

VEŠTAČENJE U INFORMACIONIM TEHNOLOGIJAMA

- prezentacija digitalnih dokaza pred sudom -

Momčilo Maksić, dipl. pravnik

Kratak sadržaj

U istrazi, dokazivanju kompjuterskog incidenta i sankcionisanju počinioca najbolje rezultate daje timski rad istražnog organa, tužioca veštaka za informaciono komunikacione tehnologije (ICT). Veštačenje u ovoj kompleksnoj oblasti zahteva izvlačenje iskustava iz poznatih naučno-tehničkih oblasti sudskog veštačenja (saobraćaj, medicina i.t.d.). Veštačenje u oblasti IT ima specifičnosti zbog složenosti ICT i posrednosti digitalnih dokaza. Tužioci u dokaznom postupku i pripremi prezentacije digitalnih dokaza moraju razmatrati niz pitanja, uključujući kompjuterski uskladištene i generisane dokaze i pripremu IT veštaka za svedočenje pred sudom.

Ključne reči: istraga, kompjuterski uskladišten/generisan dokaz, tužilac, IT ekspert

Abstract

In a computer incident a working team consists of of an investigator, a prosecutor and an IT expert gives the best result in investigation, adducing of proofs, and sanctioning of perpetrator. IT expert witnesses use different experiences from other scientific and technical field of expert testimony (traffic, medicine, e.g.). IT expert testimony is specific due to complexity and circumference of digital evidence. In investigation and preparation of IT expert witness for presentation of digital evidence in court room a prosecutor have to consider various questions, involving computer stored and computer generated evidence and preparation of IT expert witness for presentation of digital evidence in court room.

Key words: investigation, computer stored&computer generated evidence, prosecutor, IT expert

1. Uvod

Naglim širenjem i razvojem informacione tehnologije (IT) rastu i zloupotrebe, a to znači i potreba za suzbijanjem te pojave. Zloupotreba kao rezultat nestručnog rukovanja uređajima manje je opasna od veštih hakera koji često zlonamerno koriste mogućnost IT radi pribavljanja neke koristi. Ukazala se potreba da država u većoj meri posveti prostora u zakonskoj regulativi, u građanskoj i krivično pravnoj zaštiti oštećenih. Kako su hakeri izuzetno sposobni rukovaoci IT, ukazuje se potreba normativnog regulisanja uslova, načina i postupka, kolektivno organizovanih stručnih lica ili pojedinaca – veštaka, koji bi morali ispunjavati odgovarajuće stručne, etičke i legalne uslove, radi otkrivanja, dokazivanja i razrešavanja odlučujućih činjenica. Česta pojava je izvođenje dokaza veštačenjem svuda gde je potrebno stručno znanje kojim sud ne raspolaže, što je naročito potrebno u kompleksnim informacionim tehnologijama.

U svakom kompjuterskom incidentu, od trenutka otkrivanja do prezentacije izvučenih, analiziranih i za suđenje pripremljenih digitalnih kompjuterskih dokaza na sudu, najbolje rezultate, prema svetskim iskustvima, daje timski rad od najmanje tri profesionalca: zvaničnog organa istrage, tužioca i eksperta u oblasti IT.

Kada ne poznaju pitanja o kojima se raspravlja, problem odluke da li je neki IT ekspert dovoljno kvalifikovan, pravosudni organi razrešavaju prihvatanjem sertifikata profesionalnog strukovnog udruženja ili profesionalne interesne zajednice.

U svakoj nacionalnoj državi postoje tela i institucije za sertifikaciju iz predmetne naučne oblasti. Sud treba da prihvati da je određeni IT ekspert kvalifikovan, ako ima relevantni

sertifikat ovih tela i institucija. Iako se reputacija tela i institucija koje daju sertifikate procenjuje u svakom konkretnom slučaju, sud obično ne sumnja u takve preporuke. Priroda naučne ekspertize je takva da je grupa, organizovana u strukovano udruženje, zainteresovana da zaštiti standarde u određenoj naučnoj oblasti. Nažalost, u IT oblasti tipovi ekspertskih grupa i udruženja su različiti po formi i funkcijama od drugih naučnih i profesionalnih zajednica. Tako jedan kompetentan ekspert lako može ugroziti otkrivanje činjenica, ako ih sam pravi ili izmišlja nepostojeće standarde u toku svedočenja.

Veći je problem kada se zbog moralnog stava jedan IT ekspert ne može suprostaviti drugom, ili zauzeti suprotan stav u toku svedočenja/veštačenja, iako je suočen sa legalnim zahtevom da svedoči krajnje objektivno,

2. Iskustva veštačenja iz drugih naučno-tehničkih disciplina

2.1. Sudski veštaci za saobraćaj

Iskustva veštačenja iz drugih disciplina dragocena su za oblast IT veštačenja. Korisno iskustvo iz prakse je slučaj procenitelja štete u saobraćajnim udesima. Primeri su brojni i ta iskustva treba koristiti. Klasičan je primer tehničkih eksperata, gde dva poštena i kvalifikovana svedoka iznesu svoja svedočenja, ali ne uspevaju da adekvatno razreše tehnička pitanja, a slučaj presuđuje forenzički analitičar utvrđujući identičnost hemijskog sastava guma optuženog sa tragovima guma na mestu zločina [4]. Spremnost advokata da po svaku cenu odbrane svoju stranku, odvraća tehničke eksperte da svedoče pred sudom, jer dolaze u neprijatne situacije unakrsnog ispitivanja advokata.

