

FUNKCIONALNI MODEL ISTRAGE KOMPJUTERSKOG DOGOĐAJA

Mr Gojko Grubor, dipl. inž.

Udruženje "IT Veštak"

Kratak sadržaj

Za 60 godina razvoja *kompjuterski digitalni dokazi* su evoluirali u *digitalne dokaze*, koji uključuju kompjuterske digitalne dokaze, digitalne audio i video, mobilni telefon i razne druge digitalne podatke i uređaje. Naučna forenzička analiza digitalnih dokaza razvija se poslednjih 25 godina. Objavljeni su standardi, preporuke, osnovni principi, kriterijumi i procedure istrage kompjuterskog događaja i menadžmenta digitalnih dokaza (SWGDE¹ i IOCE², 1999.).

Istraga, forenzička akvizicija i analiza obezbeđuju čvrste dokaze u slučaju kompjuterskog događaja. Forenzička akvizicija i analiza odnose se na analizu softvera, računara i medija i računarskih mreža. Forenzička akvizicija i analiza digitalnih dokaza u istražnom potupku, vrše se prema standardnoj proceduri i sa standardnim, verifikovanim forenzičkim tehnikama i alatima.

Ključne reči: *incident, istraga, digitalni, forenzički dokazi, procedure, akvizicija, analiza, tehnike, alati*

Abstract

Computer digital evidence has been evolving into *scientific digital evidence* during last 60 years of its development. The scientific digital evidence involved computer digital evidence, digital audio and video, mobile phone and some other digital data and devices. The scientific forensic digital evidence have been developing during last 25 years. Principles, criterias and standard operation procedures (SOP) for computer incident investigation and digital evidence management were published in 1999 (SWGDE³ and IOCE⁴), Investigation, acquisition and forensic digital evidence provide digital proves in computer incident cases. Acquisition and forensic digital evidence analysis involve software, hardware, electronic media and computer network. They are performed through the SOP using standard and verified forensic techniques and tools.

Key words: *incident, investigation, digital forensic evidence, procedures, acquisition, techniques, tools*

1. Uvod

U većini slučajeva u informatički razvijenim organizacijama u čijem se informacionom sistemu (IS) desio kompjuterski događaj, prvo se pokušava rešiti problem svojim snagama, a često i sakriti događaj od javnosti. Najčešće, vlasnik IS angažuje svog administratora mreže i administratora zaštite, a zatim poziva stručnog konsultanta – IT eksperta ili interventni tim privatne institucije za brzo reagovanje i istragu kompjuterskog događaja (CERT⁵). Interventni tim za istragu kompjuterskog događaja na korporacijskom nivou radi do faze utvrđivanja prirode događaja, procene o težini i posledicama događaja i odluke da li je u pitanju greška u programu operativnog sistema (OS), greška operatera, ili namerni hakerski napad. U slučaju da je kompjuterski događaj nameran napad koji je naneo štetu IS, glavni menadžer ili vlasnik IS donosi odluku o nastavku istrage, obustavi ili pozivanju zvaničnih organa istrage (npr. Odeljenje za suzbijanje kompjuterskog kriminala MUPa). Brojni su razlozi zašto organizacije u startu ne pozivaju zvanične organe istrage kompjuterskih događaja, počev od straha gubljenja klijenata i kompromitacije kompanije, do zaziranja od prevelikog uplitanja zvaničnih organa. Hapšenje počinioca, zaplena računara kao

¹ SWGDE- *Scientific Working Group on Digital Evidence*

² IOCE - *International Organization on Computer Evidence*

³ SWGDE- *Scientific Working Group on Digital Evidence*

⁴ IOCE - *International Organization on Computer Evidence*

⁵ CERT - *Computer Emergency Response Team*

dokaza i transnacionalno praćenje traga i hapšenje počinioca, isključivo je u nadležnosti zvaničnih organa istrage.

Osnovna pretpostavka uspešne istrage svakog kompjuterskog događaja je čvrst oslonac na dokumentovanu i konzistentnu politiku zaštite i jasnu proceduru dobre prakse menadžmenta kompjuterskih događaja. Sankcionisanje počinioca zloupotreba u IT i kompjuterskih kriminalaca zahteva od svih organa istrage, tužilaštva, advokata i pravosudnih organa, shvatanje suštine i prirode digitalnih dokaza, forenzičke akvizicije i analize digitalnih dokaza i pripreme i prezentacije digitalnih dokaza pred sudom.

Pojam **digitalnih dokaza** obuhvata kompjuterski pohranjene i generisane digitalne dokaze, digitalni audio i video, digitalnu fotografiju, mobilni telefon i sve druge digitalne podatke i uređaje. Naučna forenzička akvizicija i analiza digitalnih dokaza razvija se poslednjih 25 godina. Nauka o digitalnim dokazima je standardizovana (IOCE i SWGDE). Izdate su preporuke za osnovne principe forenzičke analize digitalnih dokaza, kriterijumi, standardne radne procedure za: zaplenu računara, forenzičku akviziciju i analizu, čuvanje, kopiranje originalnih digitalnih dokaza, i dr.

Prema novom naučnom pristupu digitalnim dokazima sudija deluje kao čuvar kvaliteta digitalnih dokaza, odnosno, digitalni dokaz nije prihvatljiv sve dok generalno nije naučno prihvaćen, dok se ne može testirati, metoda dokazivanja proveriti, a dokazi lako i razumljivo prezentirati na sudu. Dakle, digitalni dokaz mora biti autentičan, tačan, kompletan, ubedljiv i prihvatljiv za sud.

2. Definicije termina

Definicija termina je prvi korak u standardizaciji radnih procedura za istragu kompjuterskog događaja, dokazivanje i sankcionisanje počinioca [20]. Jedinstveni standardi, principi, kriterijumi i procedure glavni su markeri pravnog i tehnočkog aspekta razmene digitalnih dokaza između suverenih država, kao posledice IT globalizacije gde se počinioc kompjuterskog događaja javlja u jednom, a digitalni dokaz se dobija iz drugog pravosudnog sistema.

