STRUČNI RAD
UDK: 343.98

Krešimir Filipić,
bacc. crim., policijski službenik PU Zagrebačke,

Nikola Protrka,
struč.spec.crim.-univ. spec. inf.,
predavač na MUP-a Visokoj policijskoj školi RH u Zagrebu.

Uloga forenzičkog softvera EnCase pri radu s elektroničkim tragovima

Sažetak

U suvremeno doba svjedoci smo nezaustavljivog i izuzetno brzog trenda razvoja informacijskih tehnologija. Internet je postao glavno mjesto razmjene podataka, reklamiranja i komunikacije među ljudima. Međutim, moramo biti svjesni da se Internetom koriste i brojne kriminalne organizacije i pojedinci radi ostvarivanja svojih kriminalnih namjera, kao što su „cyber" terorizam, razmjena zabranjenog pornografskog materijala, dječja pornografija, iznude, krađe identiteta ili nekom drugom oblik zabranjenog ponašanja. Elektroničke tragove pohranjene na računalima i raznim drugim medijima moguće je pronaći čak i kada korisnik te podatke obriše ili su oni skriveni na diskovima, za što računalni forenzičari koriste razne programske alate pomoću kojih obnavljaju i pronalaze takve dokumente, a kao jedan od takvih alata jest računalni program „EnCaseForensics". Ovim računalnim programom koristi se velik broj razvijenih policijskih organizacija poput SAD-a, Velike Britanije i drugih, a njegova osnovna namjena u policijskom smislu predstavlja pretraživanje računala i drugih nositelja elektroničkih tragova s ciljem pronalaska mogućih elektroničkih tragova. Encase predstavlja forenzički sveobuhvatan alat, ali zahtjeva visoku razinu stručnosti i znanja forenzičara koji se alatom koristi. Tako forenzičar mora imati dobra znanja o operativnim sustavima Windows, MacOS, Unix i Linux, kao i oblike datotečnog sustava u kojima su programi, datoteke i dokumenti pohranjeni (FAT, NTFS i slično). Prilikom pretraživanja medija za pohranu podataka Encase prikazuje izbrisane dokumente, particije, promijenjene dijelove dokumenata, šifrirane dokumente i drugo, te uključuje i programski jezik EnScript.

Najčešće se koristi za pretrage računala i tvrdih diskova, ali se može koristiti i za mobilne telefone, tablete i cijeli niz drugih elektroničkih uređaja.

Ključne riječi: *Računalna forenzika, Internet, kriminal, elektronički tragovi, EnCase*

1. UVOD

U današnje suvremeno doba sve učestalije su pojave nedozvoljenih oblika uporabe Interneta na globalnoj razini, čime se bave razne sigurnosne službe, od obavještajnih agencija do policijskih organizacijskih jedinica, ali i sigurnosne službe velikih poslovnih korporacija. Najvećim dijelom upravo se svjetske policije bore protiv „online" kriminala, odnosno svih kriminalnih oblika korištenja i zlouporabe Interneta, računala i drugih naprednih tehnologija.

U svakodnevnoj policijskoj praksi sve češće se susrećemo s kaznenim djelima u kojima su računala i razni drugi elektronički uređaji sredstvo pomoću kojeg se takva kaznena djela čine. Kao jedan od alata koji posjeduje hrvatska policija za potrebe pronalaska elektroničkih tragova, na raspolaganju stoji razna informatička tehnologija (IT), od nadzora telekomunikacija putem Operativno-tehničkog centra za nadzor telekomunikacija, za te potrebe razvijene i zaista impresivne aplikacije TIRM kreirane u sklopu informacijskog sustava MUP-a, pa sve do pojedinih računalnih programskih rješenja kao što je primjerice „EnCase", program koji služi za pretraživanje računala, raznih medija i većeg broja nositelja elektroničkih tragova.

Ovim radom biti će prikazan upravo program „EnCase" u verziji 7, ponajprije kroz njegovu uporabu u policijskoj praksi MUP-a RH, te će se pokušati utvrditi uporabljivost u istraživanju kaznenih djela u kojima je korištena IT tehnologija za počinjenje ili bilo kakav oblik participacije u kaznenim djelima.

2. NASTANAK I RAZVOJ PROGRAMA „ENCASE"

Američka tvrtka „GuidanceSoftwareInc." je javno trgovačko društvo osnovano 1997. godine, a ima sjedište u mjestu Pasadena, Kalifornija, SAD. Bavi se razvojem i izradom računalnih programa kao rješenja u elektroničkim istragama, a njihovi se programi koriste diljem svijeta. „GuidanceSoftwareInc." jest najveći svjetski opskrbljivač alatima za računalnu forenziku[1] i digitalne tragove.

