STRUČNI ČLANAK

UDK: 343.98
343.533:004.056
Primljeno: prosinac 2010.

NIKOLA PROTRKA*

Računalni podaci kao elektronički (digitalni) dokazi

Sažetak

U radu se objašnjava što su to elektronički dokazi, te koja je njihova važnost u kaznenom postupku. Navode se neke potencijalne vrste elektroničkih dokaza, te gdje se oni mogu sve nalaziti u digitalnom obliku. Kako napreduje računalna tehnologija, tako napreduju i tehnike pohranjivanja računalnih podataka, koji se u današnje vrijeme nalaze svuda oko nas. Prikupljanje takvih podataka, koji se mogu kasnije koristiti kao dokazi u postupku, mora se obaviti profesionalno i stručno.

Potpisivanjem Konvencije o kibernetičkom kriminalu, Republika Hrvatska preuzela je obveze za kaznena djela iz područja računalnog kriminala, a samim time i nekoliko novih zakonskih rješenja u području elektroničkih (digitalnih) dokaza.

U policijskoj se praksi sve više djelatnika susreće s elektroničkim dokazima, jer su prisutni u sve više kaznenih djela. Da bi se što bolje prikupili i analizirali takvi dokazi, policijski službenici morali bi posjedovati osnovna znanja o pojmovima i načinu rada samog računala, računalne opreme ili drugog uređaja koji sadrži elektroničke dokaze, te bi morali biti upoznati s pravilnim načinom izuzimanja i osiguravanja takvih dokaza.

Ključne riječi: *elektronički dokaz, računalni kriminal, kibernetički kriminal, forenzika računala, pretraga računala.*

1. RAČUNALNI KRIMINALITET I ELEKTRONIČKI DOKAZI

Analiza podataka i forenzika ulazna su vrata u polje računalnog kriminaliteta. Kao i u stvarnome svijetu, dete ktivi i forenzičari otkrivaju nove slučajeve računalnog kriminali-

* Nikola Protrka, univ. spec. inf., Odjel za policijsku obuku, Policijska akademija MUP-a RH, Zagreb.

teta skoro svaki dan. Korištenje ICT (eng. *Information and communication technologies*) tehnologija u kriminalne svrhe zahtijeva posebne metodike za vođenje kriminalističkog istraživanja. Elektronički dokazi su osjetljivi, lako se brišu i mijenjaju a time i kompromitiraju. Specijalni forenzični alati omogućavaju povrat i analizu i obrisanih, skrivenih i privremenih datoteka koje u svakodnevnom normalnom radu nisu vidljive.

S obzirom na to da se računalo može koristiti kao oruđe za počinjenje zločina, ono može, odnosno mora sadržavati dokaze koji se odnose na bilo koji zločin, poput ubojstva ili silovanja. Nije nevažno napomenuti da većina eksperata pohranjuje svoje podatke na računala. Bilo koje kriminalističko istraživanje može koristiti računala ili internet, i svi koji sudjeluju u istraživanju mogu izvući koristi iz poznavanja upotrebe te tehnologije.

Policijski službenik koji skuplja dokaze s računala ili računalne mreže, mora znati pravila postupanja glede prikupljanja tih podataka, jer ako on skupi te podatke nezakonito, ti se podaci neće moći koristiti u sudskom postupku. Pojam *digitalni dokazi* koristi se u američkom zakonodavstvu i označava bilo koji računalni podatak koji može potvrditi da je počinjeno kazneno djelo, ili koji može ukazati na povezanost između zločina i žrtve, ili zločina i njegova počinitelja.

Elektronički dokazi su vrlo važni, jer predstavljaju kombinaciju različitih informacija poput teksta, slike, audiosnimke i videosnimke. Ponekad informacija koja je pohranjena na računalu može biti jedini trag koji će kriminalističko istraživanje dovesti na pravi put. Postoji cijeli niz elektroničkih dokaza koji nas okružuju u svakodnevnom životu, a kojih smo skoro u potpunosti nesvjesni. Tvrdi disk može sadržavati cijelu biblioteku informacija, digitalna kamera u svojoj memoriji može pohraniti tisuće fotografija, a računalna mreža može sadržavati još više informacija o osobama i njihovu ponašanju. Brojevi bankovnih računa, novčane transakcije, povjerljivi dokumenti i drugi različiti podaci putuju oko nas kroz zrak ili putem žičnih vodova, a svaki od njih predstavlja potencijalni izvor elektroničkog dokaza. Forenzika osigurava načela i tehnike koje omogućuju kriminalističko istraživanje i progon počinitelja računalnog kriminaliteta. Općenito gledajući, forenzika je primjena pravnih znanosti i drugih znanstvenih procesa i tehnika koje se mogu iskoristiti u identifikaciji, povratku, rekonstrukciji ili analizi dokaza tijekom kriminalističke istrage. Forenzičari pokušavaju uz pomoć elektroničkih dokaza rekonstruirati događaj te ga približiti i na taj način pojasniti istražiteljima[1].

Načelom "ledenog brijega" samo mali postotak elektroničkih dokaza moguće je otkriti "klasičnim alatima" kao što je Windows Explorer (alat za rad s datotekama u operacijskom sustavu Windows). Ostatak elektroničkih dokaza moguće je otkriti samo posebnim alatima (bilo komercijalnim bilo *freeware* /eng. *Freeware* – besplatni alati/).