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.

Originalni digitalni dokaz je fizički predmet i/ili podaci sadržani u tom predmetu u vreme akvizicije (otkrivanja, prepoznavanja, izvlačenja) ili zaplene predmeta.

Duplikat digitalnog dokaza 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.

Akvizivija digitalnih dokaza, proces otkrivanja, prepoznavanja i izvlačenja digitalnih podataka za potrebe analize digitalnih dokaza, prva je glavna faza forenzičke analize digitalnih dokaza, analogna uzimanju otiska prsta kod klasičnog kriminala. a počinje kada su podaci i/ili fizički predmeti skupljeni i uskladišteni za potrebe ispitivanja. Termin

implicira da je proces skupljanje legalan, izvršilac neko koga sud prepoznaje i da skupljeni materijal sud prihvata kao dokazni materijal.

Menadžment upada u IS je zatvoreni proces od 4 faze: preventivna zaštita; ispitivanje otpornosti IS na napad; otkrivanje napada, i istraga kompjuterskog događaja.

Glavni cilj je da se potencijalni rizik uspešnog napada održava na kontrolisanom nivou, kroz efikasnu preventivnu zaštitu, procese regularnog ispitivanja otpornosti sistema na napade i pravovremeno otkrivanje događaja, kao i da se olakšaju istražni postupak i sankcionisanje počinilaca nekog događaja.

Bezbednosni događaj u IS nisu svi kompjuterski događaji. Za većinu IS kompjuterski događaji mogu se podeliti na događaje u bezbednosti IS koji: ne predstavljaju glavnu pretnju i koji mogu izazvati zaustavljanje poslova.

Ako postoji standardna i konzistentna politika zaštite IS, koja definiše sve procese u slučaju kompjuterskog događaja, to je od velike koristi za otpočinjanje istrage kompjuterskog događaja. U istražnom postupku uvek treba kombinovati klasične policijske metode sa naučnom forenzičkom akvizicijom i analizom digitalnih dokaza, koje pomažu da se rekonstruiše događaj kompjuterskog kriminala i eventualno otkrije počinilac.

3. Principi, standardi, procedure i kriterijumi menadžmenta digitalnih dokaza

3.1. Glavni principi menadžmenta digitalnih dokaza

Karakteristike glavnih principa menadžmenta digitalnih dokaza, moraju [11]:

1. biti konzistentne sa pravosudnim sistemima u svakoj državi,
2. koristiti uobičajen i razumljiv jezik,
3. imati trajnu vrednost,
4. biti međunarodno priznate i prihvatljive,
5. ulivati poverenje i štiti integritet digitalnih dokaza,
6. biti primenjive na sve digitalne dokaze,
7. biti primenjive na pojedinca, zvanične agencije i najviši nacionalni nivo.

Glavni principi menadžmenta digitalnih dokaza:

1. U toku akvizicije, akcije ne treba da unose nikakvu izmenu digitalnih dokaza.
2. Samo kompetentna osoba za forenzičku analizu može pristupiti originalnom digitalnom dokazu.
3. Sve aktivnosti akvizicije, pristupa, skladištenja ili transfera digitalnih dokaza, moraju biti potpuno dokumentovane, sačuvane i raspoložive za uvid.
4. Lice je odgovorno za sve aktivnosti preduzete prema digitalnim dokazima dok su u njegovom posedu.
5. Svaka agencija odgovorna za akviziciju, pristup, skladištenje ili prenos digitalnih dokaza, odgovorna je za usklađenost svoje prakse sa ovim principima.

Primenom **Glavnih principa**, u skladu sa preporukama IOCE, menadžment digitalnih dokaza (rukovanje, čuvanje i prenos), biće prihvatljiv i izvan nacionalnih granica.

3.2. Standardna radna procedura

Da bi se osigurala bezbedna **istraga** kompjuterskog događaja, forenzička analiza i menadžment digitalnih dokaza i da bi se sačuvao integritet dokaza, zvanični istražni organi i privatne institucije za forenzičku analizu digitalnih dokaza, moraju uspostaviti i održavati efikasni sistem kontrole kvaliteta. **Standardna radna procedura (SRP)** je dokumentovano uputstvo za kontrolu kvaliteta celokupnog postupka istrage, forenzičke analize i menadžmenta digitalnih dokaza. SRP mora obuhvatiti propisno registrovanje svih aktivnosti istrage kompjuterskog incidenta, kao i korišćenje drugih, u kriminalistici široko prihvaćenih procedura, opreme i materijala.

Forma SRP treba da obuhvata sledeće elemente: **naslov, namenu, opis opreme i materijala, standarda i kontrola, algoritam procedure, opis elemenata kalibracija i proračuna, ograničenja, sigurnost i pouzdanost, i reference.**

Većina SRP imaju snagu preporuke IOCE, neke nisu objavljene i nisu podvrgnute javnoj raspravi niti su generalno prihvaćene u praksi. Alati sa otvorenim izvornim kodom imaju objavljene procedure, pa istraživač može izabrati da li da koristi takav alat ili ne [6].

3.3. Standardi i kriterijumi

Objavljene su i u praksi primenjivane i sledeći standardi i kriterijumi [17], [14], [], []:

1. SRP dokument sa jasno definisanom politikom zaštite i radnom procedurom, potpisan od strane menadžerskog autoriteta za sve aktivnosti.
2. Striktno sprovođenje svake radne procedure, moraju biti obavezni za sve zvanične i druge forenzičke organe, zbog prihvatanja rezultata istrage i zaključaka analize na sudu.
3. Menadžment agencije mora revidirati SRP jedanput godišnje, zbog brzih tehnološki promena u oblasti IT.
4. SRP moraju biti generalno prihvaćene u oblasti forenzičke analize i menadžmenta digitalnih dokaza i da ih podržavaju poznate i priznate naučne metode.
5. U izboru metoda evaluacije naučne vrednosti primenjenih tehnika i procedura glavni kriterijum u oceni validnosti tehnike i/ili procedure treba da bude potvrda tačnosti i pouzdanosti specifične tehnike (korisna je javna naučna rasprava).
6. Akreditovana agencija mora posedovati pisanu kopiju odgovarajućih tehničkih procedura koje koristi u radu, sa spisom potrebnih hardverskih i softverskih alata, opisom propisanih koraka za njihovu upotrebu i jasno navedenim svim ograničenjima upotrebe tehnika i alata.
7. Lica koja primenjuju procedure moraju biti ovlašćena da koriste procedure i alate za istragu i/ili forenzičku analizu digitalnih dokaza, upoznata sa procedurama, kvalifikovana i dobro obučena za rad.
8. Alati za akviziciju i/ili analizu digitalnih dokaza moraju biti testirani i sa važećim sertifikatom o verifikaciji funkcionalnog kvaliteta nadležne nacionalne institucije i moraju biti u dobrom radnom stanju.
9. Aktivnosti i rezultati forenzičke akvizicije (uključujući zaplenu), analize i menadžmenta digitalnih dokaza moraju biti registrovani u pisanoj formi i na raspolaganju za uvid svim stranama koje na to imaju zakonsko pravo. Generalno, dokumentacija koja se odnosi na zaključke forenzičke analize, mora biti tako pripremljena da je, u odsustvu autora, na glavnom preteresu može prezentirati i drugo kompetentno lice.

10. Mora se uspostaviti neprekidno čuvanje svih digitalnih dokaza, vođenje pisanih zabeleški i zapažanja o slučaju (mastilom, hemijskom u boji), sa inicijalima autora kod svake korekcije (precrtane jednom crtom), lično potpisanom svakom zabeleškom sa inicijalima, DS, ili drugom identifikacionom oznakom autora.
11. Samo kvalifikovano lice, u skladu sa propisanom SRP, može vršiti akcije koje mogu oštetiti ili uništi originalni dokaz. Svaka akcija mora biti dokumentovana, pouzdana i kontrolabilana.
12. Obučeno forenzičko osoblje mora koristiti verifikovane forenzičke softverske programe i odgovarajuću poverljivu hardversku opremu.

4. Relevantne procedure za istragu i dokazivanje kompjuterskog događaja

4.1. Planiranje i organizacija istražnog postupka kompjuterskog događaja

Brzina reakcije na kompjuterski događaj je ključna i kritična faza. Pokazalo se u praksi da su podaci otkriveni u toku prvih nekoliko dana presudni za uspešan ishod istrage.

Zvanični istražni postupak kompjuterskog kriminala optimalno se odvija u 4 faze, po modelu “korak po korak” u okviru jedne faze. Svaki korak u okviru jedne faze istrage treba da vodi u drugi i da je obezbeđena kontrola aktivnosti u okviru svake faze [17].

1. Inicijalna istraga,
2. Ulazak u trag napadaču.
3. Otkrivanje identiteta napadača.
4. Hapšenje.

Korporacijska istraga kompjuterskog događaja u funkcionalnom koristi prve tri faze, koje su primenjive za istragu u okviru kompanije. Da bi uspeh istrage bio potpun svaku fazu treba preduzimati sa sledećih 6 postavljenih ciljeva [17]:

1. Eliministi očiglednosti;
2. Postaviti hipotezu o napadu;
3. Rekonstruisati kriminalni akt;
4. Otkriti trag do osumnjičenog računara sa koga je napad izvršen;
5. Analizirati izvorni, ciljni i posredne računare;
6. Priprema dokaza, uključujući ako je moguće i sam računar, za prezentaciju pred sudom, i
7. Predaja nalaza i dokaznog materijala (Izveštaja o istrazi) korporacijskim istražnim organima, ili zvaničnim istražnim organima za dalji postupak.

Istraga otpočinjanje sa eliminisanjem očiglednog, zatim počinje proces stvaranja hipoteze kako se napad dogodio. Sledeći korak je skupljanje dokaza koji potvrđuju hipotezu o događaju, ali se uključuju i alternativna objašnjenja. Analiza i priprema prezentacije kompjuterskih dokaza imaju za cilj: verifikaciju elemenata hipoteze, ispitivanje alternativnih objašnjenja, i generisanje dodatnih veza za dalju istragu. Sve nalaze u Izveštaju o istrazi treba predati korporacijski organima istrage ili zvaničnim istražnim organima za dalji postupak.

Najbolja kombinacija u istrazi je zajednički timski rad zvaničnog organa istrage i eksperata za IT. Ne postoji superzvezda i istrazi kompjuterskog kriminala. Svaki učesnik treba da ima svoj zadatak u skladu sa svojim znanjem, specijalizacijom i obukom.

4.2. Standardna procedura korporacijske istrage kompjuterskog događaja

1. Ispitivanje osumnjičenih i svedoka.

2. Priprema organa za pretragu (lociranje kompromitovanog računara).
3. Pretres resursa osumnjičenog.
4. Provera evidencija log datoteka i ostalih informacija o osumnjičenom.
5. Markiranje i sortiranje svog posrednog dokaznog materijala sa detaljnim oznakama o sadržaju i mestom za potpis lica koje preuzima dokazni materijal.
6. Zaštita od izmene memorisane datoteke sa dokazima (npr. CRCMD5, NTI).
7. Obezbeđenje vremenske evidencije događaja kao čvrstog dokaza.
8. Korišćenje forenzičkih alata za verifikaciju događaja kao kriminalnog akta.
9. Kontrolna provera svih faza istrage.
10. Prikupljanje, analiza i priprema dokaza za glavni pretres.
11. Izrada detaljnog Izveštaja o istrazi, dokumentovanje i preporuka za dalji postupak.
12. Odluku na nivou organizacije: stornirati, nastaviti u organizaciji ili predati slučaj nadležnim organima.

Osnovni problemi u korporacijskoj istrazi kompjuterskog događaja mogu biti:

1. Korporacijska istraga po zakonu nema organa za potragu i zaplenu napadačkog računara.
2. Organi korporacijske istrage kompjuterskog događaja ne mogu voditi istragu izvan svoje organizacije i svog IS.
3. Organi korporacijske istrage kompjuterskog događaja moraju voditi računa o iznošenju u javnost informacije o upadu u IS zbog poslovnog ugleda, poverenja klijenata, straha od ponovljenih napada, neefikasnosti sistema zaštite, itd.