Konstruktivno unakrsno ispitivanja eksperta druge strane može potvrditi tačnost osnovnih činjenica, principa ili ograničenja datih u svedočenju eksperta. Najplodnije tle za napad u unakrsnom ispitivanju IT eksperta je ispoljena pristrasnost, predrasuda ili neobjektivnost koja se može pojaviti u svedočenju jednog IT eksperta. Tu spada i činjenica da li je neki ekspert plaćen i koliko da svedoči, ili nije, i zašto svedoči ako nije plaćen.

2.2. Eksperti za forenzičku analizu umetničkih dela

Eksperti za forenzičku analizu umetničkih dela imaju velike sličnosti i nude dobra iskustva ekspertima za forenzičku analizu digitalnih dokaza. Kao u proceni falsifikata velikih umetničkih dela, IT ekspert u civilnim parnicama ili krivičnim delima kompjuterskog kriminala mora izvršiti: rekonstrukciju digitalnih kompjuterskih dokaza, ponašanje računarske mreže (RM) u slučaju napada, rekonstrukciju traga napada, identifikaciju i autentifikaciju digitalnih dokaza i njihovih autora ili korisnika.

2.3. Forenzičar geolog i ekspert za tajne grobnice

Forenzičar geolog i ekspert za tajne grobnice nude veoma dragocena iskustva za razumevanje IT ekspertize - kako na jednostavan i razumljiv način izneti naučna saznanja zvaničnim pravosudnim i istražnim organima, koji nemaju ta znanja i iskustava. Ovi eksperti potpisuju i u praksi sprovode etičke i druge kodekse ponašanja, maraju poštivati mnoge procedure i standarde, potpuno ih dokumentovati, a rezultate i zaključke bazirati na podacima, informacijama i znanjima koja pripadaju polju njihove ekspertize. Oni moraju održati svoju akademsku i profesionalnu reputaciju na najvišem nivou, jer suprotna strana

uvek pokušavati dovesti u pitanje neki deo reputacije eksperta. Ekspert- veštak mora biti spreman profesionalno i lično da uvek pruži najbolju predstavu svoje karijere, iako bez činjenica nema garancije da ispravna teorija, metode i adekvatna veština prezentacije dokaza, mogu uspešno razrešiti ijedan forenzički problem.

2.4. Sudska medicina

U sudskoj medicini, uspostavljeni standardi su podvrgnuti proverbi naučne javnosti, dok u oblasti IT, mnogi aspekti IT veštačenja samo su objavljeni kao uspešni ili neuspešni hakcerski napadi bez izlaganja široj naučnoj javnosti i uspostavljanja pouzdanih standarda u većini zemalja u svetu. Uspostavljanjem standarda iz oblasti IT ekspertskog svedočenja i IT veštačenja, olakšaće se rad IT profesionalaca, njihovih organizacija i udruženja, kao i pravosudnog sistema i društva u celini.

Kao forenzičar sudske medicine, ekspert koji u kriminalnom slučaju skuplja uzorke tela za analizu, tako i IT forenzički ekspert – IT veštak, treba da uzme tačnu fizičku kopiju slike podataka sa medija računarskog sistema i drugih uređaja za skladištenje podataka za kasniju forenzičku analizu i ispitivanje. Sudnica je sama po sebi strana i negostoljubiva sredina za IT eksperta – naučnika. Nedostatak regulative o sudskom veštačenju u oblasti IT može biti noćna mora za advokate i sudije koji nemaju načina da procene kvalifikaciju, stručne sposobnosti IT eksperta, kvalitet i pouzdanost digitalnih dokaza.

2.5. Forenzički entomolozi

Forenzički entomolozi (nauka o insektima) pomažu u utvrđivanju vremena ubistva i lokaciji tela u trenutku ubistva, analizom dokaza koji se odnose na insekte. U kompjuterskom svetu preuzeta je reč **bug** (**bag**-buba), koja označava seriju problema u programima računara, vezanih za tokove podataka.

3. VEŠTAČENJE U OBLASTI ICT

3.1. Specifičnosti veštačenja u oblasti ICT

IT eksperti iz naučnih krugova, bez obzira da li su angažovani u akademskim profesijama ili nisu, uvek su iznenađeni sa fenomenom ispitivanja u parničkom procesu. Za njih su neprihvatljiva pravila rivalstva u legalnom pravosudnom sistemu, nasuprot principa kolegijalnosti, koji je barem teoretski prisutan u svetu nauke i akademske profesije. Posebno je to slučaj u unakrsnom ispitivanju agresivnih advokata suprotne strane. Eksperti se moraju navići i na uobičajenu ležernu atmosferu u sudnici pre ulaska sudije i porote i atmosferu posle njihovog ulaska kada se sve drastično menja.

Svi izneseni primeri tehničke ekspertize ukazuju na značaj formiranja interesne zajednice (udruženja IT veštaka u oblasti IT) u datoj oblasti ekspertize, koja treba da sertifikuje principe, metodologiju i tehnologiju ekspertize i profila samih eksperata.

Suočeni sa nizom kompleksnih pitanja pravosudnog aspekta veštačenja iz raznih tehničkih oblasti, uključujući i oblast IT, iskustva svetski poznatih veštaka pokazala su da je korisno postati član asocijacije ili grupe profesionalaca koji mogu obezbediti spcifična znanja i

veštine za raznovrsne zahteve iz prakse, da bi se izvršila kompleksna istraga i prezentirali dokazi. Tako je 1990. godine formirana prva svetska asocijacija u oblasti IT - FIRST (*Forum for Incident Response and Security Teams*). Danas asocijacija FIRST ima preko 100 timova širom sveta, formiranih od članova iz akademskih institucija, komercijalnih organizacija i vladinih agencija. FIRST je internacionalna organizacija sa članovima u svim glavnim globalnim regionima u svetu.

