CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Računalna forenzika

NCERT-PUBDOC-2010-05-301

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni CERT, www.cert.hr

Nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.LSS.hr

Laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

U današnje vrijeme kriminalci sve više koriste računala za izvođenje krađa, prijevara i drugih zlonamjernih radnji. Pojava *cyber*-kriminala je dramatično porasla u posljednje vrijeme ponajviše zbog napretka u informacijskoj tehnologiji. Istu tehnologiju koja se koristi u svakodnevnom životu moguće je zloupotrijebiti za kriminalne radnje. Mnogi ljudi koji na zlonamjeran način koriste računala pretpostavljaju da se mogu izgubiti u moru osobnih i prijenosnih računala koja se koriste u svijetu te da su sigurni od kaznene odgovornosti. Ipak, ukoliko je otkrivena zlouporaba računala, ono se može pretražiti za dokazima i analizirati te je tako moguće utvrditi odgovornost osobe koja je počinila nedjelo. Upravo to rade računalni forenzičari. Vrlo je važno da digitalne dokaze prikupljaju certificirani računalni forenzičari jer se podaci tokom prikupljanja mogu izgubiti ili oštetiti.

Mnogo je načina na koje se računalo može zloupotrijebiti, a neki od slučajeva uključuju posjedovanje dječje pornografije, iznudu novca, krađu identiteta, pronevjeru, pokretanje napada na druga računala ili organizacije i slično.

Digitalne dokaze moguće je otkriti čak i kada je zločinac obrisao podatke s računala. To se izvodi različitim alatima za obnovu podataka. Ukoliko taj postupak obavlja forenzički istražitelj, dokazi se prihvaćaju na sudu i on može svjedočiti o njima. Kao i sve organizacije koje sudjeluju u kriminalističkoj istrazi, računalni forenzičari moraju slijediti stroge procedure kako bi se dokazni materijali mogli iskoristiti u sudskom postupku.

U dokumentu je dan uvod u računalnu forenziku, te su opisani osnovni pojmovi i procedure koje istražitelji moraju slijediti. Također, opisani su forenzički alati koji su u čestoj upotrebi te načini osposobljavanja računalnih forenzičara za njihovu upotrebu.

2. Što je računalna forenzika?

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

Slika 1. Računalo kao digitalni dokazni materijal

Cilj računalne forenzike je objasniti trenutno stanje digitalnog artefakta. Pojam digitalni artefakt može uključivati računalni sustav, medij za pohranu podataka, kao što su čvrsti disk ili DVD medij, elektronički dokument (poruku elektroničke pošte, digitalnu fotografiju) ili niz mrežnih paketa.

Postoji mnogo razloga za primjenu računalne forenzike, a neki od njih su:

- u pravnim slučajevima tehnike računalne forenzike se koriste za analizu računalnih uređaja koji pripadaju optuženicima.
- za oporavak podataka u slučaju kvara računalnih komponenti i uređaja te analize računalnih programa.
- za analizu računalnog sustava nakon napada kako bi se utvrdilo kako je napadač pristupio sustavu i što je učinio nakon što je upao u sustav.
- za prikupljanje dokaza protiv zaposlenika za kojeg organizacija smatra da se bavi aktivnostima koje nisu dozvoljene.
- za prikupljanje podataka o računalnim sustavima u svrhu pronalaska pogrešaka u programima, optimizacije učinkovitosti programa ili obrnutog inženjerstva (eng. *reverse engineering*).

Prilikom provođenja forenzičke istrage potrebno je poduzeti posebne mjere ukoliko dokazi trebaju biti prihvatljivi na sudu. Jedna od najvažnijih mjera je osiguravanje da je dokaz prikupljen na ispravan način i da se poštuje lanac posjeda dokaza od mjesta zločina do laboratorija i konačno do suda.

