PREGLEDNI ZNANSTVENI RAD (REVIEW ARTICLE)
UDK: 343.14:004 (497.11)

Dr Milana Pisarić, asistent s doktoratom
Pravni fakultet u Novom Sadu, Univerzitet u Novom Sadu

OD ELEKTRONSKIH ZAPISA, KAO TRAGOVA, DO ELEKTRONSKIH DOKAZA

Apstrakt:

Polazeći od toga da se priroda računarskih podataka, koji bi mogli imati značaj dokaza u krivičnom postupku za dela visokotehnološkog kriminala, i potreban forenzički rad u prikupljanju i obradi tih podataka u znatnoj meri razlikuju u odnosu na uobičajene tragove i dokaze (s obzirom na brzinu kojom se radnja može preduzeti a tragovi u elektronskom obliku izmeniti, sakriti ili uništiti), posebna pažnja je posvećena pravilima digitalne forenzike prilagođenim specifičnostima podataka u računarima, računarskim sistemima i računarskim mrežama. Stoga je u radu prikazan put od elektronskih zapisa, kao tragova, do elektronskih dokaza.

Ključne reči: *krivični postupak, digitalna forenzika, elektronski dokazi.*

1. POJAM DIGITALNE FORENZIKE

Postoji više definicija digitalne forenzike, a u literaturi je najčešće citirana (uz neznatne modifikacije) definicija koju je 2001. godine stvorila Radna grupa za istraživanje digitalne forenzike (The Digital Forensics Research Workshop: DFRWS , http://www.dfrws.org/), po kojoj „digitalna forenzika“ podrazumeva „upotrebu naučnoizvedenih i potvrđenih metoda radi očuvanja, prikupljanja, validacije, identifikovanja, analize, tumačenja, dokumentovanja i predstavljanja digitalnih dokaza izvedenih iz digitalnih izvora za potrebe omogućavanja ili poboljšanja rekonstrukcije krivičnog događaja“ (DFRWS technical report: A Road Map for Digital Forensic Research, New York 2001, http://www.dfrws.org/2001/dfrws-rm-final.pdf, 15).

Osim termina digitalna forenzika, pojedini autori koriste termin „forenzičko računarstvo“, kojim označavaju iste one aktivnosti koje su obuhvaćene prethodno pomenutom definicijom digitalne forenzike, ali sa dodatnom funkcijom analize bezbednosnih napada na informacione sisteme (D. Barrett, G. Kipper, Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments, Elsevier Science & Technology, Heidelberg 2010, 22).
Uprkos minornim razlikama u postojećim definicijama, za sve njih se kao zajednički imenitelj može uočiti cilj, a koji se ogleda u potrebi da se obezbedi dokazana snaga rezultata digitalne forenzike. Taj element se označava kao: „pravna prihvatljivost“ (R. McKemmish, „What is forensic computing?“, Trends and Issues in Crime and Criminal Justice 118/2002, www.aic.gov.au/publications/tandi/ti118.pdf.), „usklađenost sa pravilima o dokazivanju“ i „kvalitet naučnog dokaza“. Iz ovoga se može izvesti zaključak da je smisao digitalne forenzike iznalaženje procedura, metoda i tehnika koje rezultiraju digitalnim dokazom koji treba da ima snagu naučnog dokaza. Prema tome, cilj ove forenzičke discipline je iznalaženje naučnoizvedenih i potvrđenih metoda identifikovanja, očuvanja, prikupljanja i analize računarskih podataka i predstavljanja rezultata te analize za potrebe krivičnog postupka.

2. DIGITALNA FORENZIKA KAO NAUČNA DISCIPLINA

Cilj i svrha forenzičkih disciplina je da se kroz primenu naučno proverenih i objašnjenih metoda prirodnih i tehničkih nauka obezbedi razumevanje činjenica koje su predmet dokazivanja u krivičnom postupku. Danas se dokazi koji nastaju kao rezultat DNK analize uzimaju kao nesporni i nepobitni u krivičnom postupku. Ipak, tako nije bilo na samom početku. Prvi put se ovaj dokaz pojavio u krivičnom postupku u SAD svega dva godine nakon što je 1987. Džefris otkrio da se pomoću DNK izuzetnog iz krvi može izvršiti nesporna identifikacija lica, a što je usledilo 32 godine nakon što su Votson i Krik ukazali na postojanje ove supstance. Kao što se može uočiti iz ovog podataka, proces od faktičkog otkrića metoda do upotrebe u dokazne svrhe u krivičnom postupku je vremenski dugo trajao. Naime, nakon otkrića je bilo je potrebno da se proveri validnost upotrebljenog metoda od strane drugih naučnika, odnosno da primenom iste metodologije dođe do istih rezultata i time dokaže tačnost naučnog otkrića. Bez tog procesa, sud nije bio spreman da se osloni i pokloni veru određenom naučnom rezultatu i upotrebi ga kao dokaz u postupku. Posmatrajući razvoj forenzičkih nauka koje su danas prihvaćene kao posebne naučne discipline, nedvosmisleno se dolazi do zaključka da za uspostavljanje i validaciju jednog naučnog metoda potrebno vreme, a da bi rezultat primene tog metoda bio prihvaćen kao dokaz u krivičnom postupku, isti treba da se zasniva na proverenim naučnim saznanjima, a svi alati i procedure koji su korišćeni da bi se do dokaza došlo, trebalo bi da budu predmet nezavisnog testiranja. Međutim, šta se dešava u situaciji kada se materijal na kom se određeni

metod primenjivao menja tokom određenog vremena potrebnog za validaciju tog metoda? Od kada su utvrđeni jedinstveni markeri u DNK, metodi za analizu DNK su se menjali: razvijali su se a pojedini su bili odbacivani kao nedovoljno precizni, ali je DNK kao materijal ostao isti. Isto tako, metodi za analizu boje su se tokom godina menjali, ali su retke nove tehnologije za izradu boje koje se ne mogu analizirati nekom od postojećih i prihvaćenih metoda za analizu, što nikako nije slučaj sa informacionim tehnologijama (P. Sommer, „Forensic science standards in fast-changing environments“, Science and Justice 1/2010, 12).