Pošto glavni napadi dolaze sa Interneta, nužna je kooperacija FIRST i lokalnih (nacionalnih) CERT (*Computer Emergency Respons Team*) grupa iz celog sveta u na razmeni informacija, usklađivanju standarda i procedura, u konsultacijama i sl. Interesna zajednica forenzičkih analitičara (udruženja IT veštaka) u oblasti IT, mora obezbediti efikasnu zaštitu od neetičke prakse samozvanih eksperata, kritičku evaluaciju njihovog rada, i stalno preispitivanje primenjenih metoda.

3.2. Priprema dokaza za sudski process

Najznačajnije pitanje za tužioce u toku istragu, dokazivanja i pripreme za prezentaciju slučaja koji uključuje digitalne dokaze je[2]:

- da obezbede osnovna znanja o tehničkim aspektima digitalnih dokaza, i
- da dopuste dovoljno vremena za rukovanje raspoloživim digitalnim dokazima.

Kako efikasne pripreme za glavni pretres počinju već nakon završetka istražnog postupka, potreba za kompetentnim tehničkim znanjima održava se kroz ceo tok slučaja. U predistražnom postupku, u procesu pripreme treba obratiti pažnju na:

1. pripremu tužioca na obim istrage koja se odnosi na digitalne dokaze,
2. efikasnu komunikaciju između tužioca, organa istrage i forenzičkog analitičara, i
3. na rukovanje sa digitalnim dokazima.

3.3. Preliminarna priprema tužioca

Idealno, slučaj sa digitalnim dokazima treba da razvije i priprema tim koji se sastoji od najmanje tri lica [3]:

- tužioca,
- kriminalističkog inspektora, rukovodioca istrage, i
- forenzičkog analitičara (IT veštaka).

Često slučaj sa digitalnim dokazima predstavlja posebno proceduralno i materijalno pitanje. Jedan od prvih zadataka tužioca naimenovanog za slučaj, je pregled obima istrage, što uključuje nekoliko ključnih pitanja:

- a. Priprema razumljive prezentacije slučaja za glavni pretres (otkrivanje činjenica), i
- b. Razjašnjavanje prirode tehnoloških pitanja (tehnika i alata), odnosno:
 - da li je digitalni dokaz u slučaju, kriminal “visoke tehnologije”?,
 - iako nije, da li je digitalni dokaz ipak važan aspekt slučaja?
 - da li je digitalni dokaz jednostavno uključen u istargu ili prezentaciju slučaja? (**na primer:** kompjuterska simulacija u slučaju ubistva).
- c. Identifikacija i objašnjenje izvora i prirode digitalnog dokaza u slučaju:
 - da li su kompjuterski memorijski uređaji dokazi kriminalnog akta ili su oni kontradokazi, ili su instrumenti samog kriminalnog akta,

- koji hardver, softver, OS i sistem konfiguracije su korišćeni od strane napadača ili napadnutog računara.
- da li je digitalni dokaz pronađen na izolovanom računaru ili na RM.
- d. Identifikovanje potencijalnih izvora materijalnih digitalnih dokaza (**na primer:** bekap datoteke, log datoteke, itd.).
- e. Razmatranje svih odgovarajućih kazni (**na primer:** da li slučaj posedovanja dečije pornografije, takođe uključuje kaznu za širenje dečije pornografije, itd.)

3.4. Komunikacije u predistražnom postupku

Sva tri člana istražnog tima treba da se sastaju više puta pre glavnog pretresa radi planiranja prezentacije nalaza i mišljenja u konkretnom slučaju. Ovde je uključeno nekoliko ključnih pitanja:

- a. Diskusija po svim pitanjima radi razjašnjavanja, dalje analize ili istrage, nakon uvida u slučaj tužioca;
- b. Sastanak u predistražnom postupku sa organom istrage i forenzičkim analitičarom za razjašnjenje zakonske osnove slučaja, elemenata krivičnog dela i prihvatljivih elemenata odbrane;
- c. Razmatranje sa organom istrage i forenzičkim analitičarem najverovatnijeg obima i pravca glavnog pretresa i saslušanja svedoka i unakrsnih ispitivanja, i
- d. Pravljenje razlike o tipu digitalnih dokaza.

3.5. Razmatranje propisa o rukovanju sa digitalnim dokazima

3.5.1. Definisane uslova za iznošenje digitalnih dokaza

Uslovi koje treba razmatrati pre iznošenja digitalnih dokaza pred sudom obuhvataju:

a. Diskretno pravo sudija kada je u pitanju prihvatljivost digitalnih dokaza. Svaki sudija treba biti upoznat sa Pravilnikom o rukovanju sa digitalnim dokazima.

b. Relevantnost digitalnog dokaza, odnosno, da li dokaz pomaže u dokazivanju ili pobijanju neke činjenice u slučaju, kada, normalno, takav dokaz mora biti prihvatljiv. (Pravilnik o rukovanju sa digitalnim dokazima: "relevantan dokaz je prihvatljiv", osim ako ga neki specijalni zakonski ili ustavni član ne isključuje). Relevantni dokaz se najčešće definiše kao "dokaz koji ima tendenciju da izgrađuje nepobitnu činjenicu". Za relevantnost digitalnih dokaza od posebnog su značaja:

- **Štetnost:** relevantni dokaz može biti isključen, ako sudija odredi da je dokaz neopravdano štetan, tj. "opasnost od nepotrebne štete, konfuzije ili zavođenja porote, neopravdanog kašnjenja, gubljenja vremena ili nepotrebne prezentacije kumulativnih dokaza, znatno nadmašuje njegovu dokaznu vrednost".
- **Druge akcije:** prigovor da je dokaz "dokaz drugog zločina, greške ili dela" i u slučaju digitalnih dokaza, iako takav dokaz može biti prihvatljiv za dokazivanje "motiva, prilike, namere, pripreme, plana, znanja, identiteta, ili odsustva greške ili incidenta

c. Autentifikacija, ili da li je ono što digitalni dokaz pokazuje stvarno to, mora se pokazati u toku svedočenja. Ipak, ne traži se da svedok/veštak odbaci sve moguće dokaze koji nisu ispravno autentifikovani. Standard prihvata da je dokaz autentičan, ako je autentičan sa nekom razumnom verovatnoćom.

