Pregledni članak 004.6:343.3/.7

Milana Pisarić, saradnik u nastavi
Pravnog fakulteta u Novom Sadu

ELEKTRONSKI ZAPISI KAO DOKAZI U KRIVIČNOM POSTUPKU

Sažetak: *S dostignućima tehnike i tehnologije razvile su se i nove mogućnosti i metodi zloupotrebe istih, među kojima posebno mesto zauzima kompjuterski kriminalitet. Razvoj informacione tehnologije karakteriše izuzetno velik protok digitalnih podataka u vidu elektronskih (računarskih) zapisa, a koji se nalaze u računaru ili se prenose putem računara, a mogu da budu ključni dokaz u otkrivanju i dokazivanju najraznovrsnijih zloupotreba informacione tehnologije, a pre svega zloupotrebe računara i računarskih mreža (među kojima su i kompjuterska krivična dela). U ovom radu biće reči o elektronskim (kompjuterskim) zapisima u digitalnom obliku (bitovima), načinu rukovanja istim i mogućnosti njihovog korišćenja u otkrivanju i dokazivanju kompjuterskih krivičnih dela.*

Ključne reči: *podaci kao elektronski zapisi, zloupotreba informacione tehnologije, digitalna forenzika, kompjuterska krivična dela, otkrivanje i dokazivanje kompjuterskih krivičnih dela*

1. Uvodna razmatranja

Brzi razvoj računara i računarskih mreža stvorio je i stvara čitav novi svet za nas. Računarske mreže omogućavaju lakši i brži način komuniciranja, brži prenos informacija i obavljanje poslovnih aktivnosti, pri čemu se može uočiti izuzetno velik protok digitalnih podataka u vidu elektronskih (računarskih) zapisa. Ovi podaci mogu se pojaviti u obliku teksta, slike i glasa, i mogu se prikazati na ekranu računara ili biti odštampani, i kao takvi nositi značajnu saznajnu vrednost.

Podaci kao elektronski zapisi, u vidu datoteka i direktorijuma, koji se nalaze u računaru ili se prenose putem računara - mogu da budu ključ-

ni dokaz u otkrivanju i dokazivanju najraznovrsnijih zloupotreba informacione tehnologije, a pre svega zloupotrebe računara i računarskih mreža, među kojima su i kompjuterska krivična dela.

2. Otkrivanje i dokazivanje kompjuterskih krivičnih dela

Kompjuterski kriminalitet (kriminalitet vezan za kompjutere) mogao bi se odrediti kao vršenje određenih krivičnih dela zloupotrebom kompjutera/ računara, odnosno kompjuterskih sistema.[1] Kompjuterski kriminalitet predstavlja oblik kriminalnog ponašanja kod koga se korišćenje kompjuterske tehnologije i informatičkih sistema ispoljava kao način izvršenja krivičnog dela, ili se kompjuter upotrebljava kao sredstvo ili cilj izvršenja, čime se ostvaruje neka u krivičnopravnom smislu relevantna posledica.[2] Da bi se stalo na put i ušlo u trag ovakvim zlopotrebama, vremenom su se razvijale nove procedure u prikupljanju dokaza za dela kompjuterskog kriminala,[3] a u teoriji se govori o „istrazi u virtuelnom okruženju".[4] Uobičajeni alati koji se koriste u otkrivanju i dokazivanju zloupotreba računarske tehnike i tehnologije su softverski, često isti oni programi koje upotrebljavaju i izvršioci kompjuterskih krivičnih dela, mada se u novije vreme sve više koriste posebni, za te namene konstruisani softveri.[5]

U okviru kriminalističke policije formiraju se posebne organizacione jednice koje se bave otkrivanjem i dokazivanjem kompjuterskih krivičnih dela. U slučaju nepostojanja istih,[6] angažuju se eksperti informaci-

---

[1] Z. Stojanović, O. Perić, Krivično pravo, posebni deo, Beograd 2007. god, str. 248.

[2] Ž. Aleksić, M. Škulić, Kriminalistika, Beograd, 2002. god, str. 396.

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

[4] M. Goodman , The emerging consensus on criminal conduct in cyberspace, International journal of law and information technology, 2002, vol. 10, No 2, str. 139- 232; D. Wall, Catching Cybercriminals: Policing the Internet, International review of law computers& technology, 1998, vol. 12, No 2 str. 201–218

[5] M. Goodman , The emerging consensus on criminal conduct in cyberspace, International journal of law and information technology, 2002, vol. 10, No 2, p. 177

[6] Ako se kriminalni akt ne otkrije već u toku izvršenja ili neposredno nakon toga, verovatno će do trenutka otkrivanja nestati mnogi tragovi i dokazi, pa krivac, iako je opravdano sumnjiv, neće moći biti uspešno krivično gonjen.

one tehnologije, a iz razloga što je otkrivanje i dokazivanje kompjuterskih krivičnih dela najčešće izuzetno težak zadatak. S obzirom na specifičnosti računarskog sistema, sasvim je moguće da svaki pojedinačni slučaj zahteva angažovanje stručnjaka sa posebnim informatičkim znanjima. Za uspešno otkrivanje i razjašnjenje kompjuterskih zloupotreba neophodan je timski rad operativnih i kompjuterskih stručnjaka, kao i multidisciplinarni pristup, koji podrazumeva upotrebu klasičnih kriminalističkih metoda i tehnika vezanih za rad i funkcionisanje računara i računarskih sistema.[7]

Postoji čitav niz poteškoća čije postojanje maksimalno otežava otkrivanje i dokazivanje ovog oblika kriminaliteta. Pored osetljive prirode elektronskih zapisa koji mogu poslužiti kao dokaz, postavlja se i pitanje pristupa istima i pitanje njihovog adekvatnog čuvanja. Osim toga, poteškoću predstavlja i činjenica da je pristup informacijama moguć u okviru jednog računarskog sistema i sa vrlo udaljenih terminala, a da se na isti način može vršiti i manipulisanje podacima, zatim mogućnost da se preko globalnih računarskih mreža, upotrebom personalnih računara, prodre u niz faktički potpuno međusobno odvojenih računarskih mreža.[8] Stoga je otežana identifikacija osumnjičenih koji se koriste najnovijim dostignućima savremene tehnologije i uvek idu korak unapred u odnosu na organe otkrivanja i gonjenja.