Da bi se digitalna forenzika mogla smatrati naučnom disciplinom, potrebno je da zadovoljava nekoliko kriterijuma: da postoji razvijena teorija (sistem izjava i principa kojima se nastoje objasniti kako stvari funkcionišu) i u okviru teorije određene apstrakcije i modeli (razmatranja povrh očiglednog, faktičkog i uočenog); da teorije polazi od određenih praktičnih elemenata (povezane tehnologije, alati i metodi); da postoji korpus literature i profesionalne prakse kao i poverenje u teorijom potvrđene rezultate u praksi (korisnost i svrsishodnost). U vezi sa navedenim, može se postaviti pitanje, da li je digitalna forenzika naučna disciplina?

Trenutno bi se moglo reći da digitalna forenzika zadovoljava samo neke od ovih kriterijuma, da je još u povoju i da postoji potreba za daljim usmeravanjem njenog razvoja. Naime, ne postoji saglasnost u pogledu sadržaja i značenja pojedinih pojmova - pojedine definicije su neadekvatne a brojni pojmovi nisu ni definisani. Praktični elementi se ogledaju u uobičajenoj upotrebi određenog broja alata i tehnika kojima se ukazuje određen stepen poverenja, iako nisu razvijeni u skladu sa specifičnim naučnim standardima niti su testirani u dovoljnoj meri.

Takođe, ne postoje standardna pravila koja bi omogućila jednoobrazno postupanje, niti su određene specifične oblasti znanja i veština u pravcu kojih je potrebno obučiti lice da bi se ono moglo smatrati stručnjakom za digitalnu forenziku.

Digitalna forenzika je izvorno nastala kako bi se primenom određenih tehnika i metoda prikupili računarski podaci koji se mogu upotrebiti dokazi potrebni u krivičnom postupku protiv učinilaca krivičnih dela kod kojih je računar bio sredstvo izvršenja ili objekt napada. Nadležni organi postupka već nekoliko desetina godina oduzimaju računare i sa njima povezane uređaje prvenstveno zbog toga što mogu da posluže kao izvor dokaza u krivičnom postupku, a veći deo istraživanja u okviru digitalne forenzike je bio fokusiran na ekstrakciju računarskih podataka radi prezentovanja pred sudovima. Iako se do skoro oblast digitalne forenzike stihijski razvijala (B. Lathoud, “Formalization of the Processing of Electronic traces”, International journal of Law, Computers and Technology 2/2004,188), uloženi su veliki napori u pravcu formalizacije postupanja sa elektronskim dokazima kroz izdavanje određenih vodiča[1], a

[1] Association of Chief Police Officers: Good Practice Guide for Computer-Based electronic

digitalna forenzika postala je priznata akademska disciplina koja se izučava na visokoškolskim ustanovama[2].

Međutim, danas se digitalna forenzika suočava sa brojnim izazovima. Jedan od najvećih izazova jeste kompleksnost problema prikupljanja i analize podataka usled sve veće raznolikosti digitalnih uređaja koji su izvori elektronskih dokaza i obima materijala (računarskih podataka/digitalnih dokaza). Svaki novi hardver i softver nameće razne izazove stručnjacima koji nastoje da ekstrahuju dokaze: nepoznate aplikacije, novi formati datoteka, karakteristike operativnog sistema, do tada nepoznate probleme u funkcionisanju hardvera i slično (A. Geschonneck, Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklaren, Springer, Heidelberg 2012, 53). Osim toga, pojedine konfiguracije ili uređaji sa sobom nose neke nespecifične probleme, pa ranije utvrđeno rešenje za sličan problem, a koje je u prethodnim slučajevima bilo efikasno, u konkretnoj situaciji ne funkcioniše i potrebno je pronaći novo rešenje, za šta je potrebno vreme (nekada dani i nedelje).

Kako se raznovrsnost predmeta forenzičke istrage povećava, forenzičkim stručnjacima su potrebni alati koji vrše više funkcija od proste pretrage i prezentovanja datoteka, primera radi funkcije rekonstrukcije, analize, ekstrahovanja i grupisanja podataka, te autonomnog donošenja odluka o daljim koracima. Problem predstavlja i to što se olako prihvataju kao validni rezultati analize do kojih se došlo primenom komercijalnih alata za digitalnu istragu, a ti alati nisu provereni u skladu sa zahtevima koji su postavljeni pred metodima i tehnikama jedne naučne discipline. Da bi se obezbedila ponovljivost i proverljivost rezultata, a time i validnost određenog alata, potrebno je da bude prihvaćen od strane šire naučne zajednice, ali to nije moguće pošto proizvođači komercijalnih alata ne čine izvorni kod dostupan javnosti (S. Garfinkel et al., „Bringing science to digital forensics with standardized forensic corpora“, Digital Investigation 6/2009, 4). Obezbediti ponovljivost rezultata jednog metoda je mnogo komplikovanije nego omogućiti proverljivost rezultata digitalne istrage u konkretnom slučaju u krivičnom postupku. Osim toga, s obzirom na rapidan tempo razvoja informacionih tehnologija, veoma je teško verifikovati metode koji se koriste u obradi računarskih podataka za potrebe krivičnog postupka. Može se postaviti pitanje: da li je otuda opravdano pokloniti veru digitalnom dokazu koji je nastao kao rezultat primene neprihvaćenog metoda i neproverenih tehnika?

