Mr Branislav Božičković*
Mr Sandi Božičković
Saobraćajna i elektro škola, Doboj
Republika Srpska

UDK 343.533:004
Stručni članak
Primljen: 24. X 2014.

SPECIFIČNOSTI SVJEDOČENJA I VJEŠTAČENJA U KOMPJUTERSKOM KRIMINALU

SAŽETAK: U procesu pripreme digitalnih dokaza tužilac mora razjasni relevantana pitanja kao što su: dokazna vrednost, posrednost i prihvatljivost; štetnost i značaj za slučaj; čvrst kompjuterski uskladišteni i kompjuterski generisani dokazi i ilustrativni (pomoćni) kompjuterski dokazi za slučaj. U procesu pripreme IKT vještaka za svedočenje (vještačenje) pred sudom, tužilac mora pripremi veštaka za: dokazivanje naučnog karaktera digitalnih dokaza, jednostavnu i uverljivu rekonstrukciju kompjuterskog incidenta (identeta i znanja osumnjičenog, i hronologije incidenta) pred sudom, neophodnu edukaciju svih prisutnih u sudnici o najnužnijim znanjima o primenjenim IKT u slučaju i za instruisanje porote.

KLJUČNE RIJEČI: visokotehnološki kriminal, digitalni dokazi, svjedočenje IT vještaka.

Uvod

Visokotehnološki kriminal obuhvata skup krivičnih dela gde se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku. Ova definicija uključuje veliki broj zloupotreba informacionih tehnologija, kao i oblast zloupotreba u radio-difuznim tehnologijama. Tako se razlikuju krivična dela gde su računari pojavljuju kao sredstvo izvršenja (Computer Related Crime) i kao objekat izvršenja (Computer Crime), kao i krivična dela u čijem se načinu izvršenja pojavljuju elementi nezakonitog korišćenja Interneta.

Broj i vrste krivičnih dela iz oblasti visokotehnološkog kriminala, kao i ekonomsku štetu koja nastaje izvršenjem ovih krivičnih dela, veoma je teško proceniti. Međutim, broj izvršenja krivičnih dela i ekonomska šteta koja je do sada registrovana iz godine u godinu u stalnom je porastu. Načini izvršenja krivičnih dela, zbog same prirode savremenih informacionih tehnologija, veoma su raznoliki i sve sofisticiraniji.

Visokotehnološki kriminal obuhvata skup krivičnih dela protiv bezbednosti računarskih podataka i to:

- Oštećenje računarskih podataka i programa;
- Računarsku sabotažu;
- Pravljenje i unošenje računarskih virusa;
- Računarsku prevaru;
- Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka;
- Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži i
- Neovlašćeno korišćenje računara ili računarske mreže.

*tumac@teol.net

Pored navedenih krivičnih dela u ovu oblast spadaju i krivična dela protiv intelektualne svojine, imovine i pravnog saobraćaja kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. U skladu sa ovom zakonskom definicijom u oblast visokotehnološkog kriminala spadaju i krivična dela gde se računari i računarske mreže javljaju kao sredstvo izvršenja krivičnih dela prevare, kod zloupotreba platnih kartica na Internetu, zloupotreba u oblasti elektronske trgovine i bankarstva, zloupotrebe dece u pornografske svrhe na Internetu (tzv. dečja pornografija), govora mržnje na Internetu (širenje nacionalne, rasne, verske mržnje i netrpeljivosti i sl.). Najčešći oblici izvršenja krivičnih dela na Internetu su računarske prevare vezane za aukcijske Internet sajtove (elektronske prodavnice), kompromitovanje i zloupotreba platnih kartica, „Nigerijske“ prevare, DDoS napad.

1. Vještačenje u kompjuterskom kriminalu

Eksperti IKT iz naučnih krugova, bez obzira da li su angažovani u akademskim profesijama ili nisu, uvek su iznenađeni sa fenomenom ispitvanja u parničkom procesu. Za njih su neprihvatljiva pravila rivaliteta u legalnom pravosudnom sistemu, nasuprot principa kolegijalnosti, koji je se podrazumeva i barem je teoretski prisutan u svetu nauke i akademske profesije. Posebno je to slučaj u unakrsnom ispitivanju agresivnih advokata suprotnih strana. Takođe, eksperti se moraju navići i na uobičajenu ležernu atmosferu u sudnici pre ulaska sudije i porote i krajnje napetu atmosferu posle njihovog ulaska, kada se sve drastično menja, [10].

