiva praksa bez obzira na mogućnosti unošenja grešaka i bagova procesiranja (tehnički i ljudski faktor). Ako je to prihvatljivo za poslovne informacije, trebalo bi biti prihvatljivo i za sud. Naravno postoji razlika u korišćenju kompjuterskog procesiranja sirovih poslovnih informacije (npr. banke) od procesiranja na novi medijum i na neuobičajen način za pravljenje digitalnih podataka kao dokaza za suđenje. Na primer, može se prihvatiti procesiranje u zahtevu za izveštaj o mesečnim kretanjima na računu klijenta, ali šta je sa, npr. kretanjem svih isplata na računu Švajcarske banke u toku protekle godine, gde je neophodno višestruko pretraživanje. Da li se takav izveštaj može bezuslovno prihvatiti kao validan dokaz? Čak iako izveštaj nije sačinjen u vreme ili oko događaja, za sud ovaj dokaz može biti prihvatljiv prema Pravilniku koji prihvata "karte, kratke sadržaje ili obračune, kao zamenu za obimna pisanja, snimanja ili fotografije". Naravno, uvek se može dovesti u pitanje kompjuterski proces koji kreira sažetak dokaza.
21. Nasuprot korektno autentifikovanih dokaza, elektronski digitalni dokumenti mogu sadržavati svaku vrstu *rekla - kazala* izjave za koje nema izuzetaka. Kompjuter i njihovi proizvodi nisu inherentno pouzdani i uvek je mudro u svakom slučaju pitati koji je kompjuter korišćen i kako je napravio taj proizvod.

6. Zaključci

Digitalni dokaz je svaka informacija uskladištena ili prenesena u digitalnoj formi, koja ima dokazujuću vrednost i na koju se sud može osloniti. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i generisane dokaze, digitalni audio i video materijal, digitalni zapisi na mobilnom telefonu, digitalnoj fax mašini i drugim digitalnim uređajima.

Očekuje se da forenzička analiza digitalnih dokaza otkrije najviše potrebnih podataka za izgradnju čvrstog, neoborivog digitalnog dokaza bez tzv. pukotina. Postoji velika razlika između kompjuterskog digitalnog dokaza u računaru (*computer evidence*) i čvrstih, neoborivih dokaza (*proof*) prihvatljivih na sudu. Neoborivi, čvrsti dokaz nepobitno uspostavlja činjenice, ali je to i subjektivna interpretacija kompjuterskog digitalnog dokaza koji izvodi veštak za informacione tehnologije. Kompjuterski digitalni dokaz u računaru je objektivni digitalni podatak i može se koristiti u meri u kojoj se može dokazati da nije izmenjen, npr. ulazna log datoteka je uvek ulazna log datoteka.

Pri akviziciji kompjuterskih digitalnih dokaza treba uvek verovati u indikacije koje pokazuje istraga, sve dok se ne sastave svi delići posrednih digitalnih dokaza u čvrsti

dokaz bez tzv. pukotina. Treba tražiti nekonzistentnosti, ali prihvatiti i ono što se vidi, bez racionalizacije.

Ako se u toku forenzičke akvizicije digitalnih dokaza dobiju konflikti podaci, treba se vratiti korak unazad i pokušati otkriti šta se stvarno vidi. Možda konflikt uopšte i ne postoji. Ukoliko konflikt postoji, ne pokušavati njegovo rešavanje racionalizacijom.

Ni u kom slučaju ne menjati ništa u ispitivanim računarima, sa kojih se u procesu akvizicije digitalnih dokaza sakupljaju digitalni podaci i ne objavljivati nalaze forenzičke analize digitalnih dokaza u toku istrage. Treba uvek računati da će slučaj ići na sud, a napadač bi u međuvremenu mogao izmeniti svoj računar i izbrisati sve podatke i eventualne tragove napada, koji mogu biti potencijalni digitalni dokazi.

U periodu nepostojanja nacionalne zakonske regulative, preporuka, standarda, principa i procedura istrage, slučajeva kompjuterskog kriminala i zloupotreba u IT, akvizicije i analize digitalnih dokaza i veštačenja pred sudom, treba u što je moguće većoj meri koristiti odgovarajuća, međunarodno priznata rešenja (IOCE).

7. Literatura

1. Carrier B., *Defining digital Forensic Examination and Analysis Tools Using Abstraction layers*, International Journal of Digital Evidence, Vol.1, No. 4, 2003.
2. <http://www.atstake.com>.
3. <http://www.ensfi.org>.
4. <http://www.iacis.org/>
5. <http://www.ojp.usdoj.gov/nij/pubs.htm>.
6. *IOCE Principals & Definitions*, IOCE 2. Conference, 7. 10. 1999., Marriott Hotel, London
7. Krsul I. and Spafford E. H., *Authorship Analysis: Identifying the Author of a Program*, Department of Computer Sciences, Purdue University, CSD – TR – 96 - 052, 1996.
8. Pettinari D., Cmdr., *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, juni 2000.
9. Pollit M. Mark, *Report on Digital Evidence*, (FBI CART report, DC Washington, USA), Interpol Forensic Science Symposium, Lyon, France, 16 - 19. 10. 2001.
10. Whitcomb C. Morgan, *A Historical perspective of Digital Evidence: A Forensic Scientist's View*, International Journal of Digital Evidence, proleće 2002, vol.1, issue 1.