Kako bi se potvrdila „naučnost“ digitalne forenzike, koja crpi instrumentarijum iz praktičnih disciplina, i ispratile pomenute tendencije, potrebno je prilagođavanje postojećih okvira za postupanje forenzičara, ali i stvaranje novih metoda i tehnika, naročito iz razloga: a) ne postoje standardizovane procedure i protokole postupanja, niti je terminologija standardizovana; b) upotrebljavaju se

Evidence, 2012, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.

[2] Tako npr. University of Glamorgan ima akreditovane studijske programe svih nivoa za forenzičare računarske forenzike, http://courses.southwales.ac.uk/courses.

analitički alati koji nisu u dovoljnoj meri ispitani od strane lica u pogledu kojih postoji nedostatak iskustva i obuke; v) prikupljanje i analiza računarskih podataka za potrebe krivičnog postupka može biti u sukobu sa privatnošću pojedinca usled nesigurnosti u pogledu tačnosti i efikasnosti tehnika, dužine čuvanja podataka itd, pa najnaprednija računarska tehnologija za potrebe digitalne forenzike može biti beskorisna ako nije upotrebljena u skladu sa zahtevima pravnog sistema. U vezi sa pomenutim izazovima, potrebno je dati odgovor na nekoliko bitnih pitanja:

- Nisu svi računarski podaci tragovi, a još manje su digitalni dokazi, pa se postavlja pitanje za čim forenzičar traga?
- Polazeći od karakteristika računarskih podataka, kako se obezbeđuje integritet elektronskih dokaza?
- Ako se integritet dokaza obezbeđuje standardizovanim postupanjem, u skladu sa pravilima, ko utvrđuje, na koji način i u kom obliku te standarde i pravila postupanja?
- Ko utvrđuje standarde kvaliteta (pouzdanost, preciznost, tačnost, bezbednost, fleksibilnost, ekonomičnost) za tehnike i alate koji se koriste u forenzičkoj obradi?
- Koja znanja i veštine treba da poseduju lica koja koriste tehnike i metode, da li ih je potrebno sertifikovati i ko donosi odluku o tome?

Iako na prvi pogled može izgledati da su ova pitanja samo od praktičnog značaja, odgovor na njih zahteva naučno istraživanje i ptvrdu. U tome treba da se ogleda smisao digitalne forenzike kao naučne discipline jer je njen cilj prevazilaženje apstraktne i lako izmenjive prirode računarskih podataka radi obezbeđenja integriteta i pouzdanosti elektronskih dokaza na način da se obezbedi kvalitet naučnog dokaza (forenzički ispravnog dokaza), odnosno drugim rečima, iznalaženje metoda i tehnika čijom primenom se može obezbediti da struktura računarskog podatka ostane neizmenjena od trenutka kada je isti uočen i prikupljen do predstavljanja na sudu.

Integritet elektronskog dokaza se može dovesti u pitanje iz više razloga: a) podatke u digitalnom obliku je jednostavnije izmeniti i falsifikovati neko podatke u fizičkom obliku; b) tokom analize se na određeni način menja oblik digitalnog podatka, (ono što se prezentuje kao elektronski dokaz bilo u elektronskom bilo u fizičkom (hardcopy) obliku prolazi kroz nekoliko slojeva transformacije i prebacivanja iz jednog oblika u drugi) pri čemu ne postoje korektni mehanizmi transformacije i prevođenja iz jednog oblika (koji se obrađuje) u drugi (koji se prezentuje); v) većina analiza se obavlja na digitalnoj kopiji ili klonu uređaja; g) objašnjenja analitičkih metoda mogu biti konfuzna i pogrešno se razumeti; d) nedostaju standardi postupanja sa digitalnim podacima, pa stoga postoji problem analitičke subjektivnosti; đ) pri tome postoji veliki broj alata i metoda pomoću kojih bilo ko bez previše znanja i veština može izmeniti skoro sve atribute dodeljenje podatku u digitalnom obliku. I pored pomenutih teškoća, integritet je potrebno obezbediti i očuvati, kako se ne bi ostavilo prostora za sumnju u

pouzdanost i poverenje u dokaz koji je nastao kao rezultat analize primenom određenih metoda i tehnika, jer ako je očuvan integritet a time i pouzdanost dokaza, obezbeđena je i dokazna vrednost.

Da bi se obezbedio integritet i pouzdanost digitalnog dokaza, procedura obrade dokaze mora da zadovolji dva osnova cilja: 1. Prikupljanje i analiza elektronskih zapisa se vrši tako što se prethodno preduzmu svi koraci kako bi se obezbedilo da podaci ostanu u stanju u kom su otkriveni, i 2. Forenzički proces ne sme ni na koji način da umanji dokaznu vrednost elektronskih zapisa kroz tehničke, proceduralne ili interpretativne greške. Da bi digitalni dokaz bio „forenzički ispravan", odnosno imao karakter „naučnog" dokaza, potrebno je predvideti i pratiti korake u postupanju od otkrića elektronskih zapisa (digitalnih tragova) do njihove interpretacije kao digitalnih dokaza na sudu. Svakako da je ovaj koncept logičan i svrsishodan, ali da bi ostvario punu vrednost, potrebno je postići uniformnost u postupanju sa elektronskim zapisima. Međutim, mišljenja koje korake treba preduzeti na putu od elektronskih zapisa do digitalnih dokaza, odnosno šta čini proces digitalne istrage razlikuje se od autora do autora. Stoga nije dovoljno samo razmatrati tehničke metode i alate koje je najbolje koristiti, nego je, kako bi se garantovao integritet i pouzdanost elektronskih dokaza i umanjila analitička subjektivnost u digitalnoj forenzici, od ključnog značaja pažnju posvetiti standardizaciji.