Generalno, specifične vještine koje digitalni forenzičar za ekspertsko svedočenje i/ili vještačenje treba da poseduje mogu se grupisa u sledeće kategorije**:**

- Identifikovanje relevantne elektronske dokaze za povredu specifičnog zakona;
- Identifikovanje i objasni vjerovatni uzrok u mjeri koja je dovoljna za dobijanje naloga za pretres i razumije ograničenja naloga;
- Locira i oporavi relevantne elektronske dokaze iz računara primenom različitih forenzičkih alata;
- Razume i održava sve zahtjeva u lancu istrage;
- Sledi dokumentovan proces digitalne forenzičke istrage (standardne operativne procedure).

Posebno digitalni forenzičar mora posedova specifične vještine i poznava sledeće izvore digitalnih dokaza:

1. *Izvore korisnički kreiranih elektronskih dokaza:*
    - address book (adresar)
    - fajlovi e-pošte,
    - audio/video fajlovi,
    - fajlovi slika/grafike,
    - kalendari,
    - Internet indeksi (*bookmark*) za omiljene lokacije (*favorites*),
    - fajlovi baza podataka,
    - fajlovi tabela (*spreadsheet*),
    - dokumenta ili tekstualni fajlovi.

2. *Izvore kompjuterski generisanih digitalnih dokaza*:
    - fajlovi za bekapovanje,
    - log fajlovi,
    - konfiguracioni fajlovi,
    - printerski *spool* fajlovi,
    - kolačići (*cookies*),
    - *swap* fajlovi,
    - skriveni fajlovi,
    - sistemski fajlovi
    - fajlovi istorije rada aplikacija,
    - privremeni fajlovi.
3. *Mjesta za pretraživanje i identifikaciju digitalnih dokaza*:
    - loši klasteri,
    - računarski podaci o datumu, vremenu i lozinki,
    - izbrisani fajlovi,
    - slobodan prostor diska (neupisani klasteri),
    - sakrivene patricije,
    - izgubljeni klasteri,
    - metapodaci u fajl sistemu,
    - druge patricije,
    - rezervisane oblas u logičkim patricijama fajl sistema,
    - fajl *slack* prostor,
    - informacije o registraciji softvera,
    - sistemske oblas u fajl sistemu (FAT 16, FAT 32) i oblast podataka u NTFS fajl sistemu,
    - nealocirani prostor diska (ostaci podataka izbrisanih fajlova).

4. *Izvore dokaza o aktvnostima na Internetu:*
    - kolačići (*cookies*): lokacija, sadržaj, alati kolačića,
    - keš pretraživanja (Internet keš): lokacija, alati.

Svi izneseni primjeri tehničke ekspertize i zahtjevi za specifičnim vještnama u oblasti digitalne forenzike, ukazuju na značaj formiranja na nivou države, pored zvaničnih organa digitalne forenzičke istrage, šire interesne zajednice digitalnih forenzičara i drugih eksperata za istragu kompjuterskog kriminala (na primer, instuta ili strukovnih udruženja IKT vještaka u različim oblastima kompjuterskog kriminala). Ova zajednica treba da obezbedi standardizaciju i sertifikaciju: principa, metodologije i tehnologije digitalne forenzičke istrage, akvizicije, analize i ekspertskog svjedočenja/ vještačenja pred sudom, kao i profesionalnih profila samih IKT eksperata.

2. Priprema dokaza za sudski proces

Najznačajnija pitanja za tužioce u toku istrage, dokazivanja i pripreme za vještačenje pred sudom je da obezbede osnovna znanja o tehničkim aspektima digitalnih dokaza i 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 cijeli tok slučaja.