d. Posredno svedočenje odnosi se na to da sud više voli direktnu izjavu svedoka datu kroz živo svedočenje pred sudom, koja može biti podvrgnuto unakrsnom ispitivanju, nego iznošenje digitalnih dokaza koji su po svojoj prirodi uvek posredni.. Uprošćen i koristan okvir za razmatranje pitanja posrednog svedočenja je sledeći:

- **Da li se prezentacija digitalnog dokaza uklapa u definiciju posrednog svedočenja?** Posredno svedočenje (o nečem što je svedok čuo od nekog drugog) je, u stvari, izjava data izvan sudnice, koju svedok nudi kao dokaz činjenice o predmetu o kojem svedoči pred sudom. Ako izjava ne nudi dokaz onoga šta tvrdi, onda to nije prihvatljivo posredno svedočenje. **Na primer:** u tužbi za prevaru sa kreditnim karticama, kompjuterski odštampan materijal koji se odnosi na račun osumnjičenog, a kojeg skuplja odgovorno odeljenje kompanije za kreditne kartice, moglo bi zadovoljiti suštinsku definiciju prihvatljivosti posrednog dokaza, zato što se može dokazati istina o sadržaju. Sa druge strane, dokaz o e-mail kontaktu osumnjičenog i napadnutog bez sadržaja tog e-maila ne zadovoljava suštinsku definiciju posrednog dokaza. Ovaj dokaz je relevantan samo za činjenicu da je osumnjičeni primio e-mail a ne o njegovom sadržaju.
- **Da li dokaz sadrži izjavu za posredni dokaz,** koja se definiše kao: (1) usmena ili pisana tvrdnja, ili (2) neverbalna potvrda tvrdnje drugog lica (advokata, na primer). Kritično pitanje kod digitalnog dokaza je da li je dokaz kompjuterski generisan (verovatno ne izjava), ili je uskladišten skup podataka u računaru (može uključiti izjavu). Iako je digitalni dokaz posredan, ipak je prihvatljiv prema jednom od brojnih izuzetaka Pravilnika o rukovanju sa posrednim dokazima. Najčešći primer koji se navodi je kompjuterski listing poslovanja kompanije.

e. Razlikovanje čvrstog digitalnog dokaz, prethodno uskladišten u računaru od ilustrativnih (pomoćnih) kompjuterskih dokaza. Termin *čvrsti digitalni dokaz* odnosi se na dokaz koji pomaže da se dokaže iznesena tvrdnja, a *ilustrativni kompjuterski dokaz*, na dokaz koji samo ilustruje tvrdnju (svedočenje), ali ništa sam po sebi ne dokazuje. Primeri *čvrstih dokaza* su kompjuterski printing izveštaja banke u slučaju prevare sa kreditnim karticama, e-mail u slučaju hakerisanja u kibernetičkom prostoru, datoteka slika u slučaju dečije pornografije, a kompjuterska animacija za ilustraciju svedočenja, primer je ilustrativnog dokaza. *Kompjuterski uskladišten dokaz* uključuje dokumenta i druge snimke koje je kreirao čovek, a samo se nalazi u elektronskoj formi (datoteka sa obradom teksta, e-mail poruke i.t.d.). Ovi dokazi mogu pokrenuti pitanje autentifikacije i posrednosti. *Kompjuterski generisani dokaz* predstavlja direktan izlaz kompjuterskih programa, nezavisno od korisnika (snimak *login* datoteka internet provajdera, automatski snimak telefonskih poziva, i sl.). Neki sudovi ih nerado svrstavaju u kompjuterski generisane, pošto su oni kreirani od strane čoveka pomoću kompjuterskog algoritma. Konačno, neki dokazi mogu biti kombinacija kompjuterski uskladištenih i kompjuterski generisanih dokaza. (finansijski listing sadrži i ulazne podatke koje unosi lice i izlazne podatke koje generiše sam kompjuterski program).

Tužilac i pravosudni organ moraju poznavati razliku između kompjuterski uskladištenih podataka i kompjuterski generisanih podataka. Kompjuterski generisani dokazi mogu zahtevati autentifikaciju (na primer, log podaci se lako mogu izmeniti), ali ne spadaju u kategoriju posrednih dokaza. Glavni zadatak autentifikacije je pouzdanost funkcija procesiranja i izlaznih funkcija računara.

Većina sudova priznaje da kompjuterski generisani dokazi nisu čisti posredni dokazi i prihvataju na sudu izlazne podatke, na primer radara za merenje brzine kretanja automobila, merača količine alkohola u krvi vozača, i sl. Čvrsti kompjuterski generisani digitalni dokaz je za sud isti kao i svaki drugi čvrsti dokaz (otisak prsta, biološki uzorak, DNK otisak, lažni novac, oružje kojim je počinjen zločin).

f. Autentifikacija kompjuterski uskladištenih čvrstih dokaza znači da tužilac mora pokazati da je dokaz uskladišten u računaru, ono što on tvrdi da jeste. Ključno pitanje obično se odnosi na identifikaciju autora kompjuterski generisanog dokaza i pokazivanja da dokaz nije pretrpio značajnije izmene ni u jednom aspektu koji se odnosi na predmet slučaja.