Sud jeste taj koji ocenjuje dokaze, ali sud u oceni digitalnog dokaza opravdano očekuje pomoć lica koje poseduje stručna znanja potrebna za utvrđivanje činjenica i koje primenjuje proverene tehnike u okviru standardizovanih pravila postupanja zasnovanih na naučnom metodu, i time pruža garanciju da su rezultati njegovog rada pouzdani.

3. STANDARDIZACIJA DIGITALNE FORENZIKE

U oblasti forenzičkih nauka aktuelna je rasprava o korišćenju standarda kvaliteta kao sredstva za demonstraciju podobnosti naučnih metoda čijom primenom se dolazi do materijala koji se može koristiti kao dokaz u okviru sistema krivičnog pravosuđa , jer je „uspostavljanje validnosti novih naučnih tehnika ili teorija i osnova za njihovo tumačenje neophodno, pre nego što se dokazi do koji se dođe njihovom primenom mogu koristi na sudu", a „...odsustvo dogovorenog protokola za validaciju naučnih tehnika da pre njihovog korišćenja na sudu je potpuno neprihvatljivo"[3].

Digitalna forenzika je toliko široka oblast da je moguće govoriti o specijalizacijama digitalnih forenzičara. Iako su utvrđene definicije određenih pojmova, principi i standardi, iste je potrebno prilagoditi postojećem stanju tehnološkog okruženja. Međutim, i pored toga, kao najveći izazovi koji stoje

[3] Forensic Science on Trial, http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf, 75.

forenzičkim naukama, ističe se da postoje slučajevi u kojima je dokaz do koga se došlo neproverenom forenzičkom analizom doveo do pogrešnih osuđujućih presuda[4]; „da ne postoji uniformnost u izdavanju sertifikata forenzičarima kao ni u akreditaciji forenzičkih laboratorija“ („Strengthening Forensic Science in the United States: A Path Forward“, 6); „da se neretko primenjuju neujednačena pravila postupanja“ („Strengthening Forensic Science in the United States: A Path Forward“, 133), odnosno da ne postoji konsenzus o osnovnim aspektima digitalne forenzike.

Tokom godina je formirano više udruženja i organizacija koje za cilj imaju profesionalizaciju i standardizaciju digitalne forenzike, što se nastoji postići razvijanjem standarda za postupanje, predviđanjem osnovnih kompetencije za forenzičare i povećanjem „naučne zasnovanosti“ metoda digitalne forenzike . Međutim, problem je što sve ove grupe rade nezavisno jedna od druge na ostvarenju istog cilja, što može biti kontraproduktivno. Stoga, i pored napora pomenutih aktera, postoji potreba da se u okviru naučne zajednice postigne dogovor o određenim fundamentalnim principima digitalne forenzike, kao i o tome koja osnovna znanja, veštine i sposobnosti bi trebalo da poseduje digitalni forenzičar i na koji način se potvrđuje posedovanje tih kompetencija.

Iz svega navedenog proizlazi da je, kako bi se digitalna forenzika smatrala validnom forenzičkom naukom, čije tehnike i metode rezultiraju digitalnim dokazom, veoma važno da se sertifikuju forenzičari, akredituju forenzičke laboratorije, verifikuju metodi i tehnike i standardizuju pravila postupanja.

3.1. Sertifikovanje forenzičara i akreditacija laboratorija

Ovi procesi imaju za cilj da obezbede kvalitet usluga koje pojedinci, odnosno ustanove pružaju, pri čemu se sertifikuju pojedinci a ustanove se akredituju. Sertifikovanje pojedinaca u slučaju stručnjaka digitalne forenzike treba da garantuje da je lice kompetentno za određenu oblast digitalne forenzike, dok je akreditovanje mehanizam koji treba da pruži garanciju da forenzička laboratorija ima sistem za obezbeđenje kvaliteta i da primenjuje naučne metode čiji rezultati primene su tehnički validni[5]. S tim u vezi se postavlja pitanje, koja to znanja i veštine kvalifikuju lice da bude stručnjak digitalne forenzike, odnosno koji kapaciteti laboratotije čine čine rezultate istraživanja u njoj naučno validnim?

Tehnološki aspekt je taj koji određuje oblast obrazovanja (nastavni plan i program studijskih programa čiji obrazovni profil jeste digitalni forenzičar određenog stepena zvanja), specijalizaciju (postdiplomski i stručni kursevi, te

[4] Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, „Strengthening Forensic Science in the United States: A Path Forward“, 2009, http://www.nap.edu/catalog/12589.html, 4.