Elektronički uređaj nad kojim je počinjena kriminalna radnja ili je bio alat za obavljanje iste prenosi se u forenzički laboratorij u stanju u kojem je pronađen radi daljnje analize. Podaci s njega se kopiraju uporabom forenzičkog alata i ta kopija čini temelj istrage. Izvorni uređaj nikada nije objekt nad kojim se obavlja istraga jer mora služiti kao dokaz. Zbog toga niti jedan podatak na njemu ne smije biti izmijenjen. Kopija mora biti vjerodostojna da bi uopće mogla biti objekt istrage. Ponekad elektronički uređaj nije moguće prenijeti u laboratorij pa se kopiranje mora obaviti na mjestu zločina. Nakon što se različitim metodama dokaže vjerodostojnost kopije s nje se počinju prikupljati podaci koji se zatim analiziraju.

Računalna forenzika dijeli se na četiri grane:

- forenzika vatrozida (eng. *firewall forensics*),
- mrežna forenzika (eng. *network forensics*),
- forenzika baza podataka (eng. *database forensics*) i
- forenzika mobilnih uređaja (eng. *mobile device forensics*).

2.1. Mrežna forenzika

Mrežna forenzika se bavi upotrebom znanstveno dokazanih tehnika za prikupljanje, identifikaciju, pretraživanje, povezivanje, analizu i dokumentaciju digitalnih dokaza iz više aktivnih digitalnih izvora koji odašilju i primaju podatke u svrhu otkrivanja činjenica vezanih uz planiranje i uspješno obavljanje kriminalnih radnji.

Temelji se na praćenju mrežnog prometa i otkrivanju anomalija. Nakon što su otkrivene anomalije u mrežnom prometu, utvrđuje se predstavljaju li one napad. U slučaju da su otkrivene zlonamjerne aktivnosti, analizira se koje su to aktivnosti i koja im je svrha. Važni aspekti uključuju presretanje prometa, očuvanje dokaza, analizu i vizualizaciju rezultata. Računalni sigurnosni incident je, prema definiciji iz Pravilnika o koordinaciji prevencije i odgovora na računalne sigurnosne incidente, svaki događaj koji ugrožava bilo koji aspekt računalne sigurnosti, odnosno koji za posljedicu ima gubitak povjerljivosti, cjelovitosti i raspoloživosti podatka, zlouporabu ili oštećenje informacijskog sustava ili informacija, uskraćivanje usluge ili onemogućavanje rada informacijskog sustava te svaka nezakonita radnja čiji se dokazi mogu pohraniti na računalni medij. Forenzički specijalisti uvidom u prikupljene dokaze mogu odgovoriti na sigurnosni incident. To znači da oni mogu otkriti tko stoji iza napada na računalni sustav i prikupiti dokaze koji će osigurati njegovu osudu ukoliko dođe do sudskog postupka. Napadač može obrisati dnevničke datoteke (eng. *log files*) na ugroženom računalu klijenta te dokazi prikupljeni praćenjem mrežnog prometa mogu biti jedini dokazi koji vode do otkrivanja napadača i izvora napada.

Sustavi mrežne forenzike mogu biti tzv.:

- „Ulovi-to-kako-možeš“ sustavi (eng. *„Catch-it-as-you-can“ systems*) – svi paketi koji prolaze kroz određenu prometnu točku se presreću i spremaju za daljnju analizu. Ovaj pristup zahtjeva mnogo prostora za pohranu podataka.
- „Stani, pogledaj i poslušaj“ sustavi (eng. *„Stop, look and listen“ systems*) – svaki paket se analizira na rudimentaran način u memoriji i samo se određeni podaci pohranjuju za buduću analizu. Ovaj pristup zahtjeva brze procesore kako bi se obradio svaki paket.

2.2. Forenzika baza podataka

Forenzika baza podataka se bavi pretraživanjem i analizom baza podataka ili posebnih transakcija i relacija (eng. *tables*) izvučenih iz baze na način koji ne uništava podatke u svrhu rekonstrukcije podataka ili događaja koji su se zbili u sustavu.