Razjašnjenje svakog, pa i kompjuterskog kriminala podrazumeva otkrivanje kompjuterskog krivičnog dela i učinioca i razjašnjavanje i dokazivanje krivičnog dela. Zato, bez obzira na pomenute prepreke, osnovni zadatak stručnog tima jeste utvrđivanje činjeničnog stanja, odnosno prikupljanje i obezbeđenje dokaza potrebnih za preduzimanje odgovarajućih mera protiv izvršilaca.

3. Pojam elektronskog dokaza

Osnovni cilj preduzimanja operativnih radnji je da se pronađu dokazi koji će potkrepiti ili otkloniti sumnju da je izvršena zloupotreba u elektronskom sistemu u kom je primenjena informaciona tehnologija. Postavlja se pitanje, kakvi su to dokazi, za koje se u literaturi koriste različiti termini, a najčešće se nazivaju digitalni i elektronski dokazi.

Kao digitalni dokaz može poslužiti bilo koja informacija koja je generisana, obrađivana, uskladištena ili prenesena u digitalnom obliku, od-

[7] D. Berm, Computer forensic analysis in a virtual environment, International journal of digital evidence, fall 2002, vol. 6 , issue 2, preuzeto sa internet stranice - www.ijde.org

[8] S. Petrović , Kompjuterski kriminal, Beograd, 2001. god, str. 278.

nosno svaka binarna informacija, sastavljena od digitalnih 1 i 0, uskladištena ili prenesena u digitalnoj formi[9]. Ove informacije se u računaru/ računarskom sistemu najčešće nalaze u vidu elektronskih zapisa u datotekama (file) ili direktorijumima (folder).

Elektronski dokazi su informacije i podaci koji imaju dokaznu vrednost i „mogu se koristiti u krivičnom postupku, a koji su uskladišteni ili se prenose putem elektronskih uređaja“. [10]

Pojam elektronskog dokaza obuhvata: kompjuterski uskladištene i kompjuterski generisane dokaze; digitalne audio i video signale, podatke sa mobilnog telefona, podatke sa digitalnih faks mašina i podatke sa drugih digitalnih uređaja.[11]

Kao dokaz u postupku može se upotrebiti štampani tekst koji je generisao sam računar ili samo arhivirao (tzv. rukopis osobe u elektronskoj formi), obrađen tekst procesorima za elektronsku poštu, zapisi iz aktivnosti diskusnih grupa (foruma i blogova) i virtuelnih soba za razgovor (chat-rooms), zapisi provajdera koji se tiču identifikacije korisnika (Internet protokol), telefonski zapisi, zapisi fovornih automata i sl.[12] U tu svrhu mogu da posluže: tekuće i neko prethodno stanje podataka i programa, sistemska statistika i evidencije, konzolni izveštaji, ručne evidencije, štampani izveštaji, radni nalozi, izjave pojedinih radnika i sl.[13]

Može se uočiti da zapravo postoje dve kategorije elektronskih zapisa: one koje je računar generisao i one koji su u računaru samo arhivirani. U prvoj kategoriji elektronskih zapisa su oni zapisi koje je sam računar stvorio nezavisno od korisnika (npr. zapisi provajdera internet usluga koji se tiču identifikacije korisnika prilikom uključuvanja na mrežu). Drugu kategoriju čine zapisi koje je kreirao korisnik a koji se u računaru samo čuvaju (npr. e- mail poruke).[14]

Treba dakle, imati u vidu da dokaz o kom govorimo nije, uslovno govoreći, materijalni dokaz, jer je neopipljiv i nevidljiv. Elektronski do-

---

[9] R. Morris, Evidence, International review of law computers& technology, 1998, Vol 12, No 2, p. 281

[10] B. Banović, Kompjuterski kriminalitet i zaštita ličnosti, Bezbednost,2003. god, 1/ 03, str. 36.

[11] O. Kerr, Digital evidence and new criminal procedure, Colubmia law review, 2005, Vol.105, No.1 , p. 283

[12] V. Nikolić, Otkrivanje i praćenje kompjuterskog kriminala, Bezbednost,2004. god, 2/ 04, str. 273.

[13] B. Banović, op. cit.

[14] B. Banović, Elektronski dokazi, Revija za kriminologiju i krivično pravo, 2006. god, 3/ 06, str.226

kaz je zapravo informacija/ podatak u vidu elektronskog zapisa (odnosno u digitalnom obliku) . Kao takav, ne postoji u fizičkom svetu. Nosilac elektronskog dokaza - medijum je određeni fizički predmet,[15] ali isti ne dokazuje ništa - informacija, podatak koja je zabeležena u tom medijumu je dokaz. Međutim, podatku u elektronskom obliku ne sme se osporiti valjanost samo zato što je u elektronskom obliku, već se moraju naći načini da se isti iskoristi (s obzirom na vrednost koju može imati kao dokaz).

Karakteristike elektronskih zapisa su:

a) *Neraskidiva povezanost sa visokom informacionom tehnologijom*, a prikupljanje i analiza istih zahteva primenu najsavremenijih naučnih tehnologija;

b) *Fleksibilnost* – podaci se mogu pojaviti u više oblika, kao: tekst, slika, crtež, animacija, audio i video zapis, u različitim ekstenzijama datoteka, i sl;

v) *Latentnost elektronskih zapisa* koja onemogućuje neposrednu identifikaciju sadržaja fizičkog objekta koji čuva dokaze;

g) *Izuzetna osetljivost* - lako se mogu oštetiti, odnosno izmeniti, falsifikovati, sakriti, uništiti ili na drugi način učiniti neupotrebljivim. Stoga je neophodna je brzina reagovanja organa gonjenja,[16] ali i oprez i posebne mere predostrožnosti neophodni prilikom rukovanja istima.