[1] Računalna forenzika je grana forenzičke znanosti koja se bavi prikupljanjem, pretraživanjem, zaštitom i analizom tragova u digitalnom obliku te uključuje njihovu prezentaciju kao materijalnih tragova u kasnijim eventualnim sudskim postupcima.

Najpoznatiji njihov program jest „EnCase“ koji se koristi u digitalnoj forenzici, sigurnosnim analizama, cyber sigurnosti i u području e-discovery,[2] a s tim programom „GuidanceSoftwareInc.“ opskrbljuje razne državne agencije i policije diljem svijeta, ali i razne organizacije iz područja financija i osiguranja imovine, telefonije, zdravstva, farmacije i trgovine.[3]

Prema mnogim izvorima, „EnCase“ predstavlja najbolji računalni alat na svijetu, koji u Sjedinjenim Američkim Državama koristi 90%, a u Velikoj Britaniji čak 100% istražitelja.[4]

Korištenjem „EnCase“ programa može se kreirati slika diska ili medija (image), odnosno mobilnog telefona, GPS uređaja, iPoda i sličnih elektroničkih uređaja, a koji su predmet istrage, nakon čega se podaci mogu pretraživati prema specifičnim tragovima ili prema ključnim riječima. „EnCase“ omogućava pretraživanje izbrisanih datoteka, privremenih datoteka, „swap“ datoteka, komprimiranih datoteka i drugih skrivenih ili nepoznatih dokumenata zapisanih na tim uređajima ili medijima.

Osim u forenzici vezanoj za računalni kriminalitet i njegove podoblike (dječja pornografija i drugo), „EnCase“ se vrlo često koristi kao alat za smanjivanje poslovnih rizika i sprječavanje kršenja pravila poslovanja.

„EnCase“ ima također i mogućnost pretraživanja, prikupljanja, čuvanja i analize velikih količina poslovnih podataka koje su potencijalne mete cyber napada. Najpoznatiji korisnici „EnCase“ programa, osim policijskih organizacija, su NATO i tvrtka „RollsRoys“, što svakako služi za značajnu promociju ovog računalnog programa.[5]

Iako je program EnCase izrađen tako da se njime može koristiti svaka osoba osrednjeg poznavanja rada na računalima, razvijen je i proces izdavanja certifikata, koji je prvenstveno predviđen za državna tijela, čime se stupanj vjerodostojnosti podiže na višu razinu. Sam proces certifikacije traje šest mjeseci, te se u tom periodu forenzičari upoznaju s načinom rada na EnCase-u, te ih se educira kako bi znali što kvalitetnije pretražiti kreirane „image“. Tako se forenzičare obučava kako pronaći digitalne tragove uz pomoć EnCase-a, te ih s obučava o složenijim pretragama datoteka, kriptografskoj analizi podataka, principima funkcioniranja BIOS podsustava, programskoj proceduri pokretanja računala i operacijskog sustava i drugim računalnim radnjama važnim za što kvalitetnije obavljanje poslova forenzične istrage. Program obuke na ovakav način provodi se u dosta zemalja, pa tako primjerice i u Republici Srbiji, dok bi u Republici Hrvatskoj ovakvu edukaciju trebao provoditi Nacionalni CERT (eng: Criticalemergencyresponseteam).

[2] odnosi se na razmjenu informacija između državnih tijela u elektroničkom obliku
[3] https://en.wikipedia.org/wiki/Guidance_Software
[4] http://www.in2.rs/home/-/journal_content/56/10122/20125
[5] http://www.bug.hr/vijesti/digitalna-forenzika/87288.aspx

Pa ipak, unatoč tome što edukacija u RH nije toliko sveobuhvatna i detaljna, Nacionalni CERT izdao je uputu vezanu uz forenzične istrage.[6]

U vrijeme pisanja ovog članka, izašla je nova i aktualna verzija programa EnCase - 8, dok je za potrebe prikaza korištena starija verzija 7.

3. RAČUNALNI KRIMINALITET

3.1. Pojam i temeljne pravne norme

Računalni kriminal sastoji se u kriminalnom ponašanju pri čemu su kao sredstvo počinjenja uporabljena računala i/ili informacijski sustavi, a posljedica jest počinjenje kaznenog djela opisanog Kaznenim zakonom Republike Hrvatske ili povreda nekog drugog pravnog akta.

Konvencija o kibernetičkom kriminalu[7], potpisana 2001. godine u Budimpešti, predstavlja najviši međunarodni pravni akt o ovoj vrsti kriminaliteta. S obzirom da je RH ratificirala ovu Konvenciju 23.11.2001. godine, usklađeno je u hrvatsko kazneno zakonodavstvo, te stoga u važećem Kaznenom zakonu imamo navedene sve oblike inkriminacije povezane s računalima, računalnim tehnologijama i informacijskim sustavima.