Prilikom prikupljanja baza podataka za analizu one se obavezno moraju kopirati te se analiza mora obaviti na kopiji izvorne baze kako bi otkriveni dokazi bili prihvatljivi u eventualnom sudskom procesu. Forenzička analiza baze podataka može uključivati vremenske zapise o ažuriranju zapisa u relaciji kako bi se utvrdile akcije korisnika baze. Osim toga, forenzički pregled može biti usredotočen na identificiranje transakcija u sustavu baze podataka ili aplikaciji koja sadrži dokaze o kriminalnim radnjama, kao što je pronevjera novca.

Zbog primjene posebne pažnje kod analize baze podataka potrebno je primijeniti prilagođene programske alate, kao što su ACL, Idea i Arbutus. Spomenuti alati između ostalog pružaju okružje koje dozvoljava samo čitanje baze podataka.

2.3. Forenzika mobilnih uređaja

Forenzika mobilnih uređaja uključuje skup metoda pretraživanja dokaza s mobilnih uređaja. Posebno se pažnje pridaje načinu forenzičke pohrane memorije mobilnog uređaja, odnosno stvaranju memorijske slike uređaja. Memorijska slika može biti dokaz i koristiti se za daljnju istragu. Tehnike stvaranja forenzičke slike medija su posebne za mobilne uređaje jer oni koriste drugačije tipove memorije i sučelja od osobnog računala. Mobilni uređaj se sastoji od mikroprocesora, *flash* memorije i RAM-a (eng. *Random Access Memory)*. Na mobilnim uređajima obično se nalaze podaci kao što su kontakti (brojevi telefona, adrese), fotografije, kalendari i bilješke. Prema tome, mobilni uređaji imaju važnu ulogu u istražnom procesu.

3. Proces obavljanja forenzičke analize

Postoji četiri temeljna koraka u području računalne forenzike:

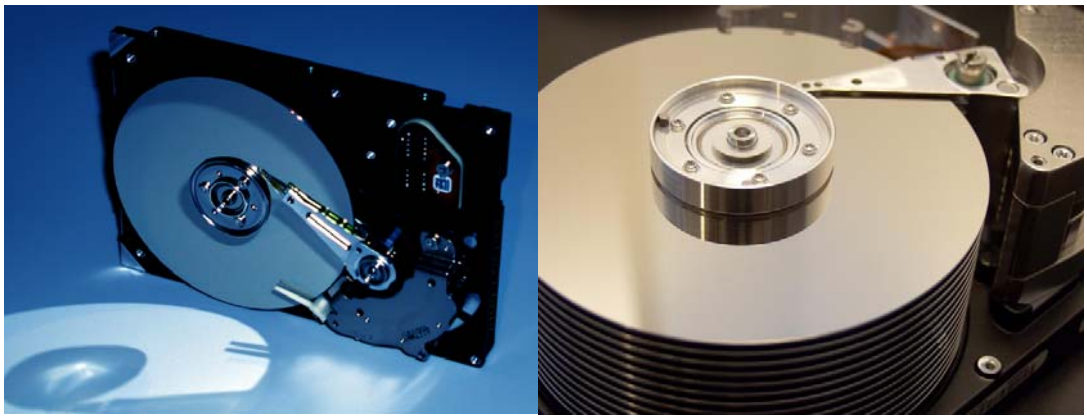
- prikupljanje,
- pretraživanje,
- analiza i
- prezentacija.

3.1. Prikupljanje digitalnih dokaza

Kad forenzički stručnjak dođe na mjesto zločina, mora odmah započeti s dokumentiranjem. Fotografiranje zatečenog stanja, snimanje, pisanje natuknica, čak i snimanje diktafonom su obavezne akcije tijekom forenzičke analize. Zatim, treba uočiti je li računalo uključeno i ukoliko jest, obavezno ga ostaviti u tom stanju. Isključivanje bi uzrokovalo izmjenu nekoliko stotina datoteka na koje djeluje operacijski sustav prilikom gašenja računala. Važno je uočiti i pod kojim operacijskim sustavom računalo radi te kojom je vrstom sklopovlja opremljeno. Digitalne dokaze je moguće prikupiti iz više izvora. Uobičajeni izvori su:

- osobna računala,
- mobiteli,
- digitalne kamere,
- čvrsti diskovi,
- optički mediji,
- USB memorijski uređaji i drugo.