Polazeći od osetljivosti, mogu se razlikovati tri kategorije elektronskih zapisa, odnosno podataka koji mogu predstavljati elektronske dokaze u komjuterskoj ekscesnoj situaciji:[17]

a) *Prelazni podaci* – to su informacije koje se mogu izgubiti svaki put nakon što se isključi računar.[18] Iz razloga što postoji mogućnost da se ovakvi podaci bespovratno izgube pošto računar bude isključen, prikupljanju istih neophodno je postupiti na oprezan način, što bi podrazumevalo da pre isključivanja računara treba odmah ispitati, locirati i obezbediti osetljive i šifrovane podatke;[19]

---

[15] Medijumi bi bili ili računar ili spoljni nocioci memorije: disketa, disk, magnetna traka i sl. spoljni nosioci memorije

[16] U skladu sa kriminalističkim načelom brzine i operativnosti neophodno je odmah po saznanju da je izvršeno krivično delo, sprovesti određene operativno- taktičke radnje.

[17] Preuzeto iz Izveštaja Interpola o digitalnim dokazima (Report on Digital Evidence) sa internet stranice http://www.interpol.int/public/Forensic/IFSS/meeting13/Reviews/Digital.pdf

[18] Kao što su veze sa otvorenom radnom memorijom, memorijski rezidentni programi, itd.

[19] Takvo isključivanje računara je posebno osetljiva operacija, i zavisno od operativnog sistema, postoje dve mogućnosti: da se računar isključi na klasičan način bez

b) *Posebno osetljivi podaci* - podaci koji su uskladišteni na hard disku koji se lako mogu izmeniti;[20]

v) *Privremeno pristupačni podaci* - podaci koji su uskladišteni na hard disku kojima se može pristupiti samo u određeno vreme.[21]

Zbog prirode elektronskih zapisa i svih navedenih karakteristika, njima se mora rukovati sa oprezom, uz primenu najsavremenijih saznanja i metoda informacione tehnologije. Rukovanje elektronskim zapisima podrazumeva sakupljanje, obezbeđenje, dokumentovanje i tumačenje, a ovaj proces naziva se kompjuterska forenzika ili digitalna forenzika (forensic computing).[22]

Da bi elektronski zapisi uopšte postali vidljivi i mogli biti upotrebljeni u krivičnom postupku kao elektronski dokaz, neophodno je da se izvrši specifični uviđaj od strane stručnjaka upotrebom posebnih tehnika, opreme i softvera.

4. Specifičnosti uviđaja

Ukoliko se pojave osnovi sumnje da je izvršeno krivično delo za koje se goni po službenoj dužnosti, organi unutrašnjih poslova preduzeće potrebne mere da se pronađe učinilac krivičnog dela, da se učinilac ili saučesnik ne sakrije ili ne pobegne, da se otkriju i obezbede tragovi krivičnog dela i predmeti koji mogu poslužiti kao dokaz, kao i da prikupe sva obaveštenja koja bi mogla biti od koristi za uspešno vođenje krivičnog postupka. Po saznanju za izvršeno kompjutersko krivično delo, uviđajna ekipa izlazi na lice mesta,[23] da bi se proverili navodi u krivičnoj prijavi koja je najčešći izvor saznanja, te da bi se razjasnio slučaj i prikupili dokazi. Kada se izađe na lice mesta, neophodno je isto na adekvatan način obezbediti [24] da bi se mogao izvršiti uviđaj.

Uviđajna ekipa treba da bude sastavljena od službenih lica koja poseduju osnovna informatička znanja, kao i kompjuterskih stručnjaka, posebno

straha da će se izbrisati dokazi o upadu, ili se računar uopšte ne sme isključivati, jer bi se isključivanjem uništili dokazi o upadu, s obzirom da mogu biti ugrađene i zamke za uništavanje datoteka sa dokazima, ako se računar isključuje po propisu.

[20] Takav bi podatak bio npr. poslednje vreme pristupa loginu datoteke

[21] Takvi bi podaci bili npr. šifrovani podaci.

[22] B. Banović, Elektronski dokazi, Revija za kriminologiju i krivično pravo, 2006. god, 3/ 06, str. 224.

[23] U slučaju kompjuterskih krivičnih dela, lice mesta je određeni centar za elektronsku obradu podataka

[24] Da bi se obezbedilo lica mesta, neophodno je najpre preuzeti kontrolu nad računarom i računarskim sistemom, a može se desiti da je neophodna i zabrana pristupa računarskoj prostoriji i samim računarima svim licima koja su radila na računaru

onih koji dobro poznaju računarske sisteme koje je potrebno ispitati.[25] Da bi kriminalistička obrada započela i da bi se odvijala kako treba, pre nego što se pristupi uviđaju nad računarima, potrebno je prikupiti što više podataka o vrsti računarskog sistema, o računarskoj opremi (hardveru), o kompjuterskim programima (softverima i operativnim sistemima) koji su korišćeni, o osiguranju podataka (konfiguraciji računara uopšte), a sve sa ciljem da bi se utvrdilo gde su tražene informacije pohranjene i na koji način su obezbeđene.[26] Na osnovu ovih informacija, potrebno je odrediti i pozvati adekvatne kompjuterske stručnjake.

Prilikom uviđaja treba u svakom konkretnom slučaju ispitati hardverske komponente, pretražiti kompjuterske datoteke i direktorijume, izraditi kopije podataka, te zaštititi elektronske zapise koji mogu poslužiti kao dokaz.