Tako Konvencija, a samim time i Kazneni zakon RH, obuhvaćaju grupu kaznenih djela protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računalima i samih sustava (Neovlašten pristup, Ometanje rada računalnog sustava, Oštećenje računalnih podataka, Neovlašteno presretanje računalnih podataka čl. 266. – 269. Kaznenog zakona), Računalno krivotvorenje i Računalna prijevara čl. 270. i 271. KZ-a, Zlouporaba naprava čl. 272. KZ-a, te razna druga kaznena djela vezana uz sadržaj podataka na računalima (npr. dječja pornografija, povreda autorskih prava i slično).

3.2. Organizacijske jedinice MUP-a

Sukladno promjeni Kaznenog zakona, u posljednjoj sistematizaciji radnih mjesta u Ministarstvu unutarnjih poslova, u samom sjedištu Ravnateljstva policije, sistematizirana je jedna organizacijska jedinica koja se bavi ovom problematikom, a to je Odjel za visokotehnološki kriminalitet, te vještak za informatiku u Centru za forenzična ispitivanja, istraživanja i vještačenja Ivan Vučetić. Problem se javlja u tome što nije specificiran stupanj stručnosti policijskih službenika, odnosno njihove osposobljenosti za bavljenje ovom problematikom u vidu obveznih licenci za poznavanje rada softvera i hardvera, dok na mezzo i micro razinama (u policijskim upravama i postajama) nisu predviđene posebne ustrojstvene jedinice ili sistematizirana radna mjesta za policijske službenike za suočavanje s ovom izuzetno složenom, zahtjevnom i globalnom problematikom.

[6] Računalnaforenzika, http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-05-301.pdf
[7] http://narodne-novine.nn.hr/clanci/medunarodni/327873.html

3.3. Elektronički tragovi

Elektroničkitragovi su svi podaci u digitalnom obliku koji su stvoreni, zapisani, pohranjeni, spojeni na uređaj, računalo ili računalni sustav,[8] a koji mogu poslužiti kao dokaz u kaznenom postupku.

S obzirom na razvoj informacijskih tehnologija, danas ima mnoštvo predmeta i uređaja koji mogu biti nositelji elektroničkih tragova. Tako nositelji elektroničkih tragova mogu biti svi oblici računala, pisač, skener, modem, pametni telefoni, navigacijski uređaji, tvrdi diskovi,CD i DVD mediji, memorijske kartice, USB memorijski stikovi,ali također i podaci koju su zapisani u tzv. oblacima (cloud servisi) kao što su npr. Dropbox, Googledisk i slični, te brojni drugi.

4. UPORABA PROGRAMA "ENCASE"

4.1. Pravni temelji hodogram postupanja za izuzimanja nositelja elektroničkih tragova

Područje računalne forenzike sastoji se od četiri ključna elementa, a to su prikupljanje, pretraživanje, analiza i prezentacija. Iako se u općem terminološkom pojmu gotovo uvijek može čuti za izraz elektronički tragovi, iako se prema Zakonu o kaznenom postupku zapravo radi o elektroničkim tragovima. No, kako se tragovi utvrđuju tek u kaznenom postupku i to na sudu, prilikom policijskog postupanja zapravo se ne može govoriti o tragovima, nego o elektroničkim tragovima. No, radi lakšeg razumijevanja, u ovom radu koristit će se uobičajeni termin elektronički tragovi.

Prikupljanje elektroničkih tragova u policijskoj praksi najčešće se provodi tijekom provođenja drugih dokaznih radnji, a to su pretrage doma i drugih prostorija, te privremeno oduzimanje predmeta.U slučaju sumnje da određena osoba u svom domu ili na drugome mjestu posjeduje računalne i druge podatke koji su kriminalizirani, odnosno predstavljaju neki oblik zabranjenog ponašanja opisanog, policija podnosi o tome pisanu obavijest mjesno i stvarno nadležnom državnom odvjetniku, uz prijedlog za izdavanje naloga za pretragu doma i drugih prostorija. Ukoliko državni odvjetnik utvrdi da postoje zakonski uvjeti za dobivanje naloga za pretragu, sačinit će pisani zahtjev koji će potom dostaviti nadležnom sucu istrage (najčešće se radi o sucu istrage mjesno nadležnog Županijskog suda), a koji tada izdaje nalog.