Sljedeće slike prikazuju kako izgledaju čvrsti diskovi kada se ukloni zaštitno kućište.



Slika 2. Čvrsti diskovi

Osim nabrojanih izvora, dokazi se mogu prikupiti i iz postavki digitalnih termometara, crnih kutija automobila (ako ih imaju), RFID oznaka, web stranica (moraju se očuvati u izvornom stanju jer su podložne promjenama) i slično.

Digitalne dokaze potrebno je prikupljati s mnogo pažnje jer je većina digitalnih podataka podložna izmjenama. Jednom kada su promijenjeni gotovo je nemoguće otkriti koja se promjena dogodila ili vratiti sustav u izvorno stanje. Zbog toga se radi kopija diska koja se još naziva i forenzička kopija diska (eng. *bit-stream image, forensic image*). Forenzička kopija nije obična logička kopija zato što ne sadrži samo korisniku vidljive podatke koji se trenutno nalaze na disku, nego i podatke koji su bili izbrisani. Ona je identična kopija svakog pojedinog dijela (eng. *cluster*) diska. Stvara se na posebnom disku koji prije kopiranja mora biti potpuno prazan. Obično formatiranje nije dovoljno jer ono ne odstranjuje sve podatke s medija. Forenzička metoda formatiranja sastoji se u ispisivanju niza nula koje ispunjavaju svaki sektor diska. Na taj način se disk u potpunosti očisti. Nakon stvaranja forenzičke kopije diska provjerava

se autentičnost kopije uz pomoć kriptografskog sažetka. Sažetak se koristi za potvrdu ispravnosti kopije, kao i za provjeru je li dokazni materijal bio izmijenjen nakon računanja sažetka.

Također, primjenjuju se metode rukovanja digitalnim dokazima koje uključuju:

- stvaranje slika (eng. *image*) računalnog medija upotrebom alata koje zabranjuje pisanje na medij kako bi se osiguralo da podaci nisu izmijenjeni, dodani ili obrisani s uređaja koji je prikupljen kao dokazni materijal,
- uspostavljanje i održavanje lanca posjeda dokaza,
- dokumentiranje svega što se čini s dokaznim materijalom i
- upotrebu alata i metoda koje su provjerene i čiju je točnost moguće izraziti u postocima.

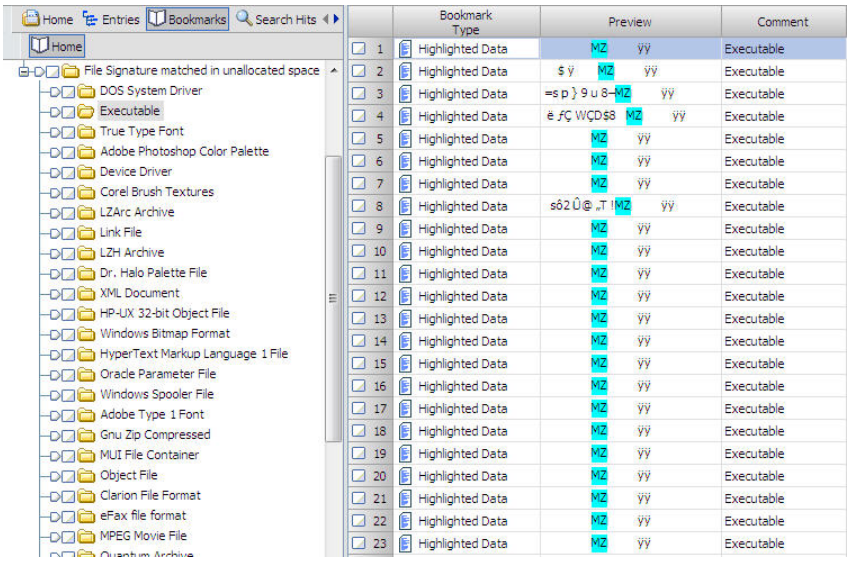
Neke od najvrjednijih dokaza moguće je dobiti od korisnika računala koje je prikupljeno kao dokaz. U razgovoru s korisnikom mogu se doznati vrijedni podaci o postavkama sustava, programskim paketima, korištenoj enkripciji i slično. Mnogo je lakše obaviti forenzičku analizu upotrebom korisnikovih zaporki za pristup kriptiranim datotekama i mrežnim poslužiteljima. U istrazi u kojoj vlasnik digitalnog uređaja, koji je uveden kao dokazni materijal, nije pristao na suradnju forenzički istražitelj mora imati nalog za kopiranje i pretraživanje podataka.