Ustrojstvom MUP-a RH računalni kriminalitet spada pod nadležnost Odjela gospodarskog kriminaliteta i korupcije pri Upravi kriminalističke policije Ravnateljstva policije, te pod Odjele gospodarskog kriminaliteta policijskih uprava. U doticaju s elektroničkim dokazima su gotovo svi policijski službenici koji se nađu u kriminalističkom istraživanju, kako u navedenim odjelima, tako i u drugim odjelima i policijskim postajama.

---

[1] CARNet CERT i LS&S, Osnove računalne forenzičke analize, 2006., *http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2006-11-174.pdf* - 8. 2. 2008.

2. POTENCIJALNI ELEKTRONIČKI DOKAZI

Elektronički su dokazi jedna vrsta materijalnih dokaza, bez obzira na činjenicu što ih je teže evidentirati. Oni predstavljaju spoj magnetskog polja i elektronskih tehnika koji se skupljaju i analiziraju uz pomoć specijalnih tehnika i alata. Pred materijalnim dokazima elektronički dokazi imaju nekoliko glavnih prednosti. Od elektroničkih je dokaza moguće načiniti točnu kopiju (sliku) koja se naknadno može istraživati kao da se radi o originalu, dok je kod materijalnih dokaza to gotovo nemoguće. Prilikom ispitivanja kopije, a ne originala, izbjegavaju se oštećenja koja bi mogla nastati na originalu prilikom istraživanja. Pomoću pravilnih alata moguće je vrlo lako odrediti je li elektronički dokaz modificiran ili uništen, jednostavno ga uspoređujući s originalom. Elektroničke je dokaze vrlo teško uništiti. Čak i onda kada su "obrisani", elektronički se dokazi mogu povratiti s računalnog diska ili nekog drugog medija za pohranu podataka.

Elektroničke je dokaze jednostavno pohraniti, a zbog lakoće izrada kopija gotovo ih je nemoguće uništiti ili izgubiti. Zbog toga što se elektroničkim dokazima može lako manipulirati i prenositi ih, istražitelji koji se bave računalnim kriminalom nailaze na nove izazove u radu s ovakvom vrstom dokaza. Ti dokazi nalaze se svugdje oko nas. Računalne mreže u svom svakodnevnom radu uključuju cijeli niz procesa od telefonskih poziva, prijma i slanja elektroničke pošte, plaćanja računa i drugih pogodnosti, a što u biti predstavlja elektroničke dokaze. Sve te pogodnosti danas su dostupne svakom čovjeku iz sigurnosti i udobnosti njegova doma. Međutim, računalne mreže sa sobom donose i određeni rizik. Računalne mreže su široko uključene u kriminalni milje, koji uključuje dječju pornografiju, prijetnje, špijunažu, sabotaže, prijevare, uznemiravanje privatnosti itd.

Kriminalne aktivnosti potpomognute novim tehnologijama razvijaju se takvom brzinom da je istražiteljima skoro nemoguće držati korak i pratiti te kriminalne aktivnosti.

Adresari – *Address Books*	Dijelovi datoteka
Elektronička pošta – *e-mail*	Datoteke za pohranu – *Backup files*
Audio/Videodatoteke	Log datoteke
Slikovne/Grafičke datoteke	Datoteke za konfiguraciju
Kalendari	Ispisne datoteke za pisače – *Printer spool*
Baze podataka – *Database files*	Kolačići – *Cookies*
Tablične datoteke	Privremene datoteke – *Swap files*
Kompresirane datoteke – *.zip, *.rar itd.	Sistemske datoteke – *System files*
Datoteke s pogrešnim nazivom	Povijest – *History files*
Enkriptirane datoteke	Privremene datoteke – *Temporary files*
Skrivene datoteke	Datoteke dokumenata
Datoteke zaštićene lozinkom	Internet favoriti – *bookmarks/favorites*

Tabela 1: Potencijalni elektronički dokazi (Izvor: vlastita izrada)

3. SVRHA I VRIJEDNOST ANALIZE ELEKTRONIČKIH DOKAZA

Analiza elektroničkih dokaza je proces koji uključuje analizu i korelaciju više vrsta podataka na različitim razinama. Svrha i vrijednost analize je ta da proučimo različite tipove podataka i zatim ih pretvorimo u korisne informacije. Kod prikupljanja elektroničkih dokaza potrebno je odrediti računala ili medije koji su predmet istraživanja, sačuvati

originalne medije i spriječiti bilo kakve izmjene sadržaja medija; ako je računalo upaljeno, preuzeti sadržaj radne memorije (RAM – *Random Access Memory*), ugasiti računalo bilo redovnim putem bilo isključivanjem napajanja, napraviti kopiju svih bitnih medija, te obaviti forenzičnu analizu na kopijama – slikama medija.

Elektronički dokazi najvažniji su čimbenik onoga što danas poznajemo pod pojmom *cybercrime* ili kibernetički kriminal, a to je računalni kriminal. Ovaj se pojam koristi za označavanje kaznenog djela u čije je počinjenje uključeno računalo, računalna mreža, uključujući i kaznena djela koja nisu u potpunosti počinjena na računalu. Ovaj se pojam koristi i za opise situacije u kojoj računalna mreža nije korištena u počinjenju kriminala, ali sadržava elektroničke dokaze povezane s kriminalom. Iako nema direktan učinak na slučaj, računalo sadrži elektronički dokaz koji je vrlo važan za istraživanje. Ako je kriminalno djelo počinjeno u stvarnom fizičkom svijetu i ako postoji računalo s mrežnim pristupom na mjestu počinjenja djela, istražitelji će učiniti pretraživanje računala i računalne mreže u potrazi za elektroničkim dokazima koji im mogu poslužiti u istraživanju. Slično tomu, ako je kriminalni čin zabilježen na računalu ili računalnoj mreži, kriminalistički istražitelji mogu utvrditi mjesto gdje se nalazi to računalo, te na taj način pokušati locirati mjesto počinjenja djela.