[5] Više o akreditaciji forenzičkih laboratrija, D. Watson, A. Jones, Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, Syngress, Waltham 2013, 795-825.

dodatno obrazovanje i obuka u određenim užim oblastima) i sertifikovanje (od strane ovlašćenih institucija i izdavanje dozvole za rad/ upis u registar sudskih veštaka). Dakle, osim akademskog obrazovanja, potrebno je da lica steknu i dodatnu obuku i da to bude potvrđeno od strane određene nacionalne, odnosno međunarodne organizacije za sertifikovanje forenzičara. Trenutno postoji više međunarodnih udruženja osnovnih sa ciljem sertifikovanja digitalnih forenzičara[6]. Međutim, usled postojanja velikog broja operativnih sistema, hardverskih uređaja i koncepata u računarstvu, ne može se očekivati da jedno lice bude stručnjak za sve, odnosno da poseduje znanja i veštine potrebna za različite okolnosti slučaja (D. Kahvedzic, T. Kechadi, „Dialog: A framework for modeling, analysis and reuse of digital forensic knowledge“, Digital Investigation 6/2009, 23-25).

Iako ovakav mehanizam nije garancija da se greške u obradi dokaza neće pojaviti, primena sistema za obezbeđenje kvaliteta digitalne forenzike obezbeđuje validnost krajnjih rezultata, odnosno digitalnih dokaza kao naučnog dokaza. Države na različite načine pristupaju prevazilaženju ovog problema, jer su prepoznale prednosti sertifikovanja forenzičara i akreditacije laboratorija u kojima se vrše forenzička obrada digitalnih dokaza za potrebe krivičnog postupka. Oba procesa je potrebno urediti nacionalnim propisima u skladu sa međunarodno ustanovljenim standardima i prihvaćnim kriterijumima. U tom smislu su vredna pomena uputstva koje je Međunarodno udruženje za akreditaciju laboratorija[7] utvrdilo u „Smernicama za laboratorije forenzičkih nauka“ (ILAC-G19)[8]. Ove smernice su relevantne za primenu standarda Međunarodne organizacije za standardizaciju postavljenih u okviru „Opšth uslova za kompetentnost laboratorija za testiranje i kalibraciju“ (ISO/IEC 17025[9]), kojim su utvrđeni opšti uslovi koje treba da ispuni laboratorija da bi dobila odobrenje da vrši ispitivanja u oblasti forenzičkih nauka. Pomenuti standardi bi ostvarili pun smisao ukoliko bi države u odgovarajućim propisima utvrdile kao obavezne uslove koje bi laboratorija kao i pojedini forenzičari trebalo da ispune da bi dobili odobrenje za praktikovanje digitalne forenzike. Tako u Velikoj Britaniji postoji dokument „Pravila prakse i postupanja“[10] koja je 2011. godine, polazeći od pomenutih međunarodnih

[6] CSFA (http://www.cybersecurityforensicanalyst.com/), SANS Institute GIAC Certified Forensics Analyst (http://www.giac.org/certification/certified-forensic-analyst-gcfa); International Society of Forensic Examiners Certified Computer Examiner (https://www.isfce.com/certification.htm); Computer Hacking Forensic Investigator (http://www.eccouncil.org/certification/computer-hacking-forensics-investigator).

[7] International Laboratory Accreditation Cooperation (ILAC), http://ilac.org/.

[8] ILAC-G19 “Guidelines for Forensic Science Laboratories”, http://ilac.org/news/ilac-g19082014-published/.

[9] ISO/IEC 17025 :2005, https://www.iso.org/obp/ui/#!iso:std:39883:en.

[10] Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118949/codes-practice-conduct.pdf. Ovim dokumentom se uređuje postupanje forenzičara da bi rezultat obrade mogao da bude dokaz prihvatljiv u sistemu krivičnog pravosuđa, te postavljaju uslovi koje forenzičari i forenzičke laboratorije moraju da zadovolje da bi dobili odobrenje, odnosno da bi bili akreditvani da obavljaju sledeće aktivnosti: inicajalnu forenzičku aktivnost na

standarda, usvojilo pomoćno telo Home Office-a radi regulisanja forenzičkih nauka, kroz utvrđivanje pravila za primenu naučnih tehnika kako bi rezultat njihove primene mogao da bude dokaz prihvatljiv na sudu u krivičnom postupku. Sve sertifikovane laboratorije bile su dužne da usklade svoje postupanje sa Pravilima do 2013. godine i samo one laboratorije i forenzičari koji su ispunili propisane uslove dobili su dozvolu za rad od strane nadležnog tela[11], sa izuzetkom laboratorija u kojima se praktijuje digitalna forenzika kojima je ostavljen rok do oktobra 2015. da ispune uslove predviđene ILAC-G19, ISO/IEC 17025 kao i sa Pravilima prakse i postupanja (Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, 5).

3.2. Validacija i verifikacija forenzičkih alata

Stručnjak digitalne forenzike u procesu od digitalnih tragova do digitalnih dokaza koristi razne softverske i hardverske alate. Što se tiče softverskih alata, mogu se klasifikovati na sledeći način: alati za pregled (za stvaranje izveštaja o stanju sistema datoteka i tipovima datoteka na svim diskovima računarskog sistema); alati za stvaranje forenzičke slike diska (što se razlikuje od običnog kopiranja datoteka jer se stvara potpuni klon diska sa svim skrivenim datotekama i prostorima u memoriji); alati za potpuno brisanje sadržaja diska (svega što ostane nakon uobičajenog brisanja datoteka u memoriji diska); te alati za detaljnu pretragu diska.