3.2. Pretraživanje

Nakon što su svi dokazni materijali prikupljeni, može se početi s pretraživanjem digitalnih zapisa. Način na koji se započinje istraga ovisi o vrsti slučaja. Ispituje li se disk kako bi se pronašla dječja pornografija, istraga započinje pretraživanjem fotografija. Istražuje li se zlouporaba podataka neke korporacije, pretraživanje se usmjeruje na elektroničku poštu. Jednostavni slučajevi, u kojima je poznat objekt pretrage, oduzimaju manje vremena, dok složeniji slučajevi, u kojima je potrebno uzeti u obzir podatke iz nekoliko izvora, oduzimaju više vremena. Vrlo je važno učinkovito iskoristiti vrijeme jer ponekad sudski proces započinje prije nego što je istraga zaključena. Zbog toga je dobar početni korak ukloniti iz istrage datoteke za koje je poznato da nisu potencijalni dokazi.

Izdvajanje podataka može započeti analizom kriptografskog sažetka. Primjerice, neka je disk koji se pregledava jedan od diskova iz velike tvrtke u kojoj se dogodilo curenje podataka. Vlasnici sumnjaju da je zaposlenik odao neke važne informacije konkurentskoj tvrtki. Tvrtka forenzičkom timu daje sve kritične podatke za koje se boje da su mogli biti proslijeđeni te ih oni pomoću algoritma kriptografskih sažetaka uspoređuju s podacima na disku. Pronađe li algoritam podudarne datoteke, ispisat će ih na ekranu računala. Na taj način radi velika većina forenzičkih programskih paketa koji obrađuju podatke analizom kriptografskih sažetaka.

Sljedeći korak uključuje provjeru potpisa datoteke (eng. *file signature*). Potpis datoteke se koristi za identifikaciju ili provjeru sadržaja datoteke. Svaka datoteka ima svoj potpis koji se sastoji od magičnog broja (kratkog niza bajtova, obično 2-4 smještenih na početak datoteke) i on govori u kojem je programskom alatu nastala. Dakle, potpis datoteke se koristi za identifikaciju formata datoteke. Ova je metoda vrlo korisna kada se provjerava je li korisnik računala promijenio ime i ekstenziju datoteke kako bi prikrio njezin pravi sadržaj. Datoteku u JPG formatu korisnik lako može preimenovati u .doc format. Obični korisnik nikada neće primijetiti da je to zapravo fotografija jer će Word svakoj .doc datoteci dodijeliti Word ikonu. Forenzički stručnjak će datoteku provesti kroz poseban alat i ukoliko se pokaže da trenutna ekstenzija ne odgovara njezinom stvarnom formatu, datoteka ide na detaljniju analizu.