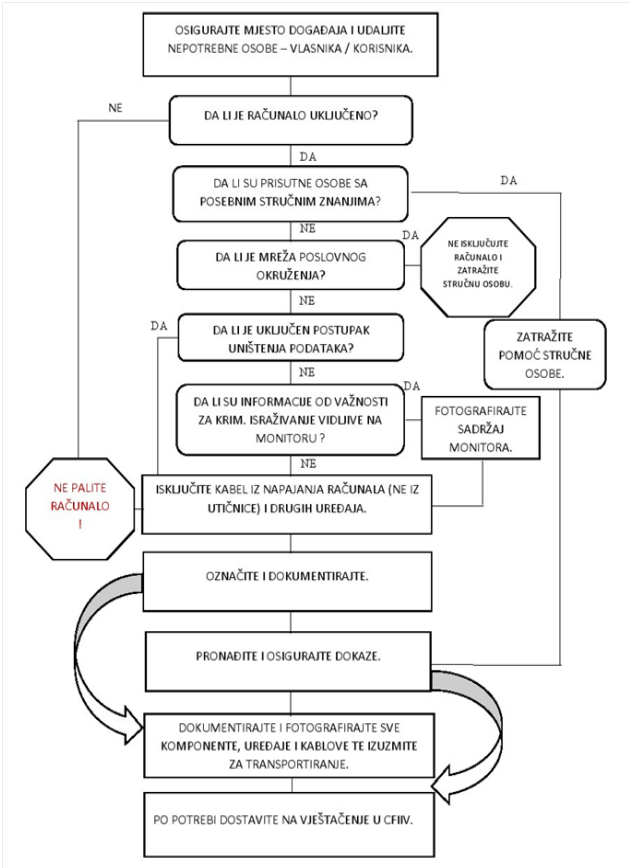
Po dobivanju naloga za pretragu, policijski istražitelj na kojega glasi nalog i policijski službenici koje istražitelj odabere u svoj tim, postupaju sukladno odredbama Zakona o kaznenom postupku koji se odnose na pretragu doma i drugih prostorija. Ukoliko se tijekom pretrage pronađu računala ili drugi nositelji elektroničkih tragova koje treba izuzeti, fotografirati će se početni ekran na uređaju (ukoliko je uređaj upaljen), nakon čega će se uređaj isključiti, te zapakirati na način da će se cijelo

[8] https://sl.wikipedia.org/wiki/Elektronički_trag

računalo obložiti papirom, folijom ili na drugi način i zapečatiti službenim pečatom kako bi se onemogućilo otvaranje računala bez skidanja pečata, a samim time i osigurao tzv. neprekinuti lanac dokaza, nakon čega se računalo odnosi u službene prostorije policije. Jedina razlika jest u postupanju s mobilnim i sličnim uređajima kada se uređaj neće gasiti (zbog mogućnosti zaštite šifrom), već će se neugašen pakirati.

Izuzimanje računala ili drugog nositelja elektroničkih tragova navest će se u Zapisniku o pretrazi i za to izdati potvrda o privremenom oduzimanju predmeta osobi kod koje se poduzima pretraga, a ukoliko se računalo ili drugi nositelj elektroničkih tragova izuzimaju bez pretrage, tada će se osim potvrde o privremenom oduzimanju predmeta sačiniti i Zapisnik o privremenom oduzimanju predmeta (bez naloga). Na ovaj način zadovoljeni su svi formalni uvjeti glede procedure izuzimanja računala/ nositelja digitalnog tragova, te će se moći u eventualnom sudskom postupku uporabiti kao dokaz.

Slika 1: Hodogram za izuzimanje računala: U.S. DepertmentofJustice, Office ofJusticePrograms, National Institute ofJustice, ElectronicCrime Scene Investigaton: „A Guide for First Responders“ Izvor: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf



Shematski prikaz vrlo precizno utvrđuje korake koje treba poduzeti prilikom izuzimanja računala, te bi bilo izuzetno korisno ovakav način postupanja unutar MUP-a obuhvatiti Standardnim operativnim postupkom kako bi se postigao jedinstven način postupanja prilikom izuzimanja računala kao nositelja elektroničkih tragova.

4.2. Pretraga pokretne stvari - računala

Nakon što je formalno na ispravan način računalo izuzeto, zapakirano i pohranjeno u službenim prostorijama policije, postupanje se nastavlja u vidu pretrage računala koju je potrebno obaviti kako bi se ponovno na valjani način pribaviti elektronički tragovi.

Zakon o kaznenom postupku[9] navodi način provođenja pretrage pokretnih stvari, među koja spadaju i računala i drugi elektronički uređaji:

„Pretraga pokretnih stvari obuhvaća i pretragu računala i s njim povezanih uređaja, drugih uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka, telefonskim, računalnim i drugim komunikacijama i nositelja podataka. Na zahtjev tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu ili drugom uređaju ili nositelju podataka, te davatelj telekomunikacijskih usluga, dužni su omogućiti pristup računalu, uređaju ili nositelju podataka, te dati potrebne obavijesti za nesmetanu uporabu i ostvarenje ciljeva pretrage.