Pretraživanje računarskog sistema i pronalaženje relevantnih podataka, nije nimalo jednostavan niti brz postupak, te iz tih razloga često neće biti realizovan na licu mesta i u kratkom vremenskom periodu, već će biti neophodno da se kompjuterska oprema prenese u kompjutersku forenzičku laboratoriju.[27] Međutim, već prilikom prvog pregleda računara stručnjak može da identifikuje skrivena, nelocirana i izbrisana mesta koja treba gledati, znake koje treba tražiti i dodatne izvore informacija za relevantne dokaze.[28]

U toku vršenja uviđaja potrebno je prikupiti sve potrebne informacije o funkciji i organizaciji kompjuterskog centra, konfiguraciji, o tome koji su podaci sadržani na kojim nosiocima informacija, nadležnostima i zadacima osumljičenog, proizvođaču i tipu elektronskog računarskog uređaja, pogonskom sastavu i perifernim jedinicima, obrascima doku-

---

[25] Zakon o krivičnom postupku u st.1 čl. 112 propisuje da organ koji obavlja uviđaj ili rekonstrukciju može zatražiti pomoć stručnog lica kriminalističko-tehničke, saobraćajne ili druge struke, koje će, po potrebi, preduzeti i pronalaženje, obezbeđivanje ili opisivanje tragova, izvršiti potrebna merenja i snimanja, sačiniti skice ili prikupiti druge podatke

[26] B. Banović, Kompjuterski kriminalitet i zaštita ličnosti, Bezbednost,2003. god, 1/03, str. 31.

[27] Veoma je važno, pri tom, privremeno oduzeti računar sa pratećom opremom uskladištiti na bezbedno mesto, zaštićeno od uticaja okoline, posebno elektromagnetnih polja i obezbediti ga od neovlašćenog pristupa, kako bi se sačuvao, pre svega, integritet - elektronskih dokaza.

[28] Dodatni izvori informacija mogu biti ranije forme datoteka podataka (npr. Memos, Spreadsheets, ..) koje postoje na hard disku, ili u bekap mediju, ili različito formatirane verzije podataka (npr. .templets, .doc, .pdf i sl), bilo da su tako namerno formirane ili tretirane drugim aplikativnim programima (npr. Word processing, spreadsheet, e-mail, timeline, sheduling, graphic).

mentacije programa, papirima za tabeliranje, etiketama, magnetnim trakama i priručniku organizacije,[29] kao i ostalim nosiocima informacija (medijumima).

Informacije se prikupljaju tako što se vrše pretrage u samom računaru - odnosno u datotekama (files) i direktorijumima (folders) u računaru. Međutim, prikupljanje relevantnih podataka nije nimalo lak zadatak, prvenstveno zbog ogromnog broja istih u samom kompjuteru. Kompjuterske datoteke i podaci mogu biti vidljivi, ali isto tako mogu biti sakriveni u direktorijumu, ili čak pothranjeni na udaljenom serveru. Datoteka može biti zaštićena šifrom, lažno naslovljena, sačuvana u neuobičajenom formatu, pomešana sa velikim brojem irelevantnih datoteka.

Kompjuterska datoteka se može nalaziti kako u računaru tako i na spoljnom nociocu memorije (medijumu) – trake, kartice, diskete, diskovi, pa je potrebno pretražiti računarske prostorije, uključujući i prostoriju za skladištenje memorijskih medijuma, te oduzeti i pretražiti pronađene nosioce podataka.[30] Takođe, kompjuterska datoteka često može egzistirati u različitim formama ranijih verzija, koje su još dostupne na hard disku, ali se poznavanjem lokacija njihovog postojanja i korišćenjem adekvatnih alata za digitalnu forenziku, čak i izmenjeni formati istih podataka mogu lako otkriti.

Otkrivanjem, analizom i rekonstrukcijom dokaza dobijenih iz kompjuterskih mreža, sistema, medija, perifernih uređaja, korišćenjem multidisciplinarnih znanja, kojima se omogućava rešavanje krivičnih slučajeva bavi se digitalna forenzika.

5. Digitalna forenzika

Suština i svrha digitalne forenzike je prikupljanje i analiza digitalnih dokaza, odnosno informacija iz elektronskih zapisa koji se najčešće, kao što smo videli, naleze u obliku datoteka (file).

Prikupljanje elektronskih/ digitalnih dokaza razlikuje se od tradicionalnih kriminalističih tehnika. Tradicionalne tehnike su neadekvatne zbog sledećih problema: Problema vezanih za nalaženje pristupa računarskim sistemima, nejasna priroda podataka, činjenica da podaci mogu biti sačuvani u povezanim sistemima, koji se ne nalaze u pretresanim prostorijama

[29] B. Banović, Kompjuterski kriminalitet i zaštita ličnosti, Bezbednost,2003. god, 1/ 03, str. 33.

[30] Priručnik Nacionalnog Instituta pravde SAD: Forenčizki pregled digitalnih dokaza: vodič za organe gonjenja (Forensic Examination of Digital Evidence: A Guide for Law Enforcement), preuzeto sa internet stranice:http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

itd.[31] Naime, za prikupljanje elektronskih/ digitalnih dokaza, neophodno je korišćenje validnih i relevantnih metoda koje su tehnološki osavremenjene, uz primenu specifičnih informatičkih znanja. Digitalna forenzika koristi naučno izvedene i dokazane metode za identifikaciju, sakupljanje, vrednovanje, analizu, interpretaciju, dokumentovanje, veštačenje, čuvanje, rukovanje digitalnim podacima.[32]

Kada se govori o tehnologiji koju digitalna forenzika koristi, pre svega se misli na standardizovane hardver i softver alate za otkrivanje, identifikaciju, validaciju, izvlačenje, oporavak i analizu digitalnih podataka.[33] Prilikom korišćenja pomenutih alata i tehnika, od forenzičara se zahteva da koristi forenzički sterilne medijume, da vodi računa o tome da se sačuva integritet orginalnih podataka, da označi rezultate uviđaja i analize, kopije elektronskih zapisa, štampane materijale, te da kontroliše, dokumentuje i čuva elektronske zapise kao dokaze za krivični postupak.