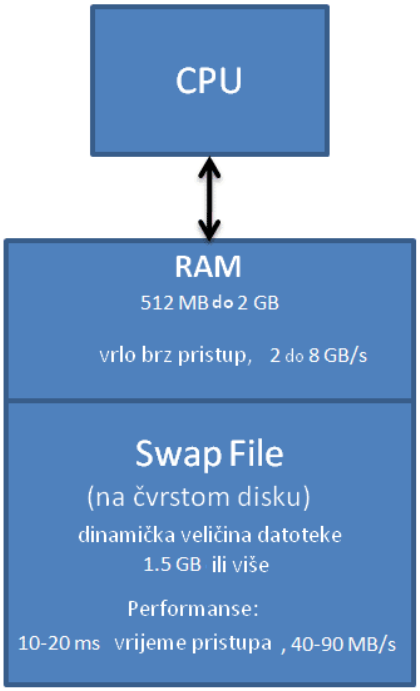
Slika 3. Pretraživanje i provjera potpisa datoteka alatom EnScript
Izvor: ForensicKB

Pretraga se može nastaviti prema ključnoj riječi (eng. *keyword analysis*). Stvara se tekstualna datoteka u koju se upisuju ključne riječi. Pomoću posebnih alata mogu se pronaći sva pojavljivanja riječi iz tekstualne datoteke te na taj način izdvojiti datoteke prema sadržaju.

Ukoliko istražitelj zna što otprilike traži, datoteka se može izdvojiti i po:

- tipu,
- veličini i
- datumu nastanka.

Nakon izdvajanja svih datoteka koje su dostupne kreće se na pregledavanje obrisanih podataka, zamjenske datoteke (eng. *swap file*) te neiskorištenih sektora na disku. Zamjenska datoteka je binarna datoteka koja predstavlja virtualnu memoriju računala. U nju se prosljeđuje sadržaj radne memorije koji se najdalje u prošlosti nije koristio te iz koje se sadržaj po potrebi ponovo vraća u radnu memoriju. Zamjenska datoteka može sadržavati podatke koji su forenzički izbrisani s diska. Zbog toga je vrlo koristan izvor informacija. Sljedeća slika prikazuje usporedbu i povezanost zamjenske datoteke s radnom memorijom i središnjom procesnom jedinicom.



Slika 4.Usporedba zamjenske datoteke sa radnom memorijom

Sljedeće mjesto koje je potrebno pregledati je *recycle bin* (prostor na disku, posebna datoteka, u koju se spremaju datoteke prije konačnog brisanja s diska). Netko je možda u strahu pokušao brzo prikriti dokaze i odlučio ih izbrisati. Međutim obrisani podaci nisu u potpunosti uklonjeni sa sustava, čak i kada su izbrisani iz *recycle bin-a*. Ako korisnik nije izbrisao datoteke iz *recycle bin-a* te je datoteke vrlo lako vratiti. Datoteke koje su obrisane iz *recycle bin-a* još uvijek se zadržavaju na disku i operacijski sustav u tablici datoteka obilježava njihov prostor slobodnim. Kada mu taj prostor bude odgovarao za zapis novih podataka samo će ih prepisati preko starih. To znači da će još neko vrijeme obrisane datoteke biti na disku. Uz to, moguće je pročitati i njihove metapodatke (podatke o podacima) koji sadrže ime, vrijeme nastajanja, vrijeme izmjene, ime autora i slično.

Bitni dokazi se mogu otkriti i u privremenim datotekama (eng. *temporary files*). Različite aplikacije ih stvaraju tokom svojeg rada i po završetku ih brišu. Microsoft Word, na primjer, stvara privremenu datoteku svaki puta kada se snimaju izmjene na dokumentu s kojim korisnik radi. To znači da će forenzički stručnjak vidjeti kada i kako se mijenjao dokument te saznati kako je nastala određena datoteka.