Po nalogu tijela koje poduzima pretragu, osoba koja se koristi računalom ili ima pristup računalu i drugim uređajima iz stavka 1. ovog članka, te davatelj telekomunikacijskih usluga, dužni su odmah poduzeti mjere kojima se sprječava uništenje ili mijenjanje podataka. Tijelo koje poduzima pretragu, može provedbu tih mjera naložiti stručnom pomoćniku.“[10]

U ustrojstvenoj jedinici policije koja je započela cjelokupno postupanje, postupanje preuzima policijski službenik koji raspolaže najvišim stupnjem poznavanja računalne tehnologije, iako za to ne mora nužno biti educiran. Naime, u sustavu MUP-a ne postoji poseban program za obuku policijskih službenika na području ove problematike, nego se sve svodi na osobno iskustvo i znanje policijskih službenika, temeljem čega bi neposredno nadređeni rukovoditelj trebao odrediti kompetencije tog policijskog službenika.

4.3. Korištenje programa „EnCase“

Nakon što je računalo ili drugi nositelj elektroničkih tragova u prostorijama policije, ponovno se od državnog odvjetnika traži nalog za pretragu računala, te se

[9] Zakon o kaznenom postupku, NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13 i 152/14

[10] članak 257. Zakona o kaznenompostupku, NN 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13 i 152/14

tek po dobivanju naloga skida službeni pečat, računalo vadi iz pakiranja i otvara, te se iz računala vadi tvrdi disk (HDD), a potom se tvrdi disk spaja odgovarajućim kablom (PATA, SATA) na uređaj za izradu identične kopije kako ne bi kontaminirali original. Napravljenu kopiju diska potom spajamo na računalo na kojemu je instaliran računalni program „EnCase".

Slika 2: HDD priključen S-ATA kablom
Izvor: https://de.wikipedia.org/wiki/Serial_ATA

S obzirom da su elektronički tragovi vrlo često dobro sakriveni pod lažnim imenima, označeni kao sasvim druga vrsta dokumenata, a nerijetko i obrisani od strane korisnika, za njihovo pretraživanje i pronalazak vrlo često nije dostatno solidno znanje o računalnim tehnologijama koje određeni dio policijskih službenika ima, već su za to potrebni specijalizirani „alati".

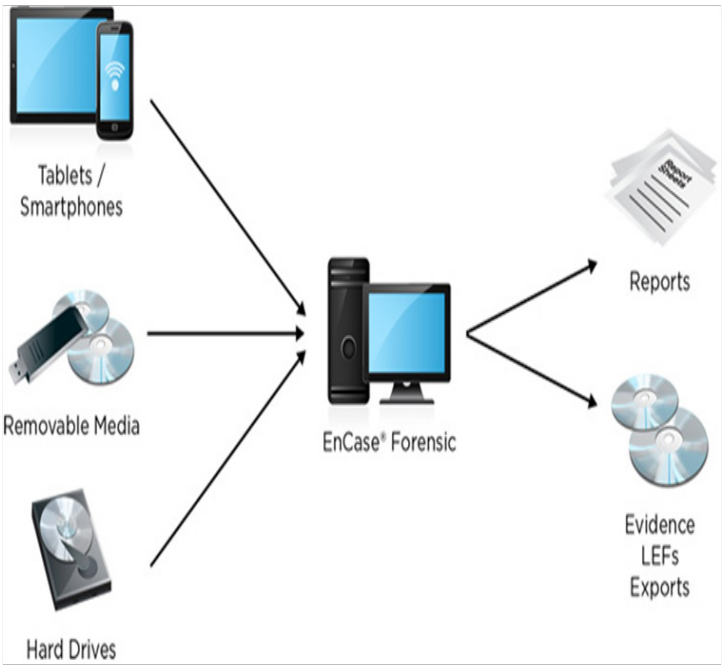
Jedan od takvih alata je i program „EnCase", koji hrvatska policija posjeduje od 2006. godine, te su računala s instaliranim programom „EnCase" uglavnom u sjedištima kriminalističke policije u policijskim upravama, ali i u Ravnateljstvu policije.

Osim što nam pomaže u pretraživanju i pronalasku inkriminiranih elektroničkih tragova, „EnCase" omogućava da izvorni podaci na ručanu ili uređaju koji je glavni nositelj takvih podataka ostane u izvornom stanju. To se postiže na način da se pomoću „EnCase"-a stvara slika diska (eng: image) i može

se načiniti više istovjetnih kopija, što omogućava da ih u isto vrijeme analizira više stručnjaka.

Također nam „EnCase“ omogućava da tako prikupljeni elektronički tragovi na sudu budu uporabljeni kao trag, zajedno sa izvješćem o forenzičkoj istrazi, koju program „EnCase“ generira na kraju obrade podataka.