Nepohranjivanjem elektroničkih dokaza istražitelji se dovode u opasnost od gubitka tih dokaza te nemogućnosti nastavka daljnjeg procesa istraživanja.

Čak i ako istražitelj nije odgovoran za prikupljanje elektroničkih dokaza s računalne mreže, u određenom slučaju, on mora posjedovati osnovna znanja o elektroničkim dokazima.

Kako će se informatizacija društva povećavati, bit će i više računalnog kriminala.[2] Taj će kriminal posebno rasti, ako počinitelji otkriju kako su policijski službenici, eksperti koji se bave računalnom sigurnošću i druge osobe uključene u prevenciju i represiju, slabo opremljeni za suprotstavljanje ovoj vrsti kriminala, te kako neadekvatno koriste elektroničke dokaze. Zbog toga je važno da djelatnici policije znaju "rukovati" elektroničkim dokazima, da ih znaju koristiti kao smjernice u istraživanju, a posebno moraju voditi brigu o tome kada i za što će pozvati u pomoć računalne stručnjake.

Istraživanje ovisi ponajprije o poznatim činjenicama koje istražitelji imaju o djelu. Ako je računalo rezultat ili posljedica računalnog kriminala, istražitelji trebaju fokusirati hardver (eng. *Hardware* – strojna podrška), a ako djelo uključuje protuzakonite informa-

[2] Jedan od najpoznatijih slučajeva računalnog kriminala veže se uz ime Albert Gonzalez, koji je jedan od najozloglašenijih računalnih kriminalaca, te je u ožujku 2010. godine osuđen na 20 godina zatvora nakon što se izjasnio krivim za pomaganje u organiziranju globalne mreže putem koje su ukradeni deseci milijuna brojeva kreditnih kartica, što je pravi primjer elektroničkih dokaza. Ovo je najveća zatvorska kazna do sada izrečena za računalni kriminal na američkim sudovima, a Gonzalez je mogao i gore proći u slučaju da nije priznao krivicu. Naime, Gonzalezu je prijetila 25-godišnja kazna zatvora, no u nagodbi sa sucem kao olakotne okolnosti uzete su činjenice kako je od djetinjstva ovisnik o računalima, te je godinama bio pod utjecajem alkohola i ilegalnih droga, a i bolovao je od Aspergerovog poremećaja (oblika autizma). Prema njegovim riječima kriminalne aktivnosti izmaknule su kontroli zbog nemogućnosti da kontrolira znatiželju i ovisnost. No tužitelj je inzistirao na strogoj kazni navodeći kako će ona poslati jasnu poruku potencijalnim kriminalcima kako Vlada "uzima" vrlo ozbiljno računalne zločine, te da će isti biti uhvaćeni i vrlo strogo kažnjeni.

cije i podatke, istražitelji trebaju potražiti bilo što štô je povezano s tim informacijama i podacima uključujući tu i medije, odnosno softver (eng. *Software* – programska podrška), na kojima se ti podaci i informacije nalaze.

Ako su informacije i podaci koji se nalaze na računalu pravno relevantni, a istražitelji znaju što traže, bit će moguće u vrlo kratkom roku prikupiti potrebne dokaze; s druge strane, ako istražitelji ne znaju što traže, potrebno je proširiti opseg istraživanja i u nj pritom uključiti svu računalnu opremu kako bi se prikupili i istražili materijali koji bi mogli poslužiti kao dokaz. Bez obzira na sve, istražitelji moraju biti u stanju dokazati autentičnost i integritet prikupljenih dokaza.

To konkretno znači da istražitelj mora biti u mogućnosti dokazati da je dokaz ono što on kaže da jest, da dolazi s lokacije za koju on kaže da dolazi i da dokaz nije bio mijenjan ili oštećen na bilo koji način. Što se elektroničkih dokaza tiče, ovo može biti vrlo teško, jer su elektronički dokazi lako promjenjivi. Jednostavno uključivanje i isključivanje računala može u potpunosti uništiti dokaze. Zbog toga je važno biti promišljen, dobro organiziran i upoznat s tehnologijom koja se istražuje.

4. PRAVNA UREĐENOST GLEDE ELEKTRONIČKIH DOKAZA

Izmjenama Kaznenog zakona i njegovim usuglašavanjem s europskom Konvencijom o kibernetičkom kriminalitetu, Hrvatska napokon dobiva nova, kvalitetna, premda još uvijek ne i potpuna zakonska rješenja u ovom području.[3]

Najvažnija novina u Kaznenom zakonu je njegovo usuglašavanje s obavezama preuzetim potpisivanjem *Konvencije o kibernetičkom kriminalitetu* Vijeća Europe (NN-MU 9/02., 4/04.). Radi se o do sada najvećem, najopsežnijem ali i najkvalitetnijem europskom dokumentu o takvoj vrsti kriminaliteta, koju su potpisale i neke neeuropske informatičke velesile, ponajprije Sjedinjene Američke Države, Kanada i Japan.