U predistražnom postupku, u procesu pripreme treba obratiti pažnju na pripremu tužioca na obim istrage, efikasnu komunikaciju između tužioca, organa istrage i forenzičkog analičara i na rukovanje sa digitalnim dokazima.

3. Preliminarna priprema tužioca

Idealno, slučaj sa digitalnim dokazima treba da razvija i priprema tim koji se sastoji od najmanje tri lica: tužioca, kriminalističkog inspektora i forenzičara (IKT veštaka). Često slučaj sa digitalnim dokazima predstavlja posebno proceduralno i materijalno pitanje. Jedan od prvih zadataka tužioca naimenovanog za vođenje slučaja, je uvid u obim istrage, što uključuje nekoliko ključnih pitanja i razmatranja:

- priprema razumljive prezentacije slučaja za glavni pretres (otkrivanje činjenica);
- razjašnjavanje prirode tehnoloških pitanja (tehnika i alata);
- identifikacija i objašnjenje izvora i prirode digitalnih dokaza;
- identifikovanje potencijalnih izvora materijalnih digitalnih dokaza (npr. bekap datoteke, log datoteke itd.);
- razmatranje svih odgovarajućih sankcija.

4. Komunikacije u predistražnom postupku

Sva tri člana istražnog tima treba da se sastaju više puta pre glavnog pretresa radi planiranja vještačenja nalaza i razmene mišljenja o konkretnom slučaju, uključujući: razjašnjavanje i analizu rezultata istrage, zakonske osnove slučaja, elemenata krivičnog dijela i prihvatljivih elemenata odbrane; razmatranje najverovatnijeg obima i pravca glavnog pretresa, saslušanja svedoka i unakrsnih ispitivanja; određivanje tipa digitalnih dokaza i razmatranje propisa o rukovanju sa digitalnim dokazima.

5. Definisanje uslova za iznošenje digitalnih dokaza

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

- Diskreciono pravo sudija o prihvatljivos digitalnih dokaza;
- Relevantnost digitalnog dokaza za dokazivanje, ili pobijanje osnovane sumnje, gde je relevantan „dokaz koji ima tendenciju da izgrađuje nepobitnu činjenicu“, a posebno se razmatraju štetnost i prigovor da je dokaz „dokaz drugog zločina, greške ili djela“;
- Autentifikacija digitalnog dokaz u toku svjedočenja sa nekom razumnom vjerovatnoćom;
- Posrednost svjedočenja zbog posredne prirode digitalnih podataka i dokaza;
- Razlikovanje čvrstog digitalnog dokaza prethodno uskladištenog u računaru, od ilustrativnih (pomoćnih) kompjuterskih dokaza koji samo ilustruje tvrdnju (svjedočenje), ali ništa sam po sebi ne dokazuje;

- Autentifikacija kompjuterski uskladištenih čvrstih dokaza čime tužilac mora pokazati da je dokaz uskladišten u računaru, upravo ono što tvrdi da jeste;
- Prihvatljivost papirne kopije kompjuterski uskladištenih čvrstih dokaza, prema pravilu najboljeg dokaza.

Čak i ako se kompjuterski uskladišten dokument može sa tehničkog aspekta smatra neoriginalnim 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 odštampanog kompjuterskog dokaza kao originalnog dokaza, ako on tačno predstavlja uskladištene podatke. Ovaj princip primenjuje se čak i ako duplikat/ kopija digitalnih dokaza nema is izgled (ima različite fontove, margine i slika). Tako je moguće obimne fakture i kompleksne dokaze u slučaju finansijske prevare iznijeti na sudu kao relevantne dokaze.

6. Prihvatljivost kompjuterski generisanih digitalnih dokaza na sudu

Prihvatljivost kompjuterski generisanih digitalnih dokaza na sudu odre uju sledeći parametri: relevantnost digitalnih dokaza; način integracije digitalnih dokaza kroz iskaz IKT veštaka u sudski proces; autentifikacija i druga osnovna pitanja zaštite integriteta digitalnih dokaza; posrednost kompjuterski generisanog dokaza, sa mogućnošću provere integriteta dokaza od uzimanja imidža u procesu akvizicije do vještačenja pred sudom, ako to sud zahtjeva.