Slika 3: SoftwareEnCase - pretraga i proizvodi pretrage
Izvor: http://www.ndm.net/ediscovery/images/stories/images/01encase_forensic.jpg



Nakon što je HDD spojen s računalom koje ima instaliran „EnCase“, potrebno je uključiti to računalo i potom pokrenuti program „EnCase“. Tada se otvara korisničko sučelje tog programa koje sadržava sve potrebne poddirektorije i opcije za obradu HDD, njegovog pretraživanja i pronalaska elektroničkih tragova.

Nakon toga potrebno je kreirati sliku diska (image), koja je istovjetna stvarnoj slici na originalnom disku. Po dovršetku kreiranja slike diska računalo je potrebno isključiti, odvojiti HDD od S-ATA kabla, te ga vratiti u originalno pripadajuće računalo.

Ponovno pokrenuti računalo na kojemu je stvorena slika diska, pokrenuti program „EnCase“ i pritisnuti tipku „open“, a zatim pronaći sliku diska i istu otvoriti u programu.

U tom trenutku prikazat će se izgled diska, koji je spreman za pretragu.

Prvi korak u pretraživanju slike diska odnosi se na pretraživanje naziva datoteka, te se po dovršetku pretraživanja prikazuju rezultati pretrage, koje se pojedinačno može označiti i zatim je potrebno sve označene dokumente prebaciti u tzv. „bookmarks“, što predstavlja svojevrsnu listu prioriteta.

U sljedećem koraku potrebno je kreirati popis ključnih riječi prema kojima će se obaviti novo pretraživanje, a ključne riječi određuju se prema logičkom slijedu, ovisno o tome što se traži, odnosno o kakvom se događaju radi. Po tim ključnim riječima ponovno se pretražuje slika diska, te se na ekranu ispisuju rezultati pretrage, koje je ponovno potrebno pojedinačno označiti i spremiti u „bookmarks“.

Nadalje se svi dokumenti spremljeni u „bookmarks“ dodaju u izvještaj, nakon čega program generira izvještaj o istrazi, što u ovom procesu predstavlja gotovi proizvod, odnosno završetak pretraživanja, dokumentiranja i fiksiranja pronađenih tragova (elektroničkih tragova).

5. POSTUPANJE U PRAKSI

Promatrajući primjenu programa „EnCase“ svakako se može doći do početnog zaključka kako se radi o zaista jednostavnom i impresivnom alatu za otkrivanje inkriminiranog sadržaja na nositeljima elektroničkih tragova, posebno računalima, pametnim telefonima, prijenosnim memorijskim uređajima i karticama, te mnogim drugim medijima.

Pa ipak, je li to u praksi zaista tako?

Odgovor ćemo potražiti u iskustvima djelatnika Ministarstva unutarnjih poslova, realnog sektora i drugih stručnjaka iz ovog područja u Republici Hrvatskoj.

Već duži niz godina program „EnCase“ stoji na raspolaganju policijskim službenicima Ministarstva unutarnjih poslova RH, poglavito u Centru za forenzična ispitivanja, istraživanja i vještačenja „Ivan Vučetić“, zatim u Odjelu za visokotehnološki kriminal Ravnateljstva policije, Policijskom nacionalnom uredu za suzbijanje korupcije i organiziranog kriminala, kao i u Službama gospodarskog kriminaliteta u četiri najveće Policijske uprave, odnosno PU zagrebačkoj, primorsko-goranskoj, osječko-baranjskoj i splitsko-dalmatinskoj.
Iako je program fizički dostupan tim ustrojstvenim jedinicama, u razgovoru s njihovim djelatnicima došlo se iznenađujućih rezultata - program „EnCase“ koristi se vrlo rijetko ili se uopće ne koristi, već se pri pretrazi računala i sličnih uređaja koriste drugi alati kao što su „ForensicToolkit“, „Belkasoft“, „X-ways“, „Winhex“ i slični forenzični programi.

Logično se nameće pitanje zbog čega se toliko hvaljeni program „EnCase“ ne koristi?

Prema iskustvima svih djelatnika navedenih ustrojstvenih jedinica MUP-a, jedan od glavnih razloga je što je „EnCase“ preglomazan, a samim time rad s ovim programom traje znatno duže od drugih navedenih programa, što znači da sam postupak obrade digitalnih tragova u praksi traje i po nekoliko dana duže pri radu s „EnCase“-om.

Drugi razlog jest što je program „EnCase“ prezahtjevan, tj. potrebna je jača računalna konfiguracija, koju većina službenih računala MUP-a ne zadovoljava. Što to zapravo znači? Pa, prema navodima proizvođača za optimalno korištenje programa „EnCase“ verzije 7 potrebno je imati sljedeće instaliran operativni sustav Windows i to XP Profesional, Server 2003 Standard, Server 2008 R2 Standard, Vista, Windows 7, Windows 8, Windows 8.1, Server 2012 ili Server 2012 R2, ugrađen DVD player/snimač, procesor Dual Core ili QuadCore, dok Intel Itanium nije podržan, RAM memorije 16 GB, te HDD slobodnog kapaciteta 425 MB.