Konvencija je svečano potpisana 23. studenog 2001. u Budimpešti, te je predstavljena kao međunarodno pravni instrument kojim se po prvi put reguliraju problemi vezani uz korištenje i prijenos informacija i podataka preko informatičkih i telekomunikacijskih sustava. Upravo se zato i zove Konvencija o kibernetičkom, a ne računalnom kriminalu.

Naime, sve brže integriranje informatičke i telekomunikacijske tehnologije i njihova međusobna ovisnost dovode i do povezanosti njihove zlouporabe, pa pojam "računalni kriminalitet" postaje preuzak i zamjenjuje se širim pojmom "kibernetičkog kriminaliteta". I premda je pojam prihvaćen, još uvijek ne postoji njegova općeprihvaćena definicija, unatoč svim nastojanjima da se ona, kao i sadržaj i opseg pojma – odrede. Najprihvaćenija definicija pak kaže da kibernetički kriminal obuhvaća sva kaznena djela počinjena unutar kibernetičkog prostora, popularnog *cyberspacea*, uz pomoć informatičke i telekomunikacijske tehnologije ili na samoj informatičkoj i telekomunikacijskoj tehnologiji, koje čini njegovu infrastrukturu.

Temeljnu infrastrukturu *cyberspacea* čini internet, koji svojom globalnošću, otvorenošću te dostupnošću postaje izvorom sve većih i opasnijih zlouporaba, a borba protiv

[3] Zakon o izmjenama i dopunama Kaznenog zakona. (NN 105/04.)

njih zahtijeva čvrstu međunarodnu suradnju. Kako takva suradnja ili nije postojala ili je bila neorganizirana i pojedinačna, Vijeće Europe je 1997. godine osnovalo posebnu komisiju, *Committee of Experts on Crime in Cyber Space*, čiji je zadatak bio utvrditi stanje i započeti rad na međunarodnim instrumentima za borbu protiv kriminala na internetu[4].

Nakon tri godine rada u tajnosti, Nacrt konvencije prvi put je predstavljen javnosti krajem 2000. godine. Njime je predviđeno da će stranke usvojiti zakonska i druga rješenja nužna da se u domaćem zakonodavstvu mogu progoniti počinitelji kaznenih djela protiv tajnosti, integriteta i dostupnosti računalnih podataka i sustava, kaznenih djela u vezi s računalom, u vezi sa sadržajem i u vezi s povredama autorskih i srodnih prava. Usvojeno je i rješavanje procesnih pitanja vezanih za pretragu i pribavljanje dokaza, ovlaštenja redarstvenih vlasti, nadležnost suda, izručenje počinitelja, uzajamnu suradnju te obaveze *internet providera* (davatelj usluge za pristup internetu).

Velika reforma domaćeg kaznenog zakonodavstva 1997. godine prvi put je u naše pravo uvela računalni kriminal, i to u članku 223. KZ-a, kazneno djelo Oštećenje i uporaba tuđih podataka. Premda je takvo zakonsko rješenje pokazalo da Hrvatska razumije probleme koje računalni kriminal donosi, teško se oteti dojmu da to rješenje nije bilo najsretnije. Prva zamjerka odnosila se na to da članak ne pravi razliku između zlouporaba i šteta počinjenih na privatnom računalu i računalu državne institucije ili poduzeća, a predviđene sankcije nisu bile razmjerne. Tako se, na primjer, počinitelja za nelegalno presnimavanje i prodaju softverskih CD medija (eng. *Compact Disk*) moglo kazniti novčano ili zatvorom do čak tri godine, dok bi ga se za provalu u tuđe računalo, tj. *hacking* kaznilo do šest mjeseci zatvora. Za oštećenje, izmjenu ili uništenje tuđih podataka ili računalnih programa zakonski maksimum mjere kazne zatvora je godinu dana. Jasna je nelogičnost i nerazmjernost ovih zakonskih rješenja. Unatoč tome, Republika Hrvatska izuzetno je uspješna u borbi protiv računalnog kriminaliteta, tako da nisu rijetke vijesti o razbijanju pedofilskih lanaca u kojima su naši stručnjaci imali veliku ulogu.

Republika Hrvatska je Konvenciju o kibernetičkom kriminalitetu potpisala 23. studenog 2001., a obveze koje su time preuzete odnosile su se na izmjenu Kaznenog zakona u koji je trebalo unijeti nova kaznena djela, i to: nezakoniti pristup, nezakonito presretanje, ometanje podataka, ometanje sustava, zloporaba naprava, računalno krivotvorenje, računalna prijevara, djela povezana uz dječju pornografiju i autorska prava, u slučajevima kada se računala i internet koriste za kažnjivu radnju.

Također je trebalo inkriminirati i djela koja uključuju pokušaj, pomaganje i poticanje na sve navedene kažnjive radnje. Izmjene koje su provedene ipak su samo djelomične, jer nisu inkriminirana sva Konvencijom predviđena djela.