4.3. Standardna procedura zaplene računara kao dokaznog materijala

Na poziv korporacijskih organa istrage, zvanični organ istrage, sa nalogom za pretres, u pripremi i realizaciji pretresa i zaplene osumnjičenog računara, radi obezbeđivanja digitalnih dokaza, treba da primenjuje **Standardnu proceduru zaplene računara kao dokaznog materijala**, koja treba da sadrži najmanje sledeće elemente [17]:

1. Legalan okvir za rad (zakon i sudski nalog) i ograničenja u radu sa poverljivim podacima.
2. Potvrda kredibiliteta i kompetentnosti istražnog organa.
3. Identifikacija označavanje svih zaplenjenih medija osim HD (trake, printerski kertridži, zip, diskete, CD ROM, DVD) za skladištenje digitalnih dokaza, (sadržaj, podatke o sertifikaciji/testiranju/ ispitavanju i ime ispitivača-analitičara).
4. Čuvanje digitalnih dokaza u propisanom okruženju (temperature, vlažnosti, prašine, magnetnih polja, i.t.d.) i na propisan način.
5. Detaljan izveštaj o procesiranju i strukturi HD osumnjičenog računara.

4.4. Standardna procedura za obezbeđivanje kopija digitalnih dokaza

Standardna procedura za obezbeđivanje kopija dokaza za osumnjičenog, advokata odbrane, itd. treba da sadrži sledeće elemente:

1. Izradu fizičkog radnog duplikata originalnog digitalnog dokaza (npr. HD).
2. Odštampanu radnu kopiju, ako sadržaj nije suviše velik.
3. Sažeti izveštaj, sa digitalnim dokazom u elektronskoj formi na mediju (FD, CD ROMU, DVD, itd.) ako je sadržaj radne kopije velik.
4. Odštampane podatke sadržane u memorijskim uređajima i medijima koji su samo za čitanje, ako se traže takva forma dokaza.
5. Za tehničku prezentaciju i veštačenje na glavnom pretresu digitalni dokazi treba da budu jednostavni, pripremljeni u kompjuterskoj prezentaciji, sa kratkim i jasnim objašnjenjem kompjuterskog kriminala na Internetu i kako radi Internet.

4.5. Standardna procedura naučnog aspekta forenzičke analize digitalnih dokaza

Sve standardne radne procedure istrage, akvizicije, analize i menadžmenta digitalnih dokaza moraju zadovoljiti minimalne zahteve naučne definicije digitalnih dokaza:

1. Da procedura izvođenja dokaza (akvizicije i analize) može biti testirana i verifikovana.
2. Da je poznat stepen grešaka svake procedure.
3. Da je procedura objavljena u vrhunskim višestruko recenziranim naučnim časopisima (konferencijski radovi nisu dovoljni).
4. Da je procedura prihvaćena u relevantnim naučnim krugovima.
5. Da je nekoliko alata za forenzičku analizu digitalnih dokaza proizvedeno prema ovom standardu.

4.6. Standardna procedura akvizicije digitalnih dokaza

Veoma je čest slučaj kada digitalne dokaze prvo skuplja sama žrtva napada, pre korporacijskih ili zvaničnih organa istrage, pa je važno prvi stići do digitalnih dokaza i obezbediti njihov integritet u celom lancu istrage i suđenja.

Forenzički analitičar digitalnih podataka u procesu akvizicije (otkrivanja, identifikacije, izvlačenja) mogućih digitalnih dokaza iz računara preduzima sledeće korake:

- **Obezbeđuje** ispitivani računarski sistem od bilo koje izmene, oštećenja, korupcije podataka ili unošenja virusa u toku forenzičke akvizicije i analize i ekspertske konsultantske usluge i/ili veštačenje ako se zahteva.
- **Otkriva** sve datoteke (postojeće, izbrisane, skrivene, zaštićene parolom i šifrovane) i što je moguće više njihovog sadržaja na ispitivanom sistemu.
- **Oporavlja** što je moguće više otkrivenih izbrisanih datoteka.
- **Pristupa** (ako je moguće i zakonski dozvoljeno) sadržaju zaštićenih i šifrovanih datoteka.
- **Analizira** sve relevantne podatke u nepristupačnim zonama HD (*nelocirani, slack i izbrisani prostor* i *swap* datoteke).
- **Štampa** celokupnu analizu relevantnih i otkrivenih datoteka računara.
- **Daje mišljenje** o konfiguraciji sistema, strukturi otkrivenih datoteka, svakom otkrivenom podatku i ličnoj informaciji, svakom pokušaju skrivanja, brisanja, zaštite i šifrovanja informacija i svemu drugom što je otkriveno, a čini se da je relevantno za kompletnu analizu računarskog sistema.

4.7. Standardna radna procedura pristupa osumnjičenom računaru

Standardna radna procedura pristupa osumnjičenom računaru koji je još uključen obavezno obuhvata sledeće elemente: obezbeđenje lokacije na kojoj je računar, uzimanje fizičke kopije HD, FD i drugih medija, i bezbedno isključuje računar. Ova procedura može sadržavati i preko 20 koraka (aktivnosti). PC sa DOS, Win ili NT OS generalno može biti isključen neregularno-izvlačenjem mrežnog utikača, bez velike trajne štete po digitalne dokaze u skrivenim datotekama. Sistem se mora ponovo podići sa inicijalnim rebutiranjem sa FD ili CD ROMa, nakon toga uzeti fizičku (mirror) sliku HD i rekonstruisati približno originalnu konfiguraciju sistema. UNIX mašine se ne smeju isključivati izvlačenjem iz mreže. One se isključuju redovnom procedurom [17], [10] .