Iz svega ovog može se zaključiti da program u većini komponenata nije zahtjeva, osim u zahtjevima za RAM memorijom koje treba čak 16 GB. Svakako treba naglasiti kako tu količinu RAM memorije ima vrlo mali broj računala, a samo kao usporedbu treba navesti da velika većina službenih računala MUP-a nema toliku RAM memoriju, nego imaju do 4 GB. Što se tiče računala na kojemu se nalazi instaliran program „EnCase“ u Službi gospodarskog kriminaliteta Policijske uprave zagrebačke, to računalo zadovoljava sve navedene zahtjeve, osim RAM memorije koje također ima 4 GB, te se najvjerojatnije upravo u ovom dijelu nalazi zapreka za uspješnu uporabu programa „EnCase“.

Temeljem iskustava policijskih službenika koji provode pretrage računala, isti su u više slučajeva započeli korištenje programa „EnCase“ radi provođenja dokazne radnje pretrage prijenosne stvari – računala, na temelju izdanog naloga za pretragu. Tom prilikom su, upravo kao što bi i trebalo, izvadili HDD iz pretraživanog računala, spojili ga kablovima na službeno računalo, pokrenuli program „EnCase“ i započeli sa stvaranjem slike diska (image). Kako su kapaciteti tih HDD bili po nekoliko TB, stvaranje slike diska računalo nije uspjelo izvršiti u roku od tri dana, čime su bili prekoračeni valjanosti naloga za pretragu.

Osim toga, nerijetko se u praksi događa da tijekom postupka kreiranja slike HDD-a nakon nekoliko dana dolazi do „pucanja“, odnosno nekontroliranog prekida rada programa, čime se u potpunosti gubi slika diska.

Iz tih razloga se program „EnCase“ više ne koristi, nego se koriste drugi alati, koje su policijski službenici uglavnom besplatno preuzeli iz legalnih Internet izvora.

Cijeneći ova saznanja, moramo se zapitati zašto MUP nije osigurao „jača“ računala, barem za uporabu programa „EnCase“, kako bi se podigla razina profesionalnosti i vjerodostojnosti prilikom provođenja ove dokazne radnje, čija učestalost će u budućnosti zasigurno rasti i biti će potrebna sve snažnija računala,

jer se kontinuirano povećava snaga komercijalno dostupnih računala.

Svakako je potrebno navesti da se tijekom procjene uporabljivosti programa „EnCase“ nisu uzela u obzir isključivo iskustva djelatnika MUP-a, već i njegovih korisnika u realnom sektoru, ali i uvaženih stručnjaka iz područja računalne forenzike. Ovaj program koriste za svoje potrebe Hrvatska narodna banka, Carnet, Zavod za sigurnost informacijskih sustava, Aerodrom Pleso, Agencija za zaštitu tržišnog natjecanja, te koncern „Agrokor“. S obzirom na različitu svrhu uporabe ovog programa u tim tijelima, ponešto se razlikuje i uporabljivost „EnCase“-a, dok svi imaju zajednički stav da ovaj program ne može predstavljati cjelovito i isključivo rješenje u radu, već se koristi isključivo kao nadopuna s nekim drugim računalnim programima.

6. Zaključak

Iz svega navedenog nedvojbeno je utvrđeno kako program „EnCase“ predstavlja globalno prihvatljivi standard u sudbenim tijelima razvijenijih zemalja. Najbolji primjer tome su uporaba „EnCase“-a u izuzetno visokim postocima u SAD-u i Velikoj Britaniji, na čijim kaznenopravnim sustavima dobrim dijelom počiva i hrvatsko kazneno zakonodavstvo.

Sukladno tome, smatram da bi i hrvatska policija, ali i cijeli pravosudni sustav morali težiti upravo prema takvim standardima najrazvijenijih zemalja, što bi svakako predstavljala uporaba ovog računalnog forenzičkog programa.

Pa ipak, kao i u mnogim drugim područjima, pokazalo se da ovaj program ima izuzetno bitnih negativnih karakteristika koje se tome da postupak rada na određenom slučaju traje predugo, traži jaku računalnu „platformu“ i nerijetko dolazi do zastoja prilikom kreiranja slike diska koji program obrađuje, što dovodi u pitanje funkcionalnost i iskoristivost ovog programa u radu hrvatske policije. Tvrtka „INsig“ d.o.o. koja je ovlašteni zastupnik programa „EnCase“ za cijelu regiju, odnosno za države bivše Jugoslavije, navodi da je verzija 6 programa „EnCase“ bila jednostavnija i učinkovitija za uporabu, te samim time i prihvaćena u širem krugu korisnika. Uvođenjem verzije 7 tog programa došlo je do prevelike širine u mogućnostima, što je rezultiralo smanjenjem učinkovitosti i stabilnosti u radu tog programa, a u konačnici upravo stoga dobar dio ranijih korisnika nije produžio licence koje su imali za korištenje programa „EnCase“. „INsig2“ svjestan je tih problema, te su u više navrata ukazivali „Guidancesoftware“-u na to, ali do sada nije došlo do promjena.