Tehnologija sve više nudi jednostavne i direktne metode autentifikacije (na primer digitalni potpis). Osumnjičeni može osporiti autentičnost tvrdnjom da je kompjuterski dokaz lako mogao biti izmenjen nakon kreiranja. Ipak u većini slučajeva sud ne prihvata takve tvrdnje bez specifičnog dokaza o izmeni predmetne datoteke. Čak šta više, ne treba dovoditi u pitanje autentičnost digitalnih podataka zbog korišćenja forenzičkog softvera koji menja beznačajne podatke, ali ne menja bitne podatke.

Moguće je pokrenuti pitanja druge vrste ulaza u predmetnu datoteku, kao što su mogućnost prisluškivanja podataka na komunikacijskim linijama, kompletnosti datoteke, ulazne procedure, primenjene tehnike i tačnosti konverzije podataka. Ako su ove stvari zaista u pitanju, tužilac mora biti spreman da dovede eksperta-svedoka koji će ih razjasniti.

Najčešći primer izuzimanja iz pravila posrednih dokaza i prihvatanje digitalnih dokaza je datoteka uskladištena u računaru koja sadrži poslovne podatke. Za ovo izuzeće tužilac mora biti spreman da pokaže da je:

- kompjuterska oprema (hardver i softver) na kojoj su uskladišteni poslovni podaci, priznata kao standardna u toj oblasti,
- unešenje podataka u računar bilo u regularnom poslovnom postupku, u prihvatljivo blisko vreme samom događaju, i
- da izvor na kojima su podaci zasnovani, kao i metoda i vreme pripreme, indiciraju da se može verovati podacima i da je njihovo prihvatanje opravdano.

Za uspostavljanje poverenja u podatke, tužilac mora dokazati:

- oslanjanje kompanije na podatke,
- zaštitu tačnosti unošenja podataka,
- sprečavanje gubitaka ili izmene podataka dok su u memoriji računara, i
- zaštitu integriteta izlaznih podataka.

Na primer: osumnjičeni je optužen za skrivanje imovine u toku procedure bankrotstva i za uništavanje ili skrivanje podataka o bankrotstvu kompanije. Sud je propisno prihvatio kompjuterske printinge o opštoj imovini kompanije, koji su sadržavali inventar, finansijske knjige i druge podatke koje je unosio knjigovođa u toku redovnog posla. Tužilac je pozvao knjigovođu koji je potvrdio: da on redovno unosi podatke u toku radnog procesa na regularnoj osnovi, da printinzi tačno pokazuju podatke unesene u regularnom postupku, da je tačnost podataka kontrolisana redovno jedanput mesečno, i da je takav sistem vođenja poslovnih knjiga standardan u industriji.

g. Papirna kopija kompjuterski uskladištenih čvrstih dokaza, prema pravilu najboljeg dokaza, zahteva da strana koja traži da dokaže sadržaj pisanog dokumenta ili podnesene

fotografije, pruži originalni pisani dokument ili fotografiju, sve dotle dok se ne primeni izuzeće od tog pravila.

Čak i ako se kompjuterski uskladišten dokument može sa tehničkog aspekta smatrati ne-originalnim dokumentom, naročito ako se uzme u obzir da su originalni podaci u računaru samo nizovi bitova (1 i 0), pravilo “najboljeg dokaza” ne pravi problem o prihvatanju kompjuterskog printinga kao originalnog dokaza, ako on tačno predstavlja uskladištene podatke. Ovaj princip primenjuje se čak i ako duplikat ili kopija digitalnih dokaza nemaju isti izgled (imaju različite fontove ili margine, i sl.).

Stranka u sporu može prezentovati sadržaj obimnog pisanog materijala, snimaka ili fotografija, koji ne mogu na pogodan način biti ispitivani u sudu, u obliku kratkog sadržaja, grafikona, ili proračuna, pod uslovom da su originali ili duplikati na raspolaganju za kopiranje ili uvid drugoj stranim u sporu. Tako je moguće obimne fakture i kompleksne dokaze u slučaju finansijske prevare izneti na sudu kao relevantne dokaze.

3.6. Prihvatljivost kompjuterski generisanih digitalnih dokaza na sudu

Prihvatljivost kompjuterski generisanih digitalnih dokaza na sudu određuju sledeći parametric:

- **Relevantnost** kompjuterski generisanih dokaza na sudu odnosi se na veliko diskretno pravo sudije da isključi dokaz na bazi: netačnosti, konfuzije, ili pogrešnog vođenja porote.
- **Način integracije:** Normalni način procesa direktnog ispitivanja sudskog veštaka je postavljanje specifičnih pitanja veštaku koja ne navode na odgovor. Advokat koji koristi kompjuterski generisani prikaz (ilustraciju) mora to pažljivo kordinirati sa postavljanjem pitanja veštaku, da bi izbegao prigovore da je prikaz u suštini produžetak usmenog iskaza ili samo vodi svedoka u iskazu, posebno ako dokaz uključuje i tonski zapis.
- **Autentifikacija i druga osnovna pitanja:** Slike koje se koriste da ilustruju svedočenje relativno je lako autentifikovati, obično je potrebno samo potvrda svedoka. Digitalna fotografija mesta zločina treba biti normalno autentifikovana kao svaka konvencionalna fotografija, ukoliko se ne pokrene stvarno pitanje nekih izmena.
- **Posrednost kompjuterski generisanog dokaza** odnosi se na karakter kompjuterski generisanog dokaza, odnosno, da li je kompjuterski generisan dokaz pripremljen za suđenje posredni dokaz, ili ne, i da li postoji neki izuzetak? Problem posrednosti dokaza može se pojaviti ako je simulacija bazirana na podacima koji nisu skupljeni u procesu akvizicije ili programima koje nije koristio IT veštak. Ako se smatra da je kompjuterski generisan eksponat posredni dokaz, svedok mora pronaći neki primenjiv izuzetak ili neki drugi način da izbege pravilo posrednih dokaza.