U toku procesa akvizicije i preliminarne ispitivanja digitalnih dokaza treba tražiti odgovore na niz jednostavnih pitanja, koja istražni organ treba da ima dokumentovane u samoj proceduri, na primer:

1. Koji tip digitalnih dokaza je skupljen, koji dokazi su posledica upada u računar?
2. Kakva je hronologija pristupa ili izmene podataka?
3. Kakva je procena oštećenja?
4. Ko može biti odgovoran za upad i zašto je neko lice (lica) osumnjičeno?
5. Kada je događaj prvo otkriven i ko je prvi upozorio na događaj ili štetu?
6. Ko vodi istragu i kakve su aktivnosti preduzete da se dokazi identifikuju, skupe, sačuvaju, i analiziraju podaci i uređaji., itd.

4.8. Standardna procedura za forenzičku analizu digitalnih dokaza

1. Nije objavljena konzistentna standardna procedura za forenzičku analizu digitalnih dokaza.
2. Za forenzičku analizu koristiti alate sa otvorenim izvornim kodom, koji omogućavaju definisanje, proveru konzekventnosti i tačnosti i kontroli standardne procedure za forenzičku analizu digitalnih dokaza.
3. Na globalnom nivou osnovni problem u oblasti standardizacije forenzičke analize digitalnih dokaza je:
 - haos u sertifikaciji eksperata za forenzičku analizu digitalnih dokaza,
 - nedovoljna primena konzistentnih principa digitalnih dokaza za sudsku praksu,
 - ne postojanje internacionalnog standarda profesionalne sertifikacije eksperata za analizu digitalnih dokaza,
 - potreba za definisanjem univerzalnih kriterijuma za evaluaciju kompetentnosti eksperata iz oblasti IT za forenzičku analizu digitalnih dokaza,
 - potreba za definisanjem univerzalnih kriterijuma za evaluaciju procedura ekspertskog sudskog veštačenja.
4. **Formirati nacionalni centar za sertifikaciju** standarda u oblasti forenzičke analize digitalnih dokaza, blisko koreliran sa internacionalnim telima za sertifikaciju u ovoj oblasti, zbog globalnog karaktera kompjuterskog kriminala, a samim tim i forenzičke analize digitalnih dokaza.

4.8.1. Standardna procedura ispitivanja diskova

Standardna procedura za kompletno ispitivanje kompjuterskih HD obuhvata: uspostavljanje forenzički sterilnih uslova; korišćenje verifikovanih, sterilnih medija bez virusa; korišćenje sertifikovanih forenzičkih softverskih alata; korišćenje ovlašćenih i kvalifikovanih istražnih organa (pojedina, agencija); obezbeđivanje integriteta svih manipuliranih dokaza; izradu fizičkih (miror) kopija originala i rad na njima; čuvanje svih dokaznih materijala u celokupnom lancu istrage i suđenja, priprema digitalnih dokaza za sudski proces u formi prihvatljivoj od strane pravosudnog sistema, i potpuno dokumentovanje detaljne analize [9].

Na sličan način sa izvesnim specifičnostima u pogledu izbora alata, propisuje se i **Proceduru ispitivanja disketa i sličnih medija** [9].

4.9. Standardna procedura testiranja alata za forenzičku analizu digitalnih dokaza

1. Nije objavljena standardna procedura (SRP) za testiranje alata za forenzičku analizu digitalnih dokaza.
2. Objavljena je SRP i metodologija za uzimanje mirror slike HD diska i disketa (CFIT⁶), koja sadrži samo obavezno testiranje radi verifikacije funkcija softverskog alata, ali ne podrazumeva kontrolu izvornog koda alata, što je i najveći nedostatak ove procedure.
3. Nema objavljenog predloga za proračun stepena grešaka hardversko - softverskih alata za digitalnu forenzičku analizu. Svaki koncept stepena grešaka treba da uključuje greške u programiranju ili bagove.

5. Forenzička akvizicija digitalnih dokaza

U IS generalno postoje 4 potencijalna izvora podataka koji mogu biti dokazi i treba ih prikupiti u procesu forenzičke akvizicije:

1. RAM, registri i diskovi u napadnutom računaru;
2. RAM, registri i diskovi u osumnjičenom računaru (napadača);
3. Log datoteke u napadnutom, osumnjičenom i posrednom računaru i drugim mrežnim uređajima, i
4. Sistem fizičko-tehničkog obezbeđenja (eventualni živi svedok, snimak sistema video nadzora, itd.) na lokaciji osumnjičenog računara.

5.1. Osnovno zahtevi za akviziciju digitalnih dokaza

1. Za forenzičku akviziciju digitalnih podataka izgubljeno je, sve što nije logovano.
2. **Centralizovano logovanje** u log serveru omogućava primenu specifičnih alata na sve podatke o logovanju sa različitih platformi. Preporučuje se korišćenje log datoteka po defaultu.
3. Vremenska sinhronizacija svih log podataka iz mrežnih uređaja u jednom memorijskom prostoru, čvrst je dokaz o događaju (NTP-*Network Time Protocol* [4]).
4. Preporučuje se konfigurisanje IS prema GMT (srednje vreme po Griniču
5. Digitalno potpisan (DS) podatak generalno obezbeđuje njegovu neporecivost (**Digital Notary** alat).
6. Pravo upisivanja u log datoteke na host i bezbednim serverima treba da imaju samo procesi koji generišu podatke o logovanju.
7. Obezbediti maksimalno zadržavanje log podataka u *off-line* režimu za bekapovanje.
8. XML protokoli za reprezentaciju i statističku agregaciju korisni su za kreiranje meta-podataka neophodnih za potrebe tipične istrage kompjuterskog događaja.
9. Akvizicija podataka sa različitih platformi, sa mrežnih uređaja i sa kompromitovanog kernela različitih OS, zahteva različite i specifične tehnike i alate [14].
10. Sa aspekta forenzičke analize, dokazi dobijeni akvizicijom podataka validni su, ako su skupljeni i potvrđeni sa više izvora podataka iz računara i mrežnih uređaja.