Nije svaka datoteka dokaz. Neophodno je od identifikovanih datoteka prepoznati relevantne, te ih izdvojiti i analizirati, što , međutim, često neće biti lak zadatak. Izvršilac krivičnog dela najčešće pokušava da nakon dela uništi sve dokaze koji bi govorili o njegovoj aktivnosti, pa tako neki podaci predstavljaju objekt brisanja. Takođe, u računaru je moguće datoteke sakriti, obrisati, kompresovati, ili sačuvati u delu hard diska koji obično nije vidljiv u operativnom sistemu.[34]

Pre nego što se pristupi prikupljanju elektronskih dokaza neophodno je najpre zaštititi računar i napraviti radnu i referentnu sliku- kopiju celog hard diska, bit po bit u .dd [35] ekstenziji primenom alata kao što su Nelson, Phillips, Enfinger& Steuart i sl.[36] Ta slika je identična kopija originalu hard diska i na njoj će se vršiti sve ostale radnje prikupljanja i analize elektronskih zapisa, podataka i sadržaja. Takođe, forenzičar oporavlja (recover) sve, ili što je moguće više izbrisanih datoteka, otkriva skrivene sa-

---

[31] Z.Đokić i dr, Problemi pribavljanja, obezbeđivanja i korišćenja dokaza u elektronskoj formi, od značaja za krivični postupak, Teški oblici kriminala, Beograd 2004.god, str.143.

[32] D. Berm, Computer forensic analysis in a virtual environment, International journal of - digital evidence, fall 2002, vol. 6, issue 2, preuzeto sa internet stranice www.ijde.org

[33] Npr. Microsoft Virtual PC 2007, VMWare softvare tools range 2007, QEMU

[34] R. Morris, Evidence, International review of law computers& technology, 1998, Vol. 12, No. 2, stp. 283.

[35] . *dd ekstenzija* (skraćenica od "dataset definition") predstavlja ekstenziju u *Uniks* programu, čija je osnovna svrha kopiranje i čuvanje neobrađenih podataka.

[36] D. Berm, Computer forensic analysis in a virtual environment, International journal of digital evidence, fall 2002, vol. 6, issue 2, preuzeto sa internet stranice - www.ijde.org

držaje (npr. u linuks operativnom sistemu to su swap i slack), pristupa sadržaju zaštićenih i šifrovanih datoteka[37].

Digitalni forenzičar će prilikom prikupljanja i analize prikupljenih i izdvojenih datoteka i podataka iskorisititi sve ove mogućnosti, i pokušaće da povrati takve podatke i da njihovom analizom ustanovi da li predstavljaju dovoljno dobar dokaz za upotrebu u krivičnom postupku. Postoje dva koraka u povraćaju podataka: hardverski i softverski.[38] Hardverski aspekt nije obavezan i sprovodi se samo u slučaju oštećenja medijuma na kome se nalaze podaci. Svaka od operacija zamene defektnog hardvera mora se izvršiti u potpuno sterilnom okruženju, te i najmanja kontaminacija može imati za rezultat trajni gubitak podataka. Softverski deo je dosta lakši jer softver nakon pokretanja traži podatke i u zavisnosti od njihovog stanja na medijumu uspeva da ih rekonstruiše i povrati.

Dakle, cilj postupanja forenzičara je naime da sakupi sve relevantne elektronske dokaze i analizira ih. Nakon toga, štampa relevantne dokaze ako nisu obimni, sastavlja izveštaj o rezultatima analize, rekonstruiše događaj/ napad i obezbeđuje ekspertsko mišljenje/ veštačenje.[39] Neophodno je da pomenute tehnike i alate kompjuterske forenzike primenjuje stručnjak iz te oblasti kako ne bi došlo do oštećenja dokaza i smanjenja njihove upotrebljivosti na sudu, s obzirom da pronalaženje skrivenih i obrisanih podataka ili snimanje stanja memorije neće mnogo značiti ukoliko ne postoji sposobnost stručnjaka koji sprovodi te tehnike da na pravilan način interpretira rezultate do kojih je došao.

6. Rukovanje elektronskim zapisima

Kao što smo utvrdili, da bi se uopšte došlo do elektronskih zapisa koji bi se mogli koristiti u krivičnom postupku, sprovodi se « kompjuterski uviđaj » koji obuhvata postupak dolaženja do podataka i utvrđivanja vremena kada su bili uneti, modifikovani, distribuirani, korišćeni, uskladišteni, sklonjeni, kao i utvrđivanje vremena kada su datoteke bile kreirane, postavljene, popunjavane sadržajem, modifikovane ili kada im se pristupilo.[40]

---

[37] M. Mayers, Computer forensics: the need for standardization and certification, - International journal of digital evidence, fall 2004, vol. 3, issue 2, preuzeto sa internet stranice www.ijde.org

[38] Priručnik Nacionalnog Instituta pravde SAD: Forenčizki pregled digitalnih dokaza: vodič za organe gonjenja (Forensic Examination of Digital Evidence: A Guide for Law Enforcement) , preuzeto sa internet stranice:http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[39] Op.cit.

[40] Problem nastaje kada su u pitanju računari koji su umreženi i kada postoji veći broj lica koji mogu biti potencijalni počinioci krivičnih dela. Pri utvrđivanju ovih vrem-

Kada govorimo o rukovanju elektronskim zapisima, treba napomenuti da se podaci u elektronskim zapisima u vidu datoteka i direktorijuma najpre prikupljaju, nakon čega se pristupa ispitivanju istih.