Najveća intervencija bila je u spomenutom članku 223. KZ-a. Inkriminirane su nove zlouporabe, tako da su sada, uz "oštećenje, izmjenu, brisanje, uništenje ili druge načine zlouporabe podataka" koji ih čine neuporabljivima, kažnjivi i svi načini kojima se oni čine *nedostupnima*. Ta je novost posebno bitna u situacijama u kojima podaci nisu izbrisani ili oštećeni, ali im se ne može pristupiti zbog djelovanja malicioznih programa, prije svega *virusa*, *crva* i *trojanskih konja*. Time se napokon programima i podacima

[4] Jurman, D., Internet – Kibernetički kriminal, http://www.djurman.com/index.php - 10. 6. 2009.

osigurava jednaka zaštita kao i materijalnim predmetima. Naime, do sada se krađa računalnih podataka nije smatrala krađom, jer podaci nisu fizički ukradeni iz računala. Činjenicu da su prekopirani i dostupni drugima, zakon nije uvažavao.

Stavak 3. članka 223. KZ-a sankcionira *"onemogućavanje ili otežavanje rada ili korištenja"* računala ili računalne komunikacije, u prvome redu kao još jedan način kažnjavanja izrade i prijenosa malicioznih programa, ali i sve druge načine uskraćivanja usluga, tzv. *Denial of Service* (DoS) napada. Interpretacija ove norme daje i mogućnost kažnjavanja tzv. *spamminga* (eng. *Spam* – neželjena pošta), slanja velikog broja e-mail poruka s namjerom zagušenja servera ili računala primatelja, uslijed kojeg sustav prestaje raditi. Premda je namjera zakonodavca problem *spamminga* riješiti u posebnom zakonu, ne treba isključiti ni ovu mogućnost. Predviđena sankcija za sva navedena djela je novčana kazna ili kazna zatvora do tri godine. To nas dovodi do druge bitne novosti, povećanja sankcija za počinitelje, koje se sada i razlikuju ovisno o tome je li kazneno djelo počinjeno na privatnom računalu (novčana kazna ili kazna zatvora do tri godine) ili "računalu, sustavu, podatku ili programu tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnog javnog interesa", a u tom slučaju je sankcija isključivo kazna zatvora, od tri mjeseca do pet godina.

Daljnje novosti odnose se na kažnjavanje neovlaštene izrade i prodaje naprava i programa prilagođenih za činjenje kaznenih djela računalnog kriminaliteta, te kažnjavanje za pokušaj bilo kojeg od svih spomenutih kaznenih djela.

Jedno od rješenja ipak nije usuglašeno s Konvencijom, a radi se o kaznenom djelu neovlaštenog pristupa podacima ili programima, tzv. *hakingu*. Naime, Konvencija predviđa sankcioniranje samog neovlaštenog pristupa, dok naš Kazneni zakon kažnjava neovlašteni pristup *"unatoč zaštitnim mjerama"*. To rješenje može biti prilično zbunjujuće, jer u Hrvatskoj još uvijek ne postoji standardizirani način zaštite informacijskih sustava. Dok se to ne utvrdi, procjenu o postojanju zaštitnih mjera morat će dati sud u svakom posebnom slučaju, a hakerima ostaje izvrsna mogućnost obrane na sudu. Laički govoreći, svaki haker se može braniti da nisu postojale zaštitne mjere, jer da jesu, on ne bi mogao provaliti u sustav.

Osim nabrojanih intervencija u članku 223. KZ-a, uvedena su i dva potpuno nova kaznena djela, *računalno krivotvorenje* i *računalna prijevara*. Svrhu inkriminiranja računalnog krivotvorenja ne treba posebno objašnjavati.

U vrijeme ekspanzije i sve veće važnosti elektronskog poslovanja, pravo mora dati jednaku zaštitu elektroničkim dokumentima kao i onim papirnatima. Konkretno, bilo kakva manipulacija podacima i programima koji imaju vrijednost za pravne odnose, recimo ugovorima ili listama plaća u računalu, rezultirat će zatvorom, a ne lako i brzo stečenom protupravnom imovinskom koristi. Računalnu prijevaru pak krasi brojnost i raznolikost pojavnih oblika, a i ta mogućnost brze zarade dovodi do realne situacije da je takvih djela sve više. Kako se interpretacijom klasičnih djela krađe, prijevare, pronevjere i drugih ne može osigurati kvalitetna zaštita podataka ili informacija u računalu, bilo je jasno da će se to morati napraviti u novom, posebnom kaznenom djelu.

Tako će pribavljanje protupravne imovinske koristi izmjenom tuđih računalnih podataka ili programa u konačnici biti kažnjeno sa tri mjeseca do pet godina zatvora. Iako

Republika Hrvatska prati suvremene pravne trendove na području računalnog kriminala, brzina kojom se on razvija zahtijeva stalne prilagodbe kako bi zakon pratio promjene u virtualnom svijetu.

5. ELEKTRONIČKI DOKAZI I PRAKSA

Izrazito je važno da svi elektronički dokazi budu pribavljeni u skladu sa zakonskim pravilima, jer će ih u suprotnom istražni sudac izuzeti iz spisa kao nezakonite dokaze. Policijski istražitelji su prva "stručna linija" koja obrađuje ovakve slučajeve. Pomoć, tijekom obrade mjesta događaja i prikupljanja elektroničkih dokaza, mogu im pružiti stručne osobe. No, sud će vještačenje elektroničkih dokaza prepustiti sudskom vještaku iz područja informatike, elektronike, elektrotehnike ili komunikacija, koji može sudu na jednostavan način pojasniti kompliciranе tehničke sadržaje vezane uz počinjenje djela iz područja računalnog kriminaliteta[5].