5.2. Akvizicija podataka sa HD u radu

Akvizicija podataka sa HD u radu vrši se kada ne postoji mogućnost isključivanja sistema. Softver **Digital Notary** i dodatni dokazi mogu pomoći u ovom slučaju. U tom slučaju, uzimanje slike sa živih sistemskih diskova, gde kompromitacija nije na nivou kernela, zahteva posebne poverljive alate [5].

⁶ CFTT- *Computer Forensic Tool Testing* - Radna grupa IOCE za testiranje forenzičkih alata

6. Forenzička analiza digitalnih dokaza

Za razliku od ranijih definicija, zavisne isključivo od znanja i stručnosti forenzičkog analitičara, glavne kategorije forenzičke analize digitalnih dokaza bolje se mogu definisati korišćenjem koncepta apstrakcionih slojeva u IS [10], odnosno na alate koji vrše analizu sloja apstrakcije: fizičkih medija, menadžmenta medija, OS, aplikacija i memorijskog prostora. U praksi se forenzička analiza kompjuterskih digitalnih dokaza realizuje kroz tri glavne oblasti:

- Forenzičku analizu softvera,
- Forenzičku analizu računarskog sistema, i
- Forenzičku analizu kibernetičkog prostora (RM).

6.1. Forenzička analiza softvera

Analiza softvera je najosetljiviji, uglavnom visoko teoretski, deo forenzičke analize računara. Izrada forenzičkog softverskog alata (FSA⁷) za analizu je težak posao. Ključ za uspešnu identifikaciju autora osumnjičenog malicioznog softverskog koda je selekcija odgovarajućeg korpusa koda i identifikacija odgovarajućih karaktersitika za upoređivanje [4], [15], [11], [12], [13] [18] i [19].

6.2. Forenzička analiza računara

Forenzička analiza računarskog sistema je aplikacija ispitivanja računara i tehnika analize u cilju određivanja potencijalno legalnih dokaza. Kompjuterski specijalisti mogu primeniti brojne metode, tehnike i alate za otkrivanje podataka koji se nalaze u računarskom sistemu, ili za oporavak izbrisanih, šifrovanih ili oštećenih datoteka podataka. Sve ove informacije mogu pomoći za otkrivanje, depoziciju ili aktuelno veštačenje u toku civilne parnice ili krivičnog sudskog postupka.

Za različite platforme računara (OS) postoje određene specifičnosti metoda forenzičke analize, tehnika i alata [17].

6.3. Forenzička analiza kibernetičkog prostora

Ovo može biti veoma spor proces. Obično je potrebno da napadač bude na liniji, da bi uspešno bio uhvaćen. Neophodna je saradnja telefonskih kompanija i provajdera internet servisa (ISP), kao i zvaničnih istražnih organa. U proceduri otkrivanja traga napadaču sa Interneta treba analizirati: IP adrese u **login** datotekama napadnutog računara mrežnih uređaja (alati tipa: *ReverseFinger*, *Nslookup*, itd.), obezbediti *online* produženo logovanje i praćenje aktivnosti, i pretpostaviti da se kompetentan napadač verovatno ubacuje u sistem, pre nego što preduzima napad.

Za različitih platforme postoje određene specifičnosti analize kibernetičkog prostora i primene tehnika i alata [17]. Sistemske log datoteke obezbeđuju dokaze o upadu u mrežu i host računar. Analiza više log datoteka u mreži ima za cilj da dokaže sinhronizaciju upada u sistem i kompjuterskog događaja i da popuni praznine u istrazi.

(⁷) Poznat proizvođač FSA u svetu je *Perdue University*, SAD

Primer: Neka imamo log na Unix računaru žrtve koji nije kompletan. Sa alatom tipa **Chklastlog** možemo proveriti da li je log datoteka menjana, ali alat ne garantuje da je log datoteka kompletna. Korisno je napraviti analitičku radnu kartu tipa u Tabeli 6.1:

Vremena	Višestruke log datoteke (isti događaj)		
	Log 1	Log2	Log 3
	15.12.2003 12:30	15.12.2003 12:35	15.12.2003 12:30

Tabela 6.1. Analitička radna karta multiplikativnih log datoteka

Ograničenja sistemskih log datoteka osnovni su problem u anlizi kibernetičkog prostora i analizi digitalnih dokaza, uopšte:

1. Da bi imala dokaznu vrednost treba dokazati da log datoteka nije izmenjena, (alati **ITA**, **RealSecure** štite log datoteke od izmene), ili obezbediti direktnog svedoka da log datoteke nisu izmenjene. Zato pristup log host mašini treba da bude ekstremno ograničen, a log datoteke treba bekapirati na pouzdan disk i čuvati kao čvrste digitalne dokaze.
2. Drugo ograničenje log datoteka je kompromis veličine i kompletnosti. Preporučuje se da log datoteka pokazuje: sve pristupe superkorisnika, ulaske i izlaske, pokušaje korišćenja kontrolisanih servisa (**FTP**, **Telnet**, **R srvis**, itd.), pokušaje pristupa kritičnim resursima (datoteci lozinki, kernelu, *wrapper*-u, itd), i detalje o e-pošti.
3. Uobičajeno je da hakeri dodaju informacije u log datoteke ili promene ID da dovedu u zabludu analitičara. Zato log datoteci nikada ne treba verovati na prvi pogled.

6.4. Potencijalna ograničenja u analizi digitalnih dokaza

Primeri ograničenog ispitivanja mogu biti:

1. Obim ispitivanja je ograničen od strane zvaničnog istražnog organa ili suda.
2. Oprema se mora ispitati na licu mesta i nema dovoljno vremena.
3. Veličina medija je suviše velika pa nije moguće kompletno ispitivanje.
4. Težina već otkrivenih dokaza je tolika da dalje ispitivanje nije potrebno.
5. Nemoguće izvesti potpuno ispitivanje zbog hardvera, OS ili drugih uslova.