7. Digitalni komjuterski dokaz

Prema defniciji IOCE u oblasti digitalne forenzičke nauke, digitalni dokaz je svaka informacija u digitalnom obliku koja ima dokazujuću vrednost, a koja je ili uskladištena ili prenesena u takvom obliku. Pojam digitalnog dokaza uključuje kompjuterski uskladištene i kompjuterski generisane dokazne informacije, digitalizovane audio i video dokazne signale, signale sa digitalnog mobilnog telefona, informacije sa digitalnih faks mašina i signale drugih digitalnih uređaja.

Digitalni dokaz je bilo koja informacija generisana, obrađivana, uskladištena, ili prenesena u digitalnom obliku na koju se sud može osloni kao validnu, tj. svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi, kao i druge moguće kopije orginalne digitalne informacije koje imaju dokazujuću vrijednost i na koje se sud može osloniti, u kontekstu forenzičke akvizicije, analize i prezentacije dokaza pred sudom. Dakle, treba sakuplja sve posredne dokaze sa lica mjesta, ne samo što digitalni forenzičar misli da treba, nego i sve ono što može potencijalno indicira šta se stvarno dogodilo. U procesu akvizicije digitalnih dokaza, treba generalno snimiti listu fajlova i logova kao dokaze, čak i bez ikakve ideje šta se stvarno dogodilo.

Treba imati u dokaznom materijalu svaki fajl koji potencijalno može sadržava dokaz, pre nego što se fajl prepiše, ili izmjeni. kompjuterskom incidentu postoje tri osnovne kategorije digitalnih podataka koji mogu činiti digitalni dokaz:

- Promenljivi podaci ili informacije koje se gube nakon isključivanja računara, kao što su podaci u radnoj memoriji (RAM), rezidentni memorijski programi itd. Ovi podaci se mogu izgubi u toku procesa regularnog isključivanja računara. Otuda je veoma važno do kraja precizno sprovodi proceduru akvizicije. Prije isključivanja računara treba odmah ispitati, locirati i izvući

osjetljive i šifrovane podatke, jer se može desi da se posle isključivanja ne može doći do njih (npr. vlasnik ključa ili smart kartice za pristup je nekooperavan ili mrtav itd.);

- Osetljivi podaci ili podaci uskladišteni na čvrstom disku (HD) koji se lako mogu izmeniti, kao što je, npr. poslednje vrijeme pristupa log datoteci itd;
- Privremeno dostupni podaci, ili podaci uskladišteni na HD kojima se može pristupiti samo u određeno vreme (npr. šifrovani podaci).

Pravosudni aspekt digitalnih kompjuterskih dokaza

Podsjetimo se kako istražitelji, pravnici i sudije definišu dokazni materijal. Postoje formalna pravila sakupljanja dokaznog materijala, što treba da definiše normativni akt (pravilnik ili uputstvo). U anglosaksonskom sistemu postoji i zakon slučaja (case law) koji pokriva defnicije i očekivane ishode bazirane na iskustvima i odlukama drugih sudova, a govori kako druge sudije i porote interprerptiraju isti zakon.

Kompjuterski kriminal je unio poseban problem u oblast sudskog vještašenja i svjedočenja. Pravilo klasičnog svjedočenja kaže da svedok može svjedoči samo ako je očevidac, odnosno samo o onome što je lično iskusio (čuo, vidio, zna), a ne iz druge ruke, što se smatra posrednim dokazom, poznat u žargonu kao „rekla – kazala“.

Međutim, kod računara imamo upravo slučaj da se, sve što se nalazi u njemu, može svesti pod kategoriju posrednih „rekla–kazala“ dokaze. Naime, ništa direktno vezano za događaj se ne vidi u računaru, jer se login fajlova može naknadno izmeniti, promjeniti datume fajlova, izbrisati ili izmjeniti dokument, što praktino znači da samo osoba koja je izazvala kompjuterski incident (kompjuterski kriminalac) ima direktno saznanje o tome i jedini je očevidac, odnosno neposredan svjedok.