Tijekom analize, sudski vještak u skladu s valjanim nalogom suda mora odgovoriti na postavljena pitanja, što nije uvijek jednostavno. Zapisi na optičkim medijima, ukoliko ih ima, prilično su nedvosmisleni. No, zapisi na tvrdim diskovima sadrže samo stanje u trenutku privremenog oduzimanja npr. od osumnjičenika, dok se pitanja suca često odnose na događaje iz prošlosti, na koja nije moguće odgovoriti jer o njima jednostavno više nema raspoloživih tragova.

Ponekad sudski vještak ne može doći do tragova koji su mu potrebni jer ih nema, nisu dostupni, skriveni su ili su uništeni. U tom slučaju, sudski vještak se ne smije upuštati u "špekulacije", mišljenje mora temeljiti na činjenicama, čak i kada je siguran u nešto o čemu nema konkretnih tragova.

Prema tome, sudski vještak mora se orijentirati primarno na činjenice iz svoje struke i treba postaviti jasne ograde prema iznošenju bilo kakvih činjenica ili stavova koji nisu dio njegova stručnog područja. Nadalje, tijekom kaznenog postupka, vještačenje sudskog vještaka može biti prihvaćeno kao meritorno pri donošenju odluke, ukoliko je napravljeno stručno, sudu prihvatljivo jasno, nedvosmisleno.

Profesionalna je dužnost sudskog vještaka da nikada svojim forenzičnim radnjama ne kontaminira dokazni materijal, odnosno oduzete medije, tvrde diskove i opremu. Ponekad je vještaku vrlo teško obavljati uvid i analizu bez mijenjanja primarnog sadržaja.

U većini slučajeva tijekom provođenja hitne istražne radnje pretrage stana i drugih prostorija, u sudskom nalogu za pretragu stana i dugih prostorija, istražni sudac ne želi uključiti i pretragu računala i računalne opreme, uz obrazloženje da je za izdavanje naloga potrebno detaljnije opisati osobno računalo ili druge elektroničke dokaze koji su predmet poduzimanja hitne istražne radnje pretrage, odnosno, potrebno je navesti barem marku ili model predmetnog osobnog računala ili računalne komponente. Vrlo su rijetke pretrage stana u kojima su prije početka pretrage poznate karakteristike osobnih računala, kako bismo ga detaljno opisali radi dobivanja sudskog naloga za pretragu osobnog računala, a

[5] Reyes, A., Brittson, R., O'Shea, K., Steel, J., Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, Rockland, Syngress Publishing Inc., 2007.

ponekad se kod same pretrage stana dođe do saznanja da se materijalni dokazi počinjenja kaznenih djela nalaze na osobnim računalima ili drugim računalnim komponentama.

Također postoje situacije kad se tijekom pretrage stana i drugih prostorija zbog osnova sumnje u počinjenje kaznih djela iz područja autorskih prava otkriju tzv. "radionice za proizvodnju CD-R ili DVD-R medija", u kojima se zatekne više osobnih računala koja su instalirana kao samostalne radne jedinice ili su međusobno povezane u mrežu, a koje nije moguće pretražiti zbog toga što bi pretraga mogla potrajati i nekoliko dana.

Postavlja se pitanje što učiniti u takvim prilikama!? Najjednostavnije rješenje je osobna računala zapečatiti službenim pečatom, kako bi se do trenutka poduzimanja njihove pretrage, osigurala vjerodostojnost dokaza. Nadalje, službenim pečatom se mogu i moraju zapečatiti i vanjski nositelji elektroničkih dokaza, kao što su čvrsti diskovi (*Hard Disk*), USB (eng. *Universal Serial Bus*) memorije (*stick*) i diskovi, optički mediji (CD, DVD, *Blu-Ray*, HD-DVD), diskete i ostali mediji na koje je moguće pohranjivati podatke (memorijske kartice).

Takvim pečaćenjem službenim pečatom sprječava se svaka mogućnost njihove uporabe do početka pretrage, što je vrlo bitno kako bi se otklonila mogućnost da se u procesnom dijelu vlasnik računala ili njegov odvjetnik pozove na proceduralnu pogrešku, uz navode da su računala bila u policiji, te postoji mogućnost da su podaci mijenjani. Skidanje službenog pečata predstavlja kazneno djelo opisano u članku 323. KZ-a, te se na taj način od eventualne zlouporabe štite sve strane i osobe koje sudjeluju u izvidima kaznenih djela u kojima se kao sredstvo ili predmet počinjenja kaznenog djela pojavljuju elektronički dokazi.

5.1. Pretraživanje računala

Radi pribavljanja materijalnih dokaza da je baš tim sredstvom počinjeno kazneno djelo, odnosno da se na/u njemu kriju dokazi koji su proizvod kaznenog djela, osobno računalo je potrebno pretražiti, odnosno potrebno je učiniti uvid u sadržaj podataka koji se nalaze na tvrdom disku računala.

Prepoznavanje elektroničkih dokaza predstavlja proces koji se mora odvijati u dva stadija. U prvom stadiju istražitelji moraju prepoznati hardver koji sadrži informacije, a nakon čega istražitelji moraju biti u mogućnosti razlikovati nevažne informacije i digitalne podatke koji su u svezi s počinjenim djelom ili mogu pružiti vezu između djela i žrtve ili djela i počinitelja. Tijekom provođenja izvida kaznenih djela iz područja računalnog kriminaliteta, kao i svih drugih izvida kaznenih djela u kojima dolazi od osnovane sumnje da je sredstvo počinjenja kaznenog djela osobno računalo ili neki njegov dio, odnosno računalna komponenta koja može biti elektronički dokaz, policijski službenici trebaju uzimati u obzir da postoji veliki broj različitih dijelova hardvera koji mogu sadržavati elektroničke dokaze, a isto tako postoji i veliki broj različitih medija za pohranu podataka, a uza sve to treba voditi i računa o medijima za prijenos podataka.