7. Tehnologije za akviziciju i analizu digitalnih dokaza

Tehnologije (tehlike i alati) za akviziciju i analizu digitalnih dokaza obezbeđuju izvlačenje, skupljanje i analizu osetljivih podataka sa diskova, RAM, registara, mreže, itd., uzimanje fizičke slike i analizu sistemskih diskova računara i ukazuju na šta se sve treba obratiti pažnja u planiranju istrage kompjuterskog događaja. Alati za akviziciju i analizu moraju biti komercijalno dostupni i verifikovani od strane strukovne forenzičke zajednice. U pravosudnom postupku može se zahtevati dodatno veštačenje IT eksperta za autentifikaciju aplikacije alata u procesu akvizicije i analize i autentifikacija forenzičkih alata koji su korišćeni.

7.1. Tehnike za akviziciju i analizu digitalnih dokaza

Osnovni principi tehnika za akviziciju i analizu digitalnih dokaza:

- moraju se tretirati svi digitalni dokazi, kao da će biti korišćeni pred sudom;

- nikada se ne sme raditi na originalnim dokazima, nego ih skupiti i raditi na kopijama;
- kada je kopija dokaza napravljena, bezbedno uskladištiti i čuvati original;
- propisno označiti sve digitalne dokaze.

Osnovne karakteristike tehnika za akviziciju i analizu digitalnih dokaza:

1. uglavnom se odnose na akviziciju podataka sa HD,
2. akvizicija se mora obaviti u pouzdanom, poverljivom okruženju (Linux butabilni CD, komanda **dd**, **Laptop** računar),
3. podaci se kopiraju na novi disk ili kroz mrežu na poverljivi (zaštićeni) server,
4. treba da prati kompjuterski događaj onako kako se vremenski odvijao u svim log datotekama,
5. sa svakog računara ili drugog mrežnog uređaja treba izvući neizmenjene dokaze,
6. za složeniji ispitivani sistem, kapacitet diska forenzičkog računara treba da bude veći, jer su veći zahtevi za forenzičku akviziciju i analizu.

7.2. Kriterijumi kvaliteta alata za forenzičku akviziciju i analizu digitalnih dokaza

Na osnovu potreba za forenzičkom analizom specifičnih delova (slojeva, prostora,...) računara, može se generisati lista zahteva za forenzičke alate sa sledećim kriterijumima kvaliteta: **korisnost, sveobuhvatnost, tačnost, određenost, proverljivost, ovlašćenja samo za čitanje i mogućnost sanitarne kontrole.**

Generalno, osnovni zahtev pravosudnih organa je da softverski alati za akviziciju i analizu digitalnih dokaza budu napisani sa **otvorenim izvornim kodom** zato što:

1. moraju procesirati podatke na isti način kao i originalni softver,
2. analitičar mora shvatiti i znati šta originalni softver radi sa podacima,
3. otvoreni izvorni kod obezbeđuje mnogo precizniji alat, koji omogućavaju analitičaru lakše otkrivanje skrivenih podataka na disku,
4. omogućava ispitivaču da verifikuje i testira kod na zahtev suda,
5. OS sa otvorenim izvornim kodom za forenzičku analizu (najčešće Linux) dopušta potpunu kontrolu ponašanja sistema (važno – podaci se ne smeju menjati).
6. može se verifikovati da OS ne zapisuje nekontrolisano na disk ili u datoteku,
7. Linux podržava oko 30 tipova sistema datoteka: NTFS drajver brz je i lako se instalira na CD za akviziciju podataka sa diska ili mreže,
8. procedura primene alata se lakše dokumentuje za javni uvid,
9. alati se lakše mogu prilagoditi za specifične istrage, itd.

7.3. Primeri softverskih alata za forenzičku akviziciju i analizu

1. **Alati za uzimanje fizičke kopije:** *SafeBack, Drivespy, Image, GUEST driver, disk za butiranje sa DOS 6.22, 3X.I, 4X, 6X...*,
2. **Alati za skupljanje podatke iz neiskorišćenih, nelociranih i izbrisanih prostora HD:** *GETSLACK, GETFREE, FILTER I, TEXTSEARCH PLUS, Norton Utility,*
3. **Alati za skupljanje podatke iz neiskorišćenih, nelociranih i izbrisanih prostora FD:** *Anadisk V. 2.10LE,*
4. **Alati za rekonstrukciju velikih log datoteka sa HD:** *TEXTSEARCH, ASAX, ACL ASCII (CDL);*
5. **Alati koji proveravaju da li je log datoteka menjana:** *Chklastlog*
6. **Alati za otkrivanje lokacije napadača, ako je napadač online:** *ReverseFinger,*

Nslookup

7. **Alati za gledanje sadržaja Web brauzera u WIN OS (Netscape, MS Internet Explorer):** *UNMOZIFY*.
8. **Univerzalni softverski alati za forenzičku akviziciju i analizu digitalnih dokaza:** *GETSLACK, FILTER I. TextSearch Plus, i najbolji alati iz grupe alata za ulančavanje podataka sa HD (TEXTSEARCH)*.
9. **Najpoznatiji alati sa otvorenim izvornim kodom** [9], [20]: *Linux OS; GNU utilities, grep, find, debugfs, readelf, objdump; TCT, TCTUIII, Foremost& fatback (DoD DCFL), AFB*.
10. **Najpoznatiji alati sa zatvorenim izvornim kodom:** *Encase, iLook, Access Data FTK, ASR Data SMART (radi samo na Linux i BeOS), Paraben PDA Seizure, Technology Pathways ProDiscover, IDA*,
11. **Alati za mrežnu akviziciju podataka:** *Snort, tcpdump, ngrep*.

8. Ostali aspekti istražnog postupka sa digitalnim dokazima

8.1. Tela za akreditaciju standarda digitalnih dokaza

Na nacionalnom nivou treba formirati **telo (entitet) za akreditaciju standarda digitalnih dokaza** koje propisuje standarde i kriterijume, koje specifične naučne i tehničke discipline moraju zadovoljiti u radu forenzičkih laboratorija za analizu digitalnih dokaza. Ovo telo treba da izda **Pravilnik za akreditaciju** koji sadrži: principe, standarde i kriterijume, kao i diskusije (pošto su standardi u razvoju). Pravilnik nameniti kao osnovno uputstvo za rad menadžmentske strukture forenzičkih laboratorija, kvalifikovanih specijalista i laboratorija i ostalog radnog osoblja.