Autor kompjuterske animacije ili simulacije pripremljene za suđenje, mora tražiti pristanak suda, u skladu sa zakonskom regulativom, jer su takvi dokazi neprihvatljivi sve dok sud ne utvrdi da “njihova dokazne vrednost u pomaganju da se proceni mišljenje IT veštaka, znatno veća od njihovih štetnih efekata”.

4. PREZENTACIJA DIGITALNIH DOKAZA NA SUDU

4.1. *Svedočenje IT veštaka (expert opinion testimony)*

U međunarodnoj praksi razvijeno je više preporuka za ispitivanje mišljenja IT veštaka i prihvatanje istih kao dokaza na sudu [1]. U praksi IT veštačenja najčešće se prihvataju naučno utvrđeni principi (u SAD: **Daubert principi**, koji su zamenili **Fry test**). Po ovim principima sudija prihvata digitalni dokaz na osnovu njegove relevantnosti, pouzdanosti i proverljivosti predloženih naučnih metoda, tehnika akvizicije i analize i prezentacije digitalnih dokaza na sudu, za svaki konkretan slučaj. Sud odlučuje da li je svedočenje IT veštaka bilo od pomoći za utvrđivanje odlučujućih činjenica i istine.

Generalno, tehničko ekspertsko mišljenje treba da bude prihvatljivo ako: forenzički analitičari koji uvode nove softverske alate i nove verzije starijih softverskih alata za akviziciju i analizu digitalnih medija, primenjuju ove principe na nove softverske alate. Takođe, tehnike za primenu alata za akviziciju i analizu digitalnih dokaza, na osnovu kojih forenzički analitičari izvlače zaključke, moraju biti za sud relevantne, pouzdane, u skladu sa usvojenim principima i da se na zahtev mogu testirati i verifikovati.

Suđenja koja uključuju digitalne dokaze razlikuju se od svih drugih suđenja sa dva glavna aspekta:

- često se pokreće pitanje legalnosti prihvatanja digitalnih dokaza, i
- ovaj proces uključuje kompleksan skup nepoznatih pojmova i termina.

Zato je pažljiva priprema digitalnih dokaza i planiranje prezentacije i korišćenja dokaza u sudskom procesu od posebnog značaja. Dobra metoda prezentacije komplikovanih dokaza, pa i kompleksnih digitalnih dokaza, uključuje:

- a. Korišćenje vrlo jednostavnih analogija za objašnjenje generalnog koncepta (npr. slanje e-maila je kao slanje poštanske karte). E-mail kao i poštanska karta (dopisnica) ide iz lokalnog poštanskog sandučeta kroz druge pošte do lokalne pošte primaoca, a zatim u njegovo poštansko sanduče. Imati na umu da sve analogije mogu imati legalne posledice.
- b. Definisane tehničkih reči pojmovima koje pravosudni organi i porota mogu razumeti.
- c. Korišćenje slika, crteža ili grafikona za demonstraciju kompleksnih sistema
- d. Izgradnju svedočenja početi kroz uvodnu reč sa jednostavnim konceptima, a zatim preći na kompleksnija pitanja koja objasniti u detalje, radi razumevanja inicijalnih koncepata.
- e. povezivanje tehnologije u slučaju sa tehnologijama koje su prisutni pravosudni organi i drugi u sudnici već indicirali, lično iskusili, upoznali ili koristili, gde je moguće.

4.2. *Edukovanje prisutnih u sudnici*

Ako je slučaj kompleksan, potrebno je edukovanje svih prisutnih u sudnici (sudije i porote) u svakoj fazi suđenja (parnice), a treba da obuhvati sledeća pitanja:

1. Proveru usklađenosti sa naučnim principima i zakonske prihvatljivosti digitalnih dokaza i saslušanja IT veštaka pre glavnog pretresa (suđenja);
2. Primenu principa uviđaja;

3. Uvodnu izjava;
4. Svedočenje IT veštaka;
5. Unakrsno ispitivanje (davanje prigovora i odgovaranje na prigovore), i
6. Završna reč (izjava) i zatvaranje svedočenja.

Iako je važno za sudiju i porotu održavati na minimalnom nivou razumevanja, nije cilj da se od njih stvaraju eksperti za samu po sebi kompleksnu problematiku IT veštačenja. Osnovno pravilo je da tužilac održava nivo prezentacije što jednostavnijim i razumljivijim jezikom i drugim ne-verbalnim i vizuelnim metodama prezentacije dokaza i svedočenja IT veštaka. Imajući na umu da će odbrana uvek pokušavati da stvari učine složenijim nego što jesu, treba razmotriti koja pitanja prezentovati na glavnom pretresu, a koja ostaviti za unakrsno ispitivanje.

4.3. Pripreme tužioca

Svaki slučaj zahteva da tužilac pažljivo razmotri šta treba da bude dokazano/opovrgnuto i ispita sve elemente optužnice, da bi obezbedio prezentaciju ubedljivih dokaza za svaki elemenat optužnice. Slučaj sa digitalnim dokazima često zahteva da tužilac odredi šta se može i šta treba eliminisati uz razumno objašnjenje za digitalne dokaze. Ključna pitanja su:

- da li je potrebno opovrći sva alternativna objašnjenja?, i
- da li sva razumna alternativna objašnjenja mogu biti opovrgnuta?

Često postoji konflikt između praktičnih ograničenja na to šta se može dokazati ili opovrći (pobiti) i šta od alternativnih objašnjenja advokat odbrane može iskoristiti da unese razumnu sumnju u dokazni postupak ili dokaze.

Priroda kompjuterskih incidenata znači da u nekim slučajevima neće biti potpuno jasnih i adekvatnih objašnjenja za svaku posebnu anomaliju u dokazima ili su vreme i troškovi neophodni za objašnjenje svake anomalije ograničavajući faktori.