Da bi se što bolje razumjela problematika koja se opisuje, nužno je posjedovati osnovna znanja o *pojmovima* i *načinu rada samog računala*. Stoga treba nešto reći i o tome. Svaki put kada se računalo pokreće, ono se mora prilagoditi okolini koja ga okružuje,

odnosno računalnoj periferiji. Proces pokretanja računala naziva se *boot* proces. *Boot* proces uključuje tri osnovne razine[6]:

- **Centralna procesorska jedinica** (eng. *Central Processing Unit* − CPU) - predstavlja jezgru svakog računala. Sve ovisi o mogućnostima procesorske jedinice da procesira primljene instrukcije. Prva razina u boot procesu je pokrenuti odnosno resetirati procesorsku jedinicu s električnim impulsom. Ovaj se električni impuls u pravilu generira prilikom pokretanja računala. Procesorska jedinica je resetirana ako se pokrene BIOS.
- **Osnovni ulazni i izlazni sustav** (eng. *Basic Inpul and Output System* − BIOS) - rukuje se osnovnim pomicanjem podataka oko računala. Svaki program koji se pokreće na računalu koristi taj sustav da komunicira s procesorskom jedinicom. Neki sustavi dozvoljavaju korisnicima postavljanje zaporke i sve dok se zaporka ne utipka, sustav se ne pokreće.
- **Samotestiranje pri pokretanju** (eng. *Power-On Self Test* − POST) - ispituje osnovne komponente računala. Prilikom aktiviranja sustava prvo se aktivira samotestiranje. U svom početku se pokazuje besprijekornost procesorske jedinice i sustava. Nakon toga pokazuje da sve računalne komponente ispravno funkcioniraju. Kod velikog broja računala, rezultati obrade samotestiranja se spremaju u CMOS sklop (eng. *Complementary Metal-Oxide Semiconductor*). Ako postoji bilo kakav problem na bilo kojoj razini samotestiranja, računalo će signalizirati zvučnim signalima i porukom na zaslonu monitora. Računalo bi trebalo za svaki zvučni signal ispisati na zaslonu monitora objašnjenje. Nakon što su svi testovi strojnih komponenata uspješno završeni, sustav upućuje procesorsku jedinicu da potraži medij koji sadrži operacijski sustav.
- **Operacijski sustav** (eng. *Operating System* − OS) - produljuje funkcije sustava i djeluje kao sučelje između računala i vanjskog svijeta. Bez operacijskog sustava u današnjim uvjetima, bilo bi skoro nemoguće zamisliti komunikaciju s računalom. Većina današnjih računala očekuje da će operacijski sustav biti omogućen na tvrdom disku ili nekom drugom mediju. Kada je računalo spremno učitati operacijski sustav, računalo pretražuje stablo diskova tražeći specifičan redoslijed. Računalo učitava prvi operacijski sustav na koji naiđe. Na ovaj način, svim je računalima omogućeno da posjeduju primarni i sekundarni operacijski sustav, te mogućnost samostalnog odabira željenog operacijskog sustava.
- **Tvrdi disk** (eng. *Hard Disk*) - prilikom formatiranja diska on se dijeli na staze i sektore. Kombinacija dvaju ili više sektora na jednoj traci naziva se *cluster* (eng. *Cluster*) - osnovna jedinica pohrane podataka na disku. Različito formatiranje diska ima različite veličine skupina podataka, ali je koncept isti. Prilikom pospremanja datoteke koja zauzima manje nego li jedan *cluster*, ostale datoteke se neće pohranjivati u preostali prostor na *cluster.* Jednom kada *cluster* sadrži podatke, rezervirana je cijela veličina istog. Svaki računalni disk čuva zapise o svakom podatku u svakom *clusteru*. Kada je datoteka izbrisana, podaci o datoteci se brišu iz zapisa o podaci-

[6] Bača, M., Uvod u računalnu sigurnost, Zagreb, Narodne novine, 2004.

ma, ali se u biti sama datoteka ne briše s računalnog diska. Zbog toga je moguće pronaći datoteku na disku i nakon što je bila izbrisana. Podatak će na disku ostati neodređen. Čak i kada je izbrisana datoteka prepisana i ako nova datoteka ne zauzme cijeli prostor koji zauzima *cluster*, dio bi izbrisane datoteke mogao biti pročitan.

5.2. Pečaćenje računala

Na što je važno obratiti pozornost prilikom pečaćenja osobnih računala? Najvažnije je osobno računalo zapečatiti tako da ga nije moguće staviti u pogon, odnosno da ga nije moguće uključiti, a da se službeni pečat ne ošteti.

Nadalje, potrebno je osigurati da se s osobnog računala ili na osobno računalo bez povrede pečata ne može staviti ili skinuti neka komponenta koja je instalirana u osobnom računalu. Poglavito se to odnosi na nositelje elektroničkih dokaza (diskove).