Dakle, kompjuterski podaci se mogu koristiti kao dokazi za svjedočenje samo ako su veoma pažljivo preuzete i ako zadovoljavaju specifične kriterijume u procesima forenzičke akvizicije, analize i sudskog vještačenja. Ovi su kriterijumi krični u pogledu spsobnosti digitalnog forenzičara da sakupi što više posrednih dokaza pomoću kojih se dolazi do neoborivog dokaza.

Praktično, posredni su svi dokazi u kompjuterskom krivičnom dijelu, koji se sakupe akvizicijom i analizom samog softvera, računara i/ili računarske mreže. Da bi posredni dokaz bio prihvatljiv za sud mora biti takav da potvrđuje hipotezu o čvrstom dokazu, ili da je pobija.

Drugo, mora postojati dokaz da je podatak u log fajlu, kao posredni dokaz, nastao u normalnom radnom procesu. Na primer u slučaju pada servera, potrebno je imati čvrste dokaze da je počinilac bio logovan kada je server pao. Ovo je dovoljno čvrst dokaz da nadležni istražitelj službeno zahteva prisluškivanje linije osumnjičenog i snimi vreme pristupa serveru. Ovo vreme se kasnije upoređuje sa login podacima u log fajlovima računara i aktivnostima drugih mrežnih uređaja, što utvrđuje neoboriv dokaz pristupa serveru.

Digitalni kompjuterski dokazi moraju zadovolji i sve ostale zahteve pravosudnih organa, koji se odnose na sudske dokaze i to: ako je potrebno koristiti kopiju, ona mora bi najbolja; ako je original na raspolaganju onda kopija ne važi; kopija može zadovolji sve zahtjeve za izvođenje dokaza (npr., printng, login fajlova), ako postoji originalni fajl u kompjuteru za poređenje; sudski veštak za IKT mora svjedoči kako je kopija napravljena (npr., štampana kopija login fajlova) kao i druge detalje rukovanja sa fajlom i štampanom kopijom.

8. Svjedočenje i vještačenje IKT eksperta

U međunarodnoj praksi razvijeno je više preporuka za ispitivanje mišljenja – svjedočenja ili vještačenja IKT eksperta (*expert opinion testimony*) i prihvatanje istih kao dokaza na sudu.
U praksi IKT vještačenja najčešće se prihvataju dokazi utvrđeni na naučnim principima. 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 svjedočenje IKT vještaka bilo od pomoći za utvrđivanje odlučujućih činjenica i istine. Generalno, sud može prihva ekspertsko svjedočenje, gde IKT ekspert na poziv suda, iznosi svoje stručno mišljenje o digitalnim dokazima koji optužuju ili oslobađaju, ali ne iznosi mišljenje o utvrđenim činjenicama, koje su relevantne za slučaj. Tehničko ekspertsko mišljenje treba da bude prihvatljivo za sud i kada ekspert/ forenzičar uvodi nove sofverske alate ili nove verzije starijih softverskih alata za akviziciju i analizu digitalnih medija, ali primjenjuje naučne principe digitalne forenzike i to na zahjtev suda može potvrdi. Takođe, tehnike za primenu alata za akviziciju i analizu digitalnih dokaza, na osnovu kojih forenzičar izvlači zaključke, moraju bi za sud relevantne, pouzdane, proverljive i u skladu sa usvojenim principima i da se na zahtjev suda mogu testirati i verifikovati. IKT vještašenje podrazumjeva da o digitalnim dokazima svjedoči zakleti IKT ekspert – ovlašteni sudski veštak, koji iznosi stručno mišljenje o digitalnim dokazima, ali i o utvrđenim relevantnim činjenicama koje se odnose na slučaj.

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. Dobar metod prezentacije kompleksnih digitalnih dokaza, uključuje:

- Korišćenje vrlo jednostavnih analogija za objašnjenje generalnog koncepta (npr. slanje e-maila je kao slanje poštanske karte);
- Definisanje tehničkih riječi pojmovima koje pravosudni organi i porota mogu razumije;
- Korišćenje slika, crteža ili grafikona za demonstraciju kompleksnih sistema;
- Izgradnju svjedočenja početi kroz uvodnu riječ sa jednostavnim konceptima, a zatim, preći na kompleksnija pitanja koja objasni u detalje;
- Povezivanje tehnologije u slučaju sa tehnologijama koje su prisutni pravosudni organi i drugi u sudnici već upoznali ili koristili, gdje je moguće.