Alati mogu biti namenjeni za detaljan dugotrajan pregled (u kontrolisanom tehničkom okruženju), za brzi pregled na licu mesta (npr. za trijažu podataka), za pregled uređaja priključenih na napajanje i spojenih sa mrežom kao i uređaja koji su ugašeni i nisu spojeni sa mrežom (P. Hunton, „The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation“, Computer Law and security Review 27/2011, 65). Veliki broj alata se koristi u forenzičke svrhe, od kojih su neki kreirani neposredno za tu namenu, a drugi imaju izvorno drugu namenu[12]. Postoji više softverskih alata koji se slobodno, odnosno besplatno mogu preuzimati sa Interneta (tzv. free/open source), a postoje i komercijalni proizvodi koje su napravili i prodaju pojedini proizvođači. Iako su većina forenzičkih alata posebno kreirani softveri, postoje i alati zasnovani na upotrebi hardvera. Hardverski uređaji su najčešće u obliku prenosivih radnih stanica, a odabir uređaja zavisi od okolnosti konkretnog slučaja i okruženja u kom se napad desio. Postoje uređaji posebno konstruisani za ovu svrhu u komercijalnoj ponudi, a forenzičar može i sam kreirati svoj.

licu mesta; stvaranje strategije za pregled lica mesta; oporavak, obezbeđenje, prevoz i skladištenje tragova i predmeta izuzetih sa lica mesta; procena, odabir, pregled, stvaranje uzoraka i analizu tragova i predmeta; testiranje upotrebom laboratorijski potvrđenih metoda; registrovanje svih preduzetih aktivnosti; procenu rezultata pregleda i testiranja; pisanje izveštaja i prezentovanje rezultata, sa pratećim tumačenjem i mišljenjem.

[11] United Kingdom Accreditation Service (UKAS), http://www.ukas.com/.

[12] Npr. JkDefrag за дефрагментизацију диска за Windows 2000/2003/XP/Vista/2008/X64.

Komercijalni alati ne dozvoljavaju korisniku uvid u način funkcionisanja (ne stvaraju se detaljni zapisi o izvršenim naredbama a time ni kako se došlo do rezultata) pa je na taj način ograničena pouzdanost i tačnost tih rezultata. Naime, radi se o tzv. closed source alatima jer prodavac alata ne daje uvid u izvorni kod softvera, za raliku od open-source alata kod kojih je kod dostupan i na osnovu njega se mogu pratiti sve aktivnosti kojima se došlo do rezultata. Da bi se obezbedila proverljivost i ponovljivost rezultata, neophodno je da alat ima mogućnost da stvara detaljan zapis o svim aktivnostima koje su preduzete da bi se do prikazanih rezultata došlo a time i da bi se obezbedio integritet elektronskih dokaza. Upravo ovo poslednje, bez obzira na tehnička poboljšanja alata, predstavlja problem. Naime, da bi se alati mogli koristiti, potrebno je, osim efikasnosti obrade i čuvanja podataka, obezbediti pouzdanost i mogućnost ponovljenog dobijanja istih rezultata, jer se u suprotnom može istaknuti prigovor ispitanosti funkcionisanja alata i poverenja u rezultate njihove primene!

Pouzdanost softverskih alata i njihova pravilna upotreba je od ključnog značaja za obezbeđenje integriteta elektronskih dokaza, a da bi alat osigurao integritet elektronskih dokaza, potrebno je da bude validan i verifikovan. Naime, metode i tehnike koje imaju za cilj da obezbede pouzdanost softvera nazivaju se validacija i verifikacija softvera, pri čemu postoje dva pristupa: inspekcija softvera (koja se odvija u svim fazama ciklusa razvoja jednog softvera) i testiranje softvera (proverava se da li funkcioniše u skladu sa namenom). U pogledu forenzičkih softverskih alata, a u skladu sa standardom ISO 17025, validacija podrazumeva potvrdu da alat, tehnika ili procedura funkcioniše ispravno i kako je predviđeno, a verifikacija je potvrda validacije u laboratorijski kontrolisanim uslovima[13]. Stoga smatramo da primena alata treba da bude u skladu sa prihvaćenom metodologijom, a da alat bude testiran da bi se rezultati dobijeni njegovom primenom mogli tretirati kao tačni i pouzdani[14]. Pri tome, nije dovoljna validacija i verifikacija koju vrše prodavci komercijalnih softverskih alata[15], jer nije u dovoljnoj meri dokumentovana i ne polazi od njihove funkcionalnosti, nego je prioritet na komercijalnim interesima. Stoga smatramo da je potrebno da to vrši telo za standardizaciju, kao što je učinjeno za metode koje se koriste u balistici ili za veštačenje DNK, kroz preispitivanje usklađenosti sa odgovarajućim ISO standardima kvaliteta (J. Beckett, J. Slay „Digital forensics: validation and verification in a dynamic work environment“, 40th Annual Hawaii International Conference on 2007. System Sciences, 2007, 266). Kako se sve više za prikupljanje i analizu računarskih podataka koriste automatizovani alati, da bi se obezbedila pouzdanost rezultata primene tih alata, potrebno je izabrati i koristiti one koji su validni, ispravni i odgovarajući u konkretnom slučaju. Iako postoji tendencija za automatizacijom digitalne istrage (automatskim izvršavanjem zadataka

[13] Više o tome, Y. Guo, J. Slay, J. Beckett, „Validation and verification of computer forensic software tool - searching Function“, Digital investigation 6/2009, 12–13.
[14] O potrebi stvaranja okvira za testiranje forenzičkih softverskih alata, Li, op.cit, 258.
[15] Kao što je Guidance Software za Encase alat ili Access data za FTK alat.

primenom određenih računarskih tehnika[16]) što je svakako dobro, jer se time umanjuje mogućnost manipulacije i greške načinjene ljudskom aktivnošću, pod uslovom da prethodni parametri za merenje efikasnosti alata budu zadovoljeni (J. Nogueira, „Ontology for Complex Mission Scenarios in Forensic Computing", The International Journal of Forensic Computer Science 1/2008, 44.), alat je, to što i treba da bude, samo pomoćno sredstvo u rukama obučenog i iskusnog stručnog licai da se forenzičar ne bi trebao oslanjati prosto na automatizovane funkcije alata, nego je nužno da razume informacione tehnologije i osnove kriminalistikei uvek da insistira na dvostrukoj validaciji tehnika (da koristi više od jedne tehnike za proveru rezultata).