Računar i OS postaju sve kompleksniji, pa se većina administratora mreža i osoblja za održavanje IS ograničavaju na rešavanje onih problema koji se najčešće pojavljuju. IT eksperti prihvataju postojanje neobjašnjivih bagova u računarima, bez sumnje u vrednost uskladištenih i procesuiranih informacija u računaru.

Šta jedan tužilac treba da opovrgava, zavisi od samog pitanja i snage preostalih dokaza u slučaju. **Na primer:** u slučaju dečije pornografije, kada je bitan elemenat poznat, može opovrći tvrdnju odbrane da su slike uskladištene u računar osumnjičenog bez njegovog znanja, jer nije razumno prihvatiti alternativu, tj. da su se u njegovom računaru slike pojavile iz etera same po sebi.

Važno pitanje je kada izabrati trenutak pobijanja tvrdnji odbrane. **Na primer,** ako je znanje osumnjičenog o sadržaju računara bitno, ponekad je mudro dopustiti da osumnjičeni pokrene pitanje i dopusti da sami dokazi (bilo kroz unakrsno ispitivanje ili u ponovljenom procesu) pobiju ovu tvrdnju, pre nego da se opovrgavanje dokaza izvrši u glavnom pretresu. Porota obično veću pažnju posvećuje pitanjima pokrenutim na glavnom pretresu i više respektuju tužioca, nego kada odbrana postavi pitanje tužiocu, a on skoro napada argumente odbrane.

5. IT VEŠTAČENJE I NAUČNE METODE DOKAZIVANJA

5.1. Rekonstrukcija događaja u sudskom postupku kompjuterskog kriminala

Dok je svaki slučaj sa digitalnim dokazima međusobno različit, postoje neki zajednički elementi koje se javljaju u odnosu na osnovne elemente optužnice i prirode računara i RM, a to su:

a. Identitet osumnjičenog: Iako digitalni dokaz može dokazati da je kriminalni akt izvršen sa kompjutera osumnjičenog, potrebno je direktno povezivanje osumnjičenog sa računarom sa kojeg je izvršen napad. Osumnjičeni može lično biti povezan za informacije nađene u računar u na razne načine, uključujući i sledeće:

- lično priznanje ili izjavu,
- posrednim putem (osumnjičeni je jedini stanovnik na lokaciji računara),
- bitne informacije u računar postoje jedino sa znanjem osumnjičenog,
- analiza sadržaja, gramatike i stila ukazuju na osumnjičenog.

b. Znanje: U nekim slučajevima potrebno je pokazati da osumnjičeni poznaje digitalni dokaz na računar. Na primer, uobičajena odbrana u slučaju posedovanje dečije pornografije je tvrdnja osumnjičenog da nije bio svestan da su mu slike bile u njegovom računar. Ovakva tvrdnja se često može opovrći sa:

- brojem takvih nađenih fotografija,
- logička povezanost direktorijuma sa slikama (C:/Pictures/young/girls/sex),
- jedinstvenim imenima datoteka (najčešće), n.p.r.: 8yrold.jpg.baby.jpg),
- druge indikacije na računar osumnjičenog (pretplate za **newsgroup**, istorija, itd.)

c. Hronologija događaja: Vreme i datum kreiranja datoteke mogu biti moćan dokaz koji povezuje osumnjičenog sa računarom i kompjuterskim incidentom, ali imaju ograničenja:

- tačnost vremena i datuma direktno zavisi od tačnosti internog,
- vreme i datum su vezani za vremensku zonu, i
- vreme i datum se mogu lako menjati.

Tačnost ili netačnost vremena i datuma može se pokazati na razne načine, uključujući:

- konzistentno vreme štampanja, odnosno da li su sadržaji datoteka konzistentno štampani sa specifičnim zakašnjenjem u vremenu i datumu (npr. uvek nakon 1 h ili 2 dana); ako jesu, to je ubedljiv argument da se vremena i datumi datoteka mogu uporediti sa vremenom/datumom štampanja i odrediti tačno vreme/datum.
- tačnost Internet datoteka, odnosno da li su vreme i datum u datoteci konzistentni sa sadržajem datoteke? Na primer, da li je datum datoteke pisma isti kao datum u samom pismu?
- poređenje datuma e-mail hедера sa vremenom i datumom kojeg upisuje system,
- poređenje poznatih vremena i datuma sa vremenom i datumom kojeg upisuje system, odnosno, da li su datoteke skinute sa računara osumnjičenog u poznato vreme i datum i da li se datoteke koje se pojavljuju na osumnjičenom računar konzistentne sa tim vremenom i datumom?
- upoređivanje mrežnih ako je predmetni računar mrežni i provera da li su časovnici na računarima na toj mreži automatski ažurirani,
- obrazac kreiranja vremena i datuma datoteka, odnosno postoji li klaster datoteka kreiranih u isto vreme i datum?

- eksperiment odnosno, korišćenje hardvera osumnjičenog (ali nikako originalnih medija) za kreiranje i izmenu datoteka i posmatrati razlike, ako ih ima i porediti sa datotekama podataka.

5.2. Instruisanje porote

Ne postoji obrazac instrukcije porote za slučajeve kompjuterskog kriminala prihvaćen u većini pravosudnih sistema. Takođe, teško je i prilagoditi neki potvrđen sistem instrukcija porote za slučajeve kompjuterskog kriminala iz drugog pravosudnog sistema u konretan pravosudni sistem.

Dakle, ako nije potvrđen obrazac instrukcija u datom pravosudnom sistemu, mogu se koristiti instrukcije porote uzete iz analognih oblasti, bazirane na elementima sličnosti kriminalnog akta. **Na primer:** instrukcije za provalu i prevaru mogu poslužiti kao model za prevaru u kompjuteru.