Edukovanje pravosudnih organa

Ako je slučaj kompleksan, potrebno je edukovati sve prisutne u sudnici (sudiju i porotu) u svakoj fazi suđenja (parnice). Edukacija treba da obuhva: provjeru usklađenosti sa naučnim principima; proveru zakonske prihvatljivosti digitalnih dokaza i saslušanja IKT vještaka pre glavnog pretresa; primenu principa uviđaja; uvodnu izjavu; svjedočenje/ vještačenje IKT eksperta; unakrsno ispitivanje i završnu riječ (izjavu) i zatvaranje svjedočenja/ vještačenja.

Iako je važno za sudiju i porotu održava na minimalnom nivou razumevanja, nije cilj da se od njih stvaraju eksperti za samu po sebi kompleksnu problematiku IKT vještačenja, nego da shvate suštinu ekspertskog svjedočenja ili vještačenja. 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.

Često postoji konnflikt između praktičnih ograničenja na to šta se može dokaza ili opovrgnuti (pobiti) i šta od alternativnih objašnjenja advokat odbrane može iskoristiti da unese razumnu sumnju u dokazni postupak ili dokaze. Šta jedan tužilac treba da opovrgava, zavisi od samog pitanja i snage preostalih dokaza u slučaju. Na primjer, u slučaju diječije pornografije, kada je bitan elemenat poznat, može opovrgniti 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 same po sebi, osim ako odbrana ne dokaže da je računar kompromitovan (*zombiran*) trojancem i rutkit tehnikom.

Važno pitanje je kada izabra trenutak pobijanja tvrdnji odbrane. Na primer, ako je znanje osumnjičenog o sadržaju računara značajno, ponekad je mudro dopustiti da osumnjičeni pokrene pitanje i da sami dokazi (bilo kroz unakrsno ispitivanje, ili u ponovljenom procesu) pobiju ovu tvrdnju, pre nego da se opovrgavanje dokaza izvrši u glavnom pretresu.

9. Rekonstrukcija događaja u sudskom postupku kompjuterskog kriminala

Dok je svaki slučaj vještačenja koji uključuje digitalne dokaze međusobno različit, postoje neki zajednički elementi koji se javljaju u odnosu na osnovne elemente optužnice i prirodu računara i mreža, a to su:

- 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, na bazi ličnog priznanja ili izjave, posrednog zaključivanja, bitne informacije u računaru koje mogu postojati jedino sa znanjem osumnjičenog, analize sadržaja, gramatike i stila koji ukazuju na osumnjičenog i slika.
- Znanje: U nekim slučajevima potrebno je pokazati da osumnjičeni ima adekvatno znanje i poznaje digitalne dokaze na računaru.
- Hronologija događaja: Vrijeme i datum kreiranja fajlova mogu biti moćan dokaz koji povezuje osumnjičenog sa računarom i kompjuterskim incidentom, uključujući sva ograničenja koja se odnose na laku izmenu vremena i datuma u računaru.

Instruisanje porote

Ne postoji obrazac instrukcije porote za slučajeve kompjuterskog kriminala prihvatljiv za većinu pravosudnih sistema. Takođe, teško je i prilagodi neki potvrđen sistem instrukcija porote za slućajeve kompjuterskog kriminala iz drugog pravosudnog sistema u konkretan pravosudni sistem. Mogu se koristit instrukcije za porotu uzete iz oblas vještačenja fizičkih dokaza, a zasnovane na elementima sličnosti krivičnog djela. Na primer, instrukcije za provalu i prevaru mogu posluži kao model za prevaru u kompjuteru.