3.3. Standardizacija pravila postupanja

Što se tiče standardizacije pravila postupanja, brojni teoretičari i praktičari iz oblasti digitalne forenzike nastojali su da osmisle najpogodnije modele za postupanje sa računarskim podacima (modele digitalne istrage). Takođe, pojedine organizacije i udruženja, kao i nadležni organi pojedinih država posvetili su pažnju stvaranju najadekvatnijih smernica u vidu standarda postupanja koji rezultira prihvatljivim dokazima za sistem krivičnog pravosuđa, a naročito su značajna nastojanja u okviru Međunarodne organizacije za standardizaciju. Osim pomenutog opšteg standarda koji se odnosi na uslove za rad forenzičara i laboratorija, formirana je radna grupa za izradu standarda koji su relevantni za digitalnu forenziku a kao rezultat rada ovog tela nastalo je nekoliko relevantnih standarda Prilikom formulisanja ovih standarda cilj nije bio stvaranje homogenizovanih, standardizovanih postupaka koji su u skladu sa nacionalnim propisima, s obzirom da je tako nešto uz pomoć ovih instrumenata nemoguće, nego isticanje osnovnih principa u vidu smernicama za postupanje u uobičajenim scenarijima. Smatramo da je prilikom regulisanja digitalne istrage ove standarde korisno uzeti u obzir, jer iako nisu pravno obavezujući za pojedine nacionalne države, isti mogu doprineti ujednačavanju postupanja sa digitalnim dokazima[17], s obzirom na to da su i nastali polazeći od metoda koji su prepoznati kao primeri dobre prakse.

[16] Primera radi, primenom tzv. data mining tehnika za pregled i pretragu određenih datoteka i direktorijuma. O primeru automatizacije alata u pretrazi i prikupljanju računarskih podataka (B.Carrier, E. Spafford, „Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence", Digital Forensic Research Workshop, 2005, 7).

[17] Tako je u Velikoj Britaniji, Britanska institucija za standarde 2008. godine usvojila standard „Dokazna snaga i prihvatljivost informacija u elektronskom obliku" kojim se utvrđuju formalni zahtevi za sisteme upravljanja elektronskim dokumentima a sa ciljem da se striktnim pridržavanjem propisanih tehničkih uslova obezbedi autentičnost podataka u elektronskom obliku koji se u okviru određene organizacije skladište, obrađuju i prenose. BS 10008:2008 " Evidential weight & legal admissibility of electronic information", http://shop.bsigroup.com/Browse-By-Subject/ICT/Legal-Admissibility. Poslednje izmene standarda su objavljene 2014.godine.

Postojanje standarda postupanja ima istovremeno i dobru i lošu stranu. Određujući minimalni nivo prihvatljivog načina za preduzimanje neke radnje, standardi imaju za cilj osiguranje kvaliteta, jer pružaju garanciju da su rezultati radnje preduzete u skladu sa standardima pouzdani. Iz tog razloga, logično je da sudovi više vere poklanjaju dokazima za koje postoje standardi postupanja utvrđeni od strane naučne zajednice. Sa druge strane, postojanje standarda može usporiti progres i ograničiti kreativnost. S pojavom novih tehničkih alata i problema, potrebno je prilagoditi postojeće i stvarati nove metode za rad sa elektronskim dokazima. Za razliku od fundamentalnih prirodnih nauka, kod kojih su temeljni postulati trajni i nepromenljivi, ne bi se moglo reći da je to karakteristika računarskih nauka. Štaviše, promenljivost i fleksibilnost su okosnice savremenog tehnološkog razvoja. Iz tog razloga pravila postupanja sa elektronskim dokazima koja nisu prilagodljiva promenama nisu dobro rešenje, pa je standardne operativine procedure potrebno kreirati tako da budu tehnički neutralne, a korisno ih je periodično procenjivati, te po potrebi inovirati u skladu sa tehnološkim razvojem (ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation, 2011, http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf, 30).

Kada se govori o standardizaciji postupanja, standard treba posmatrati kao troslojnu strukturu, u kojoj su slojevi hijerarhijski ustorojeni spram različitog stepena opštosti i obaveznosti. Tako, standard podrazumeva postojanje određenih:

1. Principa (najvišeg nivoa opštosti, obavezno primenljivi u svim slučajevima);
2. Modela (koji konkretizuju principe, a konkretozovani su kroz procedure), i
3. Procedura (najmanjeg stepena opštosti, prilagođene konkretnim slučajevima).