Pažljivo razmotriti vrstu porote koja bi bila najbolja za konkretan slučaj kompjuterskog kriminala koji uključuje prihvatanje kompleksnih visoko tehničkih dokaza. Istražni organi mogu pomoći tužiocima u razmišljanju o odgovarajućim pitanjima i u razmatranju pravljenja celokupnog panela i individualnih članova porote koje treba pozvati. Cilj je ne izabirati tehničke eksperte da budu članovi porote, nego pronaći nekoliko lica koja imaju dovoljno iskustva iz korišćenja računara, da bi bili sposobni da prate tehničko svedočenje u toku procesa. Idealno je da jedan do dva člana porote budu sposobni da shvate digitalne dokaze i da mogu to objasniti ostalim članovima kada donose odluku posle pretresa.

Treba razmišljati o problemu uključivanja IT eksperta u porotu, na isti način kao o uključivanju lekara u porotu za slučaj u kojem je relevantna sudska medicina. Doktor može objasniti komplikovan medicinski koncept ostalim članovima porote, a IT ekspert na isti način komplikovana i kompleksna pitanja razumevanja digitalnog dokaza.

Međutim, baš kako je i doktoru potrebno vođenje da ne previdi dokaz tužioca i ne opovrgne naizgled nebitne stvari, tako i IT ekspert u poroti mora biti instruisan da svoje znanje i iskustvo, koje se odnosi na forenzičku istragu i analizu digitalnih dokaza, usmeri na prezentaciju dokaza ostalim članovima porote i pomogne donošenju odluke u toku većanja.

6. ZAKLJUČCI

1. Ukazala se potreba za detaljnijom zakonskom regulativom istrage, dokazivanja i sankcionisanja zloupotreba i slučajeva kriminala u IT, kao i za normativnim regulisanjem uslova, načina i postupka organizovanja stručnih lica–veštaka u IT i odgovarajućih stručnih, etičkih i legalnih profila koje bi morali ispunjavati, radi otkrivanja, dokazivanja i razrešavanja odlučujućih činjenica u građanskoj i krivično pravnoj zaštiti oštećenih.
2. Timski rad tužioca, kriminalističkog inspektora (rukovodioca istrage) i forenzičkog analitičara digitalnih dokaza (IT veštaka) osnovni je zahtev u istrazi, dokazivanju, pripremi i prezentaciji digitalnih dokaza pred sudom.

3. U pripremi za glavni pretres slučaja koji sadrži digitalne dokaze, tužilac mora razmatrati niz važnih pitanja, kao što su: iskustva iz drugih naučno-tehničkih oblasti ekspertskog veštačenja; autentifikacija i priprema čvrstih digitalnih dokaza za prezentaciju, i priprema IT veštaka za svedočenje pred sudom.
4. U procesu pripreme digitalnih dokaza tužilac mora razjasniti relevantana pitanja kao što su: dokazna vrednost, posrednost i prihvatljivost; štetnost i značaj za sučaj; čvrsti kompjuterski uskladišteni i kompjuterski generisani dokazi, i ilustrativni (pomoćni) kompjuterski dokazi za sučaj.
5. U procesu pripreme IT veštaka za svedočenje (veštačenje) pred sudom, tužilac mora pripremiti veštaka za: dokazivanje naučnog karaktera digitalnih dokaza, jednostavnu i uverljivu rekonstrukciju kompjuterskog incidenta (identiteta i znanja osumnjičenog, i hronologije incidenta) pred sudom, neophodnu edukaciju svih prisutnih u sudnici o najnužnijim znanjima o primenjenim IT u slučaju i za instruisanje porote.

Literatura:

1. Brodsky S. L., *Testifying in Court: Guidelines and maxims for the Expert Witness*, Washington, DC, American Psychological Association, 1991, [5].
2. Fry test, USA 54 App DC 46, 293 F. 1013 (1923); Daubert test v. MERRELL Dow Pharmaceuticals, 509 US 579 (1993). [1].
3. <http://www.atstake.com>. [20]
4. <http://www.ensfi.org>. [18]
5. <http://www.ojp.usdoj.gov/nij/pubs.htm>. [19]
6. <http://www.house.gov/judiciary/evid2001.pdf>, *Federal Rule of Digital Evidence*, USA gov.,
7. Icove D., Segar K., VonStorch W., *Computer Crime, A Crimefighter's Handbook*, O'Reilly & Associates. [6]
8. Matson J.V., *Effective Expert Testimony*, 3rd edition Boca Raton, Press, 1999, p.71 [4].
9. NIJ (National center for Forensic Science), *Digital Evidence in the Courtroom: A guide for Preparing Digital Evidence for courtroom Presentation*, mart 12, 2003, [3].
10. Pettinari D., *Handling Digital Evidence from Seizure to Court Presentation*, IOCE conference, juni 2000. [1].
11. Pollit M. M., *Report on Digital Evidence*, (FBI CART report, DC Washington, USA, Interpol Forensic Science Symposium, Lyon, France, 16-19.10.2001. [12]
12. Program obuke za forenzičke eksperte vlade SAD, (0201752794.pdf) [2].
13. Ratay R.T., *Forensic Structural Engineering Handbook*, New York, McGraw-Hill, 2000
14. Smith F. C., Gurley R. B., *A Guide to Forensic Testimony – The art and Practice of Presenting testimony as an Expert Technical Witness*, Addison – Wesley, Boston SAD, 2002, [6].
15. Whitcomb C M., *A Historical perspective of Digital Evidence: A Forensic Scientist s View*, International Journal of Digital Evidence, proleće 2002, vol.1, issue 1. [2]