Ovi pokazatelji rezultirali su time da svaki računalni forenzičar u svom radu koristi različite programe i ne postoji nikakva propisana standardizacija glede programskih rješenja u obradi digitalnih tragova u RH. To zapravo znači da svaki računalni forenzičar može koristiti bilo koji program za obradu digitalnih tragova, pa iako nema pisanih rezultata takvog načina rada, bilo bi izuzetno zanimljivo vidjeti ima li uporaba drugih, besplatnih forenzičkih alata učinaka

na efikasnost i kvalitetu provođenja dokazne radnje pretrage pokretne stvari od strane policijskih istražitelja, ali i na razinu vjerodostojnosti takvih tragova u daljnjim stadijima kaznenih postupaka.

Literatura

1. Mukasey, Michael B., Sedgwick, Jeffrey L., Hagy, David W., U.S. Department of Justice, Office of Justice Programs, National Institute of Justice., Electronic Crime Scene Investigation: A Guide for First Responders, second edition. Wahington
2. Kazneni zakon, „Narodne novine“ broj125/11, 144/12, 56/15 i 61/15
3. Zakon o kaznenom postupku, “Narodne novine” broj 152/08, 76/09, 80/11, 91/12,143/12, 56/13, 145/13i 152/14
4. Konvencija o kibernetičkom kriminalitetu http://narodne-novine.nn.hr/clanci/medunarodni/327873.html, datum pristupa 25.8.2016.
5. EnCase Forensic, EnCase Endpoint Investigator, User Guide Version 7.12, http://download.guidancesoftware.com/7DRap3XOHH%2BOl1Ild74tqNw7h4PsLkO48xNZgmPmzJwdZAtvMw4FT7xk11SxKJ3e2pUcOQGJAQY%3D, datum pristupa 25.8.2016.
6. Protrka, Nikola: Računalni podaci kao elektronički (elektronički) dokazi, stručni članak, prosinac 2010. - hrcak.srce.hr/file/117711 - datum pristupa 25.8.2016.
7. https://en.wikipedia.org/wiki/Guidance_Software, datum pristupa 25.8.2016.
8. http://www.in2.rs/home/-/journal_content/56/10122/20125, datum pristupa 25.8.2016.
9. http://www.bug.hr/vijesti/digitalna-forenzika/87288.aspx, datum pristupa 25.8.2016.
10. Računalna forenzika http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-05-301. pdf, datum pristupa 25.8.2016.

IZVORI SLIKA:

- slika 1. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, datum pristupa 25.8.2016.
- slika 2. https://de.wikipedia.org/wiki/Serial_ATA, datum pristupa 25.8.2016.
- slika 3. http://www.ndm.net/ediscovery/images/stories/images/01encase_forensic.jp, datum pristupa 25.8.2016.

SUMMARY

The role of forensic software EnCase with digital trace

In modern times, we have witnessed the unstoppable trend and extremely rapid development of IT technology. The Internet has become the main place of exchange of information, advertising and communication between people. However, we must be aware that numerous criminal organizations and individuals to achieve their criminal intent, such as cyber terrorism, exchange of prohibited pornographic material, child pornography, extortion, identity theft or some other form of prohibited conduct, use Internet.

Digital evidence stored on computers and various other media can be found even when the user that data wiped or they are hidden on the disc, for which computer forensic experts used a variety of software tools to help renew and find these documents. As one of such tool is the computer program "EnCase Forensics". This computer program is used in a large number of developed police organizations such as the US, UK and others, and its main purpose in the police sense represents the search of computers and other holders of digital trace with the aim of finding of possible digital evidence.

Encase forensic represents a powerful tool, but requires a high level of expertise and knowledge of the forensic tools that are used. So forensic expert must have a good knowledge of Windows, MacOS, Unix and Linux, as well as the form of file system in which programs, files and documents are stored (FAT, NTFS, etc.). While we search for files on different kind of digital media for storing files, Encase shows deleted documents, partitions, changed parts of documents, encrypted documents and another, and includes a programming language Enscript. Most commonly used for computers and computer hard drives, but can also be used for mobile phones, tablets and a host of other electronic devices.

Keywords: *Computer forensics, Internet, crime, digital evidence, EnCase*