Prilikom rukovanja elektronskim zapisima ni u kom slučaju ne sme se ništa menjati u računarima sa kojih se u procesu prikupljanja elektronskih zapisa sakupljaju digitalni podaci, a naročito treba voditi računa o sledećem:[41]

- pre, u toku i posle uzimanja digitalnih zapisa ni jedna preduzeta akcija ne sme da dovede do izmene digitalnog zapisa;[42]
- radnje preduzete da bi se obezbedili i prikupili digitalni zapisi ne bi trebalo da utiču na integritet zapisa kao dokaza;[43]
- radnje preduzete da bi se obezbedili i prikupili digitalni zapisi, kao i samo ispitivanje zapisa treba da obavljaju lica obučena za tu svrhu, koja su pri tom odgovorna za sve aktivnosti u odnosu na digitalne podatke;
- aktivnosti koje se odnose na prikupljanje, ispitivanje, pohranjivanje, prenos elektronskih zapisa treba da su dokumentovane i sačuvane, da ih je moguće kontrolisati i da budu raspoložive za stavljanje na uvid, bilo kojoj zainteresovanoj strani u postupku;
- originalni zapis treba biti sačuvan u originalnom ili što približnijem stanju kao u momentu pronalaženja. Ako je uopšte moguće, potrebno je napraviti preciznu kopiju (sliku) originala, da bi se na kopiji vršilo ispitivanje i na taj način sačuvao i zaštitio integritet originala;
- kopije podataka napravljenih u svrhu ispitivanja trebaju biti kreirane na forenzički sterilnom medijumu;[44]
- svi zapisi moraju biti propisno označeni i dokumentovani.[45]

---

enskih serija i ograničenja razvijeni su posebni alati čije korišćenje je od izuzetne važnosti za obezbeđivanje relevantnih podataka.

[41] D. Pettinari, Handling Digital Evidence from Seizure to Court Presentation, IOCE conference 2000, preuzeto sa internet stranice http://www.ioce.org

[42] Očuvanje integriteta podrazumeva da se prilikom sveukupnog rukovanja sa zapisima (a naročito prilikom u toku procesa prikupljanja i analize) mora voditi računa da ni jedan mogući zapis ne bude oštećen, uništen ili kompromitovani na neki način, da se ni jedan mogući kompjuterski virus ne sme ubaciti u ispitivani računar, da se sa izuzetim i potencijalno relevantnim zapisima propisno manipuliše i da se isti štite od eventualnih oštećenja.

[43] Prikupljeni elektronski zapisi moraju se čuvati od štetnih uticaja koji mogu dovesti do oštećenja: toplote, hladnoće, vode, dejstva magneta, itd. Takođe, svaku datoteku trebalo bi „bekapovati" i uskladištiti sa digitalnim potpisom.

[44] Sterilan je onaj medijum ili disk na kome prethodno nije bilo podataka; trebalo bi da bude potpuno čist, bez virusa i oštećenja.

6.1. Prikupljanje elektronskih zapisa

Prikupljanje elektronskih dokaza podrazumeva traženje, prepoznavanje i dokumentovanje elektronskih zapisa.[46] Elektronski zapisi su, po prirodi, krhki i mogu se veoma lako izmneniti, oštetiti ili uništiti ako se njima nepažljivo/ nepropisno rukuje. Iz tih razloga se preduzimaju posebne mere predostrožnosti da bi se elektronski zapisi sačuvali, jer bi ih propusti u toku prikupljanja mogli učiniti neupotrebljivim, a propusti u toku analize prikupljenih zapisa bi mogli navesti na pogrešan zaključak.

U fazi prikupljanja dokaza preduzimaju se sledeći koraci: isključuje se računar; stvara se fizička slika (kopija) hard diska i svih drugih medijuma,[47] ili se privremeno oduzima računarski sistem; označavaju se i pakuju sve komponente računarskog sistema; računarski sistem se prenosi u forenzičku laboratoriju za analizu.[48] U svakom slučaju pristupa se pretraživanju računara/ računarskog sistema na licu mesta, ali je nekada neophodno oduzimanje i odnošenje računara i prateće opreme.[49] Pronađene spoljne nosioce podataka treba koristiti tako što se originali oduzimaju kao dokazni materijal, a prave se kopije istih.[50]

Sa kompjuterskom opremom može se postupati na više načina: pretražiti računar i izraditi fizičku kopiju pojedinačnih datoteka; pretražiti računar i izraditi elektronsku kopiju pojedinačnih datoteka; formirati "mirror-image"[51] elektronske kopije celog uređaja na licu mesta, da bi se isti

---

[45] Nabrojani su principi Međunarodne organizacije za kompjuterske dokaze, preuzeti sa internet stranice : http://www.ioce.org

[46] B. Banović, Kompjuterski kriminalitet i zaštita ličnosti, Bezbednost, 2003. god, 1/ 03, str. 37.

[47] Stvara se elektronska kopija, tzv. «Fizička ili mirror kopija niza bitova» primenom odgovarajućih forenzičkih softverskih alata - hard disk se „ klonira"

[48] Priručnik Nacionalnog Instituta pravde SAD: Forenčizki pregled digitalnih dokaza: vodič za organe gonjenja (Forensic Examination of Digital Evidence: A Guide for Law Enforcement), preuzeto sa internet stranice:http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

[49] Sakupiće se i analiziraće se svi flopi diskovi otkriveni na lokaciji osumnjičenog računara. Isto tako, sakupiće se svi štampani materijali, rukopisi, zabeleške, trake, CD ROM - ovi ili drugi materijali, koji mogu ukazati na rasvetljavanju spornog događaja.

[50] Najčešće se prave dve kopije: jedna koja bi služila kao rezervni dokaz, dok bi se druga koristila za neophodne analize.