Treba pažljivo razmotriti sastav porote i ne birati samo tehničke eksperte da budu članovi porote, nego pronaći nekoliko lica koja imaju dovoljno iskustva iz korišćenja računara, da bi bili sposobni da prate tehničko vještačenje u toku procesa. Idealno je da jedan do dva člana porote budu sposobni da shvate digitalne dokaze i da mogu to objasni ostalim članovima, kada porota donosi odluku posle pretresa. Treba razmišlja o problemu uključivanja IKT eksperta u porotu, na isti način kao o uključivanju ljekara u porotu za slučaj u kojem je relevantna praksa sudske medicine. Kako doktor medicine može objasni komplikovan medicinski koncept ostalim članovima porote, tako i IKT ekspert može razjasni komplikovana i kompleksna pitanja razumjevanja digitalnih dokaza.

10. Zaključak

Eksperti IKT, koji uglavnom dolaze iz naučnih krugova, uvek su iznenađeni sa fenomenom ispitivanja u sudskom/parničkom procesu, posebno u slučaju unakrsnog ispitivanja agresivnih advokata suprotne strane. Za njih su neprihvatljiva pravila rivaliteta u legalnom pravosudnom sistemu, nasuprot principa kolegijalnost, koji se podrazumeva u svetu nauke i akademske profesije.

Specifične vještine koje digitalni forenzičar za ekspertsko svjedočenje i/ili veštačenje treba da poseduje mogu se grupisa u sledeće kategorije: identifikovanje relevantne elektronske dokaze za povredu specifičnog zakona; identifikovati i objasniti vjerovatni uzrok u mjeri koja je dovoljna za dobijanje naloga za pretres i razumje ograničenja naloga; locira i oporavi relevantne elektronske dokaze iz računara primjenom različitih forenzičih alata; razumjeti i održavati sve zahtjeva u lancu istrage; sledi dokumentovan proces digitalne forenzičke istrage (standardne operativne procedure) i razvija vještinu koncizne, razumljive i terminološki pojednostavljene prezentacije digitalnih dokaza i svjedočenja/vještačenja pred sudom.Timski rad tužioca/istražnog sudije, kriminalisčkog inspektora (rukovodioca istrage) i forenzičkog analitičara digitalnih dokaza (IKT veštaka) osnovni je zahtev u istrazi, dokazivanju, pripremi i prezentaciji digitalnih dokaza pred sudom. U pripremi za glavni pretres slučaja koji sadrži digitalne dokaze, tužilac mora razmatra niz važnih pitanja, kao što su: iskustva iz drugih naučno-tehničkih oblasti ekspertskog vještačenja; autentifikacija i priprema čvrstih digitalnih dokaza za prezentaciju, i priprema IKT vještaka za svjedočenje pred sudom.

LITERATURA

Anthony F. Desante, Evidentary Consideration for Collecting and Examining Hard-Drive, Media 28.11. 2001, Forensic Sciences 262, The George Washinton University.

Milosavljević, M. (2009). *Istraga kompjuterskog kriminala*. Beograd: Singidunum.

Icove, D., Segar, K., and VonStorch, W., Computer Crime, A Crimefighter's Handbook, O'Reilly & Associates.

Carrier B., Open Source Software in Digital Forensics, carrier&atstake.com).

COAST project PERDU University, httpp://www.cs.perdue.edu/coast-library. html. htt p://www.iacis.org/.

IOCE, IOCE Principles and Definitions, 2. sastanak, 7.10.1999, Marrio' Hotel, London.

Branislav Bozickovic, M.Sc.
Sandi Bozickovic, M.Sc.

SPECIFICS OF TESTIMONY AND EXPERTISE IN COMPUTER CRIME

Summary

In the process of preparing digital evidence the prosecutor must clarify relevant issues such as: the probative value, inference and acceptability; the danger and importance of the case; sturdy computer stored and computer-generated evidence and illustrative (extra) computer evidence in the case. In preparation for the ICT expert testimony (expert) before the court, the prosecutor must prepare an expert in proving the scientific nature of digital evidence, simple and convincing reconstruction of computer incident (of identity and knowledge of the suspect, and the chronology of the incident) before the court, the necessary training of all those present in the courtroom the most essential knowledge on applied ICT in the case and for instructing the jury.

Key words: cyber crime, digital evidence, the testimony of IT experts.