U SAD telo za akreditaciju standarda digitalnih dokaza, je Direkcija za akreditaciju američkog udruženja kriminalističkih laboratorija (Bord laboratorija **ASCLD/LAB**).

8.2. Udruženja naučnika za forenzičku analizu digitalnih dokaza

Na nacionalnom nivou treba formirati Asocijaciju (udruženje) naučnika za forenzičku analizu digitalnih dokaza. Članovi udruženja treba da su najeminentniji naučnici i stručnjaci koji se bave ovim oblastima.

U SAD telo za akreditaciju standarda digitalnih dokaza, je Direkcija za akreditaciju američkog udruženja kriminalističkih laboratorija (Bord laboratorija - ASCLD/LAB).

8.3. Legalni zahtevi za digitalne dokaze

Oblast istrage kompjuterskih događaja, forenzičke akvizicije i analize digitalnih dokaza i uslova prihvatljivosti digitalnih dokaza u pravosudnim sistemima, još uvek je u razvoju u svetu i u nas. Postoje brojna nerešena pitanja. Na primer, do sada nije poznato niti pouzdano utvrđeno da li se kao digitalni dokaz treba smatrati naučno definisan digitalni dokaz, ili digitalni dokaz deriviran kao izlazni rezultat automatizovanog forenzičkog alata za akviziciju i analizu.

Ipak, bez obzira na ovakvo stanje, moraju biti zadovoljeni minimalni zahtevi legalnog sistema da bi se ulazni, naučno zasnovani digitalni podaci, smatrali prihvatljivim digitalnim dokazom za pravosudni sistem, a to su:

- naučni digitalni dokaz mora biti i relevantan i pouzdan, i
- pouzdanost naučnog dokaza se potvrđuje primenom standarda,
- istražni i dokazni postupak (procedura) mogu se testirati i verifikovati,
- primenjene metode testiranja i verifikacije naučno su priznate.

9. Zaključak

1. Vreme masovnog korišćenja kompjutera, zloupotreba i kompjuterskog kriminala novijeg je datuma.
2. Forenzička nauka digitalnih dokaza obuhvata digitalne dokaze: kompjutera, digitalnog foto/audio/video/faksa, mobilnog telefona, i drugih digitalnih uređaja.
3. Objavljeni su preporuke, principi, standardi kriterijumi i procedure za (IOCE i SWGDE): skupljanje, kopiranje, čuvanje, transport i analizu digitalnih dokaza i testiranje forenzičkih alata za akviziciju i analizu digitalnih dokaza.
4. Agencije ovlašćene za istragu kompjuterskog kriminala, moraju striktno sprovoditi sve IOCE preporuke, standarde i radne procedure, koristiti standardne i poverljive forenzičke alate i kompetentne kadrove za istragu, akviziciju, analizu i prezentaciju digitalnih dokaza na sudu, zbog globalnog karaktera zloupotreba i kompjuterskog kriminala i potrebe da se digitalni dokazi skupljeni u jednom pravosudnom sistemu sankcionišu u drugom pravosudnom sistemu (državi).
5. U nedostatku i očekivanju nacionalnih principa, standarda, kriterijuma i procedura za skupljanje, kopiranje, čuvanje, transport i analizu digitalnih dokaza i za testiranje forenzičkih alata za akviziciju i analizu digitalnih dokaza, treba koristiti IOCE usvojene standarde.

Literatura:

- [1]. Carrier Brian, *Defining Digital Forensic Examination and Analysis Tools Using Abstraction layers*, International Journal of Digital Evidence, Vol.1, No. 4, 2003.
- [2]. Carrier Brian, *Open Source Software in Digital Forensics*, carrier&atstake.com
- [3]. Carrier Brian, *Defining Digital Forensic Examination and Analysis Tools*, avgust 7, 2002, carrier&atstake.com
- [4]. COAST project PERDU University: <http://www.cs.perdue.edu/coast-library.html>.
- [5]. Desante Anthony F., *Evidentary Consideration for Collecting and Examining Hard-Drive Media*, The George Washinton University, 28.11. 2001, Forensic Sciences 262,
- [6]. <http://www.atstake.com>.
- [7]. <http://www.ensfi.org>
- [8]. <http://www.ojp.usdoj.gov/nij/pubs.htm>,
- [9]. IACIS (*International Association of Computer Investigative Specialists*), <http://www.iacis.org/>
- [10]. Icove, D., Segar, K., and VonStorch, W., *Computer Crime, A Crimefighter's Handbook*, O'Reilly & Associates, 1999.

- [11]. *IOCE Principals & Definitions*, IOCE 2. Conference, 7.10.1999, Marriott Hotel, London
- [12]. Krsul I, *Authorship Analysis: Identifying the Author of a Program*, Department of Computer Sciences, Purdue University, M.S. Thesis, CSDTR-94-030, 1994.
- [13]. 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.
- [14]. Pettinari Dave, *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, juni 2000.
- [15]. Pollit Mark M., *Report on Digital Evidence*, (FBI CART report, DC Washington, USA), Interpol Forensic Science Symposium, Lyon, France, 16-19.10.2001.
- [16]. Robbins Judd, *PC software forensic, Expert witness, An Explanation of Computer Forensics*,
- [17]. Rosenblatt, K. S., *High Technology Crime — Investigating Cases Involving Computers*, KSK Publications, San Jose, CA, 1995.
- [18]. Spafford E. H. and Weeber S. A., *Software Forensics: Can We Track Code to Its Authors?*, 15th National Computer Security Conference; pp. 641–650, Oct. 13–16, 1992.
- [19]. Spafford E. H. and Weeber S. A., *Software Forensics: Tracking Code to Its Authors*, Computers & Security, 12(6), pp. 585–595, Dec. 1993.
- [20]. Whitcomb C. M., *A Historical perspective of Digital Evidence: A Forensic Scientist's View*, International Journal of Digital Evidence, proleée1. 2002, vol.1, issue 1.