[51] Formira se elektronska kopija, klon, celog elektronskog uređaja, da bi se isti pregledao van lica mesta.

pregledao van lica mesta; oduzeti celokupnu opremu, odneti iz prostorije i pregledati sadržaj računara i opreme van lica mesta.[52]

Razlog zbog kog se pristupa kopiranju, tj. kloniranju datoteka ili celog računarskog sistema jeste priroda datoteka, tj. elektronskih zapisa – njihova latentnost i osetljivost. Podaci mogu se veoma lako izmeniti, uništiti ili na drugi način učiniti neupotrebljivim, pa je nužno načiniti kopiju da bi se izbeglo postupanje na originalu. Kada je reč o elektronskim zapisima, tehnologija je omogućila kreiranje kopija koje su u svakom smislu verne originalu. U ovom slučaju prezentovanje kopije je u principu prihvatljivo uprkos postojanju i dostupnosti originala. U praksi bi se čak možda i preferiralo prezentovanje kopija zbog otklanjanja svake sumnje u mogućnost izmene originala, a s tim u vezi bi i štampani oblik digitalnog dokumenta mogao smatrati validnim, osim u slučaju u kome on ne može prikazati sve informacije neophodne za postupak.

Dakle, da bi se elektronski zapisi – datoteke i direktorijumi - uopšte mogli smatrati dokazom, najpre iste treba prikupiti, pa potom ispitivati. Kad god je moguće, ispitivanje ne bi trebalo da se sprovodi na originalnoj datoteci. Najbolje je ispitivanje sprovoditi na kopiji originalne datoteke, a original bi trebalo da bude stečen na način koji štiti i čuva integritet elektronskog zapisa. Ukoliko, forenzičar ne poseduje kopiju datoteke, tj. elektronskog zapisa, onda on ne može izdvojiti podatak iz datoteke niti izvesti potrebne zaključke, jer bi se u slučaju da se analizi i tumačenju zapisa pristupi na originalu datoteke, moglo posumnjati u njihov integritet.[53]

Dakle, kada se informacije u vidu elektronskih zapisa prikupe ili pohrane, pristupa se ispitivanju istih.

6.2. Ispitivanje elektronskih zapisa

Cilj ove faze rukovanja sa izdvojenim elektronskim zapisima jeste da se isti izdvoje i analiziraju, te da se identifikuju digitalni dokazi i rekonstruiše događaj. Zapravo, ispitivanje se svodi na analizu izdvojenih elektronskih zapisa, pri čemu se izdvajanje odnosi na oporavak (recovering) datoteka i podataka iz medijuma, a analiza na iznalaženje mogućeg značaja i značenja tih datoteka i podataka, te njihovo dovođenje u logičnu i korisnu vezu.

---

[52] Ukoliko je hardver sam po sebi dokaz da je izvršeno krivično delo, isti se oduzima i pregleda van lica mesta. Ukoliko je hardver samo nosilac datoteka koje predstavljaju dokaze, pravi se kopija hard diska i analize se vrše na toj kopiji.

[53] Digitalni istraživanja uglavnom se oslanjaju na podatke koji se nalaze na hard disku, dok u slučaju istraživanja upada u računar, dodatne izvore informacija predstavljaju podaci koji su prikupljeni iz mrežnog saobraćaja, kao i nestabilne memorije.

Treba još jednom napomenuti da se prilikom ispitivanja prikupljenih elektronskih zapisa koristi skup forenzičkih tehnika i alata[54] i primenjuju se stroge naučno izvedene metode, a kao što smo prikazali, primat u procesu rukovanja elektronskim zapisima imaju naučna saznanja i dostignuća kompjuterske/ digitalne forenzike.

Prilikom ispitivanja bi bilo korisno postupati u sledećim koracima:

1. priprema;
2. izdvajanje datoteka i podataka (elektronskih zapisa);
3. analiza izdvojenih datoteka i podataka (elektronskih zapisa);
4. donošenje zaključka.

1. korak- priprema: Pre nego što se pristupi analizi prikupljenih podataka, trebalo bi pripremiti radni direktorijum na medijumu na koji će se izdvojiti datoteke i podaci.

2. korak - izdvajanje datoteka i podataka: Postoje dva vida izdvajanja datoteka i podataka: fizičko i logičko izdvajanje (ekstrakcija). Pod fizičkom ekstrakcijom podrazumeva se identifikacija i oporavak svih podataka na hard disku, bez obzira na sistem datoteka, a metodi se mogu odnositi na pretragu ključnih reči, pretragu nekorišćenog prostora na hard disku, i slično.[55] Logička ekstrakcija podrazumeva identifikaciju i oporavak datoteka i podataka na osnovu instaliranog operativnog sistema, sistema datoteka i / ili programa. Ova faza izdvajanja podataka i datoteka iz hard diska zasnovana je na sistemu datoteka koji je prisutan na disku, a može da obuhvati i aktivne datoteke, ali i izbrisane datoteke, zaštićene datoteke, kao i prostor neraspoređenih datoteka.

Na osnovu ovakvog izdvajanja datoteke mogu se utvrditi sledeći podaci: struktura direktorijuma, atributi datoteke, ime datoteke, datum i vreme kreiranja/ izmena datoteke, veličina datoteke, lokacija datoteke. Takođe, može se postići sledeće: izdvajanje datoteka na osnovu imena i ekstenzije datoteka, zaglavlja datoteke, sadržaja datoteke i mesta na hard disku; izdvajanje nedodeljenog prostora; povraćaj obrisanih datoteka; izdvajanje datoteka koje su zaštićene lozinkom, šifrovane ili kompresovane.

3. korak - analiza izdvojenih datoteka i podataka: Analiza podataka je proces tumačenja izdvojenih podataka sa ciljem da se utvrdi njihov značaj za konkretan slučaj. Primera radi, predmet analize mogu biti sledeći podaci: vremenski okvir, sakrivene datoteke, programi i datoteke.[56]

---

[54] O. Kerr, Digital evidence and new criminal procedure, Columbia law review, 2005, Vol.105, No.1 , str. 292.