U praksi se često pronalaze osobna računala sa čijeg su kućišta skinute bočne stranice, zbog boljeg hlađenja ili pak, što je češći slučaj, da se disk lakše izvuče i baci, u slučaju da policija zakuca na vrata, jer ako nema diska – nema dokaza. Što učiniti? Najjednostavnije je osobno računalo staviti u vreću ili kutiju ili ga umotati u papir i učvrstiti, te ga zapečatiti, tako da se komponentama računala ne može pristupiti bez povrede službenog pečata.

Primjeri ispravnog pečaćenja računala:

Računalo s bočnim stranicama kućišta

- na poleđinu osobnog računala stavljen je papir učvršćen ljepljivom trakom koji prekriva mjesta priključka napajanja i perifernih uređaja
- računalo je povezano špagom na čijem se čvoru nalazi službeni pečat.

Slika 1: Zapečaćeno računalo (Izvor: vlastita izrada)

Računalo bez bočnih stranica kućišta

- predmetno računalo nije imalo bočnih stranica, tvrdi diskovi nisu učvršćeni (vise na kablovima za spajanje)
- obična vreća za smeće poslužila je kao ambalaža za pakiranje, povezana sa špagom na koju je stavljen službeni pečat.

Slika 2: Zapečaćeno računalo bez bočnih stranica (Izvor: vlastita izrada)

Prijenosno računalo u pripadajućoj torbi

– prijenosno računalo zapečaćeno u originalnoj torbi tako da su patent-zatvarači povezani špagom na koju je stavljen pečat; otvoriti se može jedino ako se pečat skine.

Slika 3: Zapečaćeno prijenosno računalo u pripadajućoj torbi (Izvor: vlastita izrada)

6. ZAKLJUČAK

Rad predstavlja pokušaj uvoda u problematiku rada s digitalnim dokazima u prvom redu s kriminalističkim pristupom analize mjesta događaja odnosno pakiranja i pripreme za transport potencijalnih nositelja digitalnih podataka. U današnjem svijetu gotovo je nezamislivo raditi nešto bez računalnih podataka, koji se nalaze pohranjeni na nekom mediju. Elektronički dokazi su svuda oko nas jer živimo u svijetu u kojem tehnologija svakodnevno napreduje; tehnologije koje se bave pohranom podataka se danomice unapređuju. Metode prikupljanja i analize elektroničkih dokaza moraju biti temeljito ispitane i ponovljive kako bi se rezultatima dala vjerodostojnost potrebna za primjenu u daljnjem postupku.

Usuglašavanjem s obavezama preuzetim potpisivanjem Konvencije o kibernetičkom kriminalu Vijeća Europe, Republika Hrvatska je uskladila svoj Kazneni zakon s uvjetima Europske unije, i samim time smo dobili nekoliko novih zakonskih rješenja u području elektroničkih (digitalnih) dokaza.

Kazneni zakon propisuje nekoliko kaznenih djela koja se odnose isključivo na ovu problematiku, ali svakako ne treba zaboraviti još neke zakone kao na primjer Zakon o autorskom pravu i srodnim pravima, Zakon o zaštiti osobnih podataka, Zakon o elektroničkim komunikacijama i dr. U svim navedenim zakonima postoji nekoliko kažnjivih djela u kojima je jedini dokaz isključivo elektronički dokaz.

Radi dokazivanja ovih kaznenih djela, gotovo uvijek se provodi pretraživanje računala i računalne opreme. Elektronički dokazi su lako promjenjivi. Jednostavno uključivanje i/ili isključivanje računala može u potpunosti uništiti dokaze. Zbog toga je važno biti promišljen, dobro organiziran i upoznat s tehnologijom koja se istražuje.

LITERATURA

1. Bača, M. (2004). *Uvod u računalnu sigurnost*. Zagreb: Narodne novine.
2. CARNet CERT i LS&S (2006). *Osnove računalne forenzičke analize*. *http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2006-11-174.pdf* - 8. 2. 2008.
3. Jurman, D. *Internet – Kibernetički kriminal*. *http://www.djurman.com/index.php* - 10. 6. 2009.

4. Mason, S. (2008). *International electronic evidence*. London: British Institute of International and Comparative Law.
5. Protrka, N. (2009). *Računalna forenzička analiza*. Varaždin: Fakultet organizacije i informatike.
6. Reyes, A., Brittson, R., O'Shea, K., Steel, J. (2007). *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors.* Rockland: Syngress Publishing Inc.
7. Šimundić, S., Franjić, S. (2009). *Računalni kriminal*. Split: Pravni fakultet Sveučilišta u Splitu.

Summary

Nikola Protrka

Computer Data as Digital Evidence

This article explains what computer evidence is, and what is its importance for the further course of the proceedings, identifying some potential types of computer evidence, and where they can all reside in a digital format. As computer technology advances, so advances the technology of storing computer data, which today are all around us. Collecting such data, which can be later used as evidence in proceedings, must be done professionally.

By signing the Convention on Cybercrime, the Republic of Croatia has assumed the liability for criminal acts in the domain of computer crime, and thus the number of new legal solutions in the field of computer (digital) evidence.

In police practice, more and more police officers are faced with computer evidence, since they are present in more crimes. In order to better collect and analyze such evidence, the police officers should have a basic understanding of concepts and methods of computer work, computer equipment or other devices containing computer (digital) evidence and they must be familiar with the proper method of sealing and storage of such evidence.

Key words: computer evidence, computer crime, cybercrime, computer forensic, computer forensic analysis.