4. ZAKLJUČAK

Države treba da u svojim opštim aktima predvide operacionalizaciju ovih principa u svim fazama suočavanja sa potencijalnim izvorima elektronskih dokaza. Ove principi treba da univerzalno važe kao načela bez obzira na promene u hardveru i softveru. Osim toga, potrebno je da budu utvrđena određena pravila primene određenih radnji i mera koja se preduzimaju u vezi sa elektronskim dokazima. Ta pravila bi trebalo da budu „omeđena“ opštevažećim principima. Pri tome, iako je primena odgovarajućih alata i tehnika prilagođena okolnostima konkretnog slučaja, pravila u pogledu faza u okviru kojih se preduzimaju pojedine radnje treba da su u dovoljnoj meri generalizovana u vidu modela postupanja sa elektronskim dokazima, odnosno modela digitalne istrage. Osim što je nužno da postoje opštevažeći principi i što je potrebno da se stvori model za postupanje sa elektronskim dokazima, korisno bi bilo i da se kreiraju procedure koje bi uvažavale principe a bile u skladu i sa postvaljenim modelom postupanja. Te procedure bi zapravo korak po korak predviđale taktiku postupanja, odnosno kako se pojedini alati i tehnike koriste spram okolnosti konkretnog slučaja. Zapravo, procedure

bi predstvljale konkretizacije modela na različite slučajeve. Iz toga razloga bilo bi kontraproduktivno standardizovati procedure, već ih opravdano tretirati kao prilagodljive forme postupanja.

Značaj ovakvog raslojavanja se naročito ogleda u normiranju pravila postupanja. Naime, smatramo da principe treba kao obavezujuća pravila uneti u krivično procesno zakonodavstvo koja se moraju poštovati u svakom slučaju kada se postupa sa elektronskim dokazima, bez obzira na krivično delo povodom kog se radnje preduzimaju, a nepoštovanje principa imalo bi za posledicu nezakonitost elektronskog dokaza. Opredeljenje za određeni model digitalne istrage je od značaja za opredeljenje kako regulisati pojedine radnje koje se preduzimaju a time ima implikacije na odredbe krivičnog procesnog zakonodavstva. Nepostupanje po tako uređenim odredbama bi moglo rezultirati pravnom nevaljanošću dokaza. Same procedure postupanja ne bi trebalo zbog njihove konkretne i individualističke prirode propisivati u okviru krivičnog procesnog zakonodavstva, nego u pravilnicima, kao podzakonskim aktima, ili instrukcijama u okviru nadležnih organa. Ipak, znatnije odstupanje od utvrđene procedure moglo bi u konkretnim slučajevima da dovede do nezakonitosti dokaza.

FROM ELECTRONIC TRACES TO ELECTRONIC EVIDENCE

Starting from the fact that the nature of computer data, which could have the significance of evidence in criminal proceedings for high-tech crime, and the necessary forensic work in the collection and processing of these data, differ significantly in relation to the usual traces and evidence (given the speed at which the action can be taken and the traces in electronic form are modified, hidden or destroyed), special attention has been paid to the rules of digital forensics adapted to the specifics of data in computers, computer systems and computer networks. Therefore, the paper presents the path from electronic records, as traces, to electronic evidence.

Keywords: *criminal procedure, digital forensics, electronic evidence.*

Korišćena literatura:

1. ACPO Good Practice and Advice Guide for Managers of e-Crime Investigation, 2011, http://www.acpo.police.uk/documents/crime/2011/201103CRIECI14.pdf;
2. Barrett D., Kipper G., Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments, Elsevier Science & Technology, Heidelberg 2010;

3. Beckett J., J. Slay „Digital forensics: validation and verification in a dynamic work environment“, 40th Annual Hawaii International Conference on 2007. System Sciences, 2007;
4. Carrier B., E. Spafford, „Automated Digital Evidence Target Definition Using Outlier Analysis and Existing Evidence“, Digital Forensic Research Workshop, 2005;
5. Codes of Practice and Conduct for forensic science providers and practitioners in the Criminal Justice System, 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118949/codes-practice-conduct.pdf;
6. Committee on Identifying the Needs of the Forensic Sciences Community, National Research Council, „Strengthening Forensic Science in the United States: A Path Forward“, 2009, http://www.nap.edu/catalog/12589.html;
7. DFRWS technical report: A Road Map for Digital Forensic Research, New York 2001, http://www.dfrws.org/2001/dfrws-rm-final.pdf;
8. Forensic Science on Trial, http://www.publications.parliament.uk/pa/cm200405/cmselect/cmsctech/96/96i.pdf;
9. Geschonneck A., Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklaren, Springer, Heidelberg 2012;
10. Guo Y, J. Slay, J. Beckett, „Validation and verification of computer forensic software tool - searching Function“, Digital investigation 6/2009, 12-22;
11. Hunton P, „The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation“, Computer Law and security Review 27/2011, 61-67;
12. ILAC-G19 “Guidelines for Forensic Science Laboratories”, http://ilac.org/news/ilac-g19082014-published/;
13. ISO/IEC 17025 :2005, https://www.iso.org/obp/ui/#!iso:std:39883:en;
14. Kahvedzic D., T. Kechadi, „Dialog: A framework for modeling, analysis and reuse of digital forensic knowledge“, Digital Investigation 6/2009, 23-33;
15. Lathoud B., “Formalization of the Processing of Electronic traces”, International journal of Law Computers and Technology 2/2004
16. McKemmish R., „What is forensic computing?“, Trends and Issues in Crime and Criminal Justice 118/2002, www.aic.gov.au/publications/tandi/ti118.pdf;

17. Nogueira J., „Ontology for Complex Mission Scenarios in Forensic Computing“, The International Journal of Forensic Computer Science 1/2008, 42-50;
18. S. Garfinkel et al., „Bringing science to digital forensics with standardized forensic corpora“, Digital Investigation 6/2009
19. Sommer P., „Forensic science standards in fast-changing environments“, Science and Justice 1/2010
20. Watson D., A. Jones, Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements, Syngress, Waltham 2013.