[55] R. Morris, Evidence, International review of law computers& technology, 1998, Vol. 12, No. 2, str. 281.

[56] Op.cit, stp. 285.

Analiza vremenskog okvira. Određivanje vremena nekog događaja u računarskom sistemu može biti od koristi za utvrđivanje ko se od korisnika u datom trenutku služio računarom.[57]

Analiza sakrivenih datoteka. Datoteke mogu biti sakrivene u računarskom sistemu. Analiza sakrivenih datoteka može biti korisna u otkrivanju i «oporavljanju» (recovering) takvih datoteka. Metode koje se mogu koristiti su: povezivanje zaglavlja datoteke sa odgovarajućim ekstenzijama, da bi se identifikovali pogrešni spojevi čije prisustvo može ukazati da je korisnik namerno sakrio podatke; pristup svim datotekama koje su zaštićene lozinkom, šifrovane ili kompresovane, a što može da ukaže na pokušaj da se datoteke prikriju od pristupa neovlašćenog korisnika;[58] pristup u područje zaštićeno za korisnika-domaćina (host-protected area HPA[59]) - samo postojanje ovakvog prostora koje je korisnik kreirao, kao i prisustvo podataka u istom, može da ukaže na pokušaj da se prikriju određeni podaci; i slično.

*Analiza programa i datoteka***.** Mnogi od identifikovanih programa i datoteka mogu da sadrže informacije relevantne za uviđaj i daju uvid u sposobnost sistema i znanja samog korisnika.[60] Rezultati ove analize mogu da ukažu na to koje dodatne korake treba preduzeti u daljem postupku izdvajanja i analize podataka[61].

4. korak - donošenje zaključaka: Nakon analize koja podrazumeva utvrđivanje dokazne vrednosti pojedinih elektronskih zapisa za konkretan slučaj,[62] pristupa se izvođenju zaključaka. Pojedinačni rezultati bilo kog od ovih koraka ne mogu biti dovoljni da bi se izveo tačan zaključak. Tek kada se rezultati pojedinih faza posmatraju kao celina, može se sklopiti

---

[57] Dve metode koje se mogu koristiti su: 1) pregled oznake vremena i datuma u sistemu datoteka (ovakvom analizom može se utvrditi npr. trenutak kada je sadržaj datoteka poslednji put izmenjen); 2) pregled prijavljivanja u sistem i aplikaciju (ispitivanje sistema sigurnosti može da ukaže na evidencije kada je i koji korisnik računara koristio kombinaciju korisničko ime/ lozinka da bi se prijavio u sistem).

[58] Lozinka sama po sebi može biti relevantna kao i sadržaj datoteke.

[59] Host-protected area predstavlja skriveni zaštićeni prostor, odnosno oblast hard diska koja normalno nije vidljiva u operativnom sistemu

[60] Morris R., Evidence, International review of law computers& technology, 1998, Vol. 12, No. 2, stp. 293.

[61] Neki od primera analize programa i datoteka su: pregled imena datoteke, ispitivanje sadržaja datoteke, utvrđivanje broja i tipa operativnog sistema; povezivanje datoteke sa instaliranom aplikacijom; ispitivanje veza između datoteka (npr. e-mail datoteke i priloga e-pošte), prepoznavanje nepoznatih tipova datoteka da se utvrdi njihova vrednost za istragu, ispitivanje korisnikovih konfiguracionih podešavanja itd.

[62] B. Banović, Kompjuterski kriminalitet i zaštita ličnosti, Bezbednost, 2003. god, 1/03, str. 37.

kompletna slika stvari, rekonstruisati događaj i izvesti pravi zaključak. Na taj način elektronski zapisi koji su bili izdvojeni i analizirani, mogu poslužiti kao dokaz i biti kao takvi prezentovani u krivičnom postupku.

7. Zaključna razmatranja

Razvoj informacionih tehnologija, neminovno otvara prostor i skoro neverovatne mogućnosti za zloupotrebe u virtuelnom prostoru. Sve veći broj kriminalaca koristi računare i računarske mreže, te ukoliko organi otkrivanja i gonjenja ne budu u dogledno vreme stručno osposobljeni u vezi sa tehničkim i pravnim pitanjima oko elektronskih zapisa kao svojevrsnih digitalnih dokaza, rezultat bi mogao biti da se isti previde, te da se prikupe na neispravan ili analiziraju na neodgovarajući način, čime bi se onemogućilo njihovo korišćenje u krivičnom postupku.

Da bi se u takvom virtuelnom okruženju otkrilo, razjasnilo i dokazalo određeno krivično delo, neophodno je poznavanje najnovijih dostignuća informacione tehnologije, jer samo primena istih u krivičnom postupku može organe gonjenja učiniti ravnopravnim sa počiniocima krivičnih dela. Stoga bi prvi korak morao biti razumevanje prirode elektronskih zapisa u računaru i načina na koji se mogu upotrebiti da bi se dokazalo izvršenje krivičnih dela u vezi sa računarima i računarskim sistemima/ mrežama.

Milana Pisarić, Junior Assistant
Novi Sad School of Law

Electronic Records As Digital Evidence

Abstract

Fast development of computer and computer networks has created and is creating a whole new world for us. Computer networks enable easier and faster way of communication, faster transfer of information and business activities, accompanied by the enormous flow of digital data in electronic form (computer) records. These data may appear in the form of text, images and voice, and can be displayed on a computer screen or printed. Data as electronic records which are stored in computer in form of files and folders, or transmitted via computer - can be crucial evidence in detecting and proving the various misuses of information technology.

Key words: digital data, data as electronic records, misuses of information technology, digital forensic, computer crime, detecting and proving of computer crimes