Pregledava li istražitelj sadržaj sandučića elektroničke pošte, može saznati s kime je i kada osoba komunicirala i kakve su podatke razmijenili. Ponekad se korisnici služe *webmail* uslugom pa se prilikom preuzimanja poruka elektroničke pošte s Interneta one spremaju u privremene datoteke (eng. *temporary Internet files*). Budući da se tu spremaju i različite druge aktivnosti vezane uz korištenje Interneta, moguće je pronaći i podatke poput:

- web stranica koje je korisnik posjećivao,
- kojeg dana je to bilo,
- koliko često odlazi tamo te
- što je preuzimao s Interneta i sl.

Podaci vezani uz aktivnosti na Internetu nalaze se i u *cookie* datotekama. To su podaci koji nastaju u komunikaciji poslužitelja i klijenta. Spremaju se na računalo u obliku tekstualnih datoteka i imaju široku primjenu. Na primjer, korisniku omogućuju obavljanje kupovine preko Interneta. Točnije, omogućuju mu spremanje i vađenje proizvoda iz virtualne košarice. Osim toga, olakšavaju mu prijavljivanje na različite web stranice spremanjem zapisa o tome da je on već autorizirani korisnik pa se ne traži ponovno upisivanje korisničkog imena i lozinke. Pomoću *cookie* datoteka moguće je pratiti koje stranice korisnik posjećuje.

Izuzetno važan izvor forenzičkih dokaza mogu biti dnevničke datoteke koje se nalaze na poslužitelju. One mogu sadržavati informacije o sustavskim sredstvima, procesima i aktivnostima korisnika. Ukoliko administrator sustava ne omogući bilježenje aktivnosti na mreži, moguće je da neće postojati dokazi potrebni da se počinitelj zločina poveže sa sigurnosnim incidentom. Nažalost, iskusni kriminalci znaju da je jedno od prvih pravila pri upadu u sustav obrisati ili izmijeniti sadržaj dnevničke datoteke tako da njihova aktivnost na sustavu ne bude zabilježena.

Sve opisane metode odnose se na pretraživanje diska kojeg je bilo moguće isključiti s mreže, ponijeti u laboratorij i tamo provesti daljnje korake. Međutim, česta je pojava da je računalo nemoguće isključiti s mreže i tada se istraga provodi na licu mjesta, što je puno teže jer se sustav neprestano mijenja i jedan potez mijenja više od nekoliko stvari u sustavu. Budući da je izmjene nemoguće spriječiti važno je svesti ih na minimum i to tako da se koraci pretraživanja sustava provode prema unaprijed određenom planu.

3.3. Analiza

Analiza je proces tumačenja dokaza prikupljenih tijekom procesa pretraživanja podataka. Ona je korak u kojem istražitelj dolazi do krajnjih rezultata istrage. Postoji nekoliko vrsta analiza:

- **vremenska analiza** - određuje kada se određeni događaj zbio i stvara sliku o razvoju zločina korak po korak. Provodi se pregledom vremenskih metapodataka (posljednja izmjena, posljednji pristup, vrijeme nastanka, promjena statusa) ili dnevničke datoteke (može se saznati kada se korisnik prijavio na sustav).
- **analiza skrivenih podataka** - korisna je u rekonstrukciji skrivenih podataka i može ukazivati na vlasništvo, vještinu ili namjeru. Ako se pretraživanjem naišlo na podatke koji imaju izmijenjenu ekstenziju, to odmah upućuje na namjerno skrivanje podataka. Dohvat kriptiranih, komprimiranih podataka te podataka zaštićenih lozinkama upućuje na skrivanje podataka od strane zlonamjernih korisnika.
- **analiza datoteka i aplikacija** – izvode se zaključci o sustavu i vještini korisnika. Rezultati ove analize ukazuju na sljedeće mjere koje se moraju poduzeti kako bi se analiza obavila do kraja. To mogu biti:
    - pregledavanje sadržaja datoteka,
    - identificiranje broja i vrsta operacijskih sustava,
    - utvrđivanje povezanosti datoteka,
    - pregledavanje korisničkih postavki.

Krajnji korak analize je njezin zaključak. U njemu se povežu do sada prikupljeni i analizirani podaci u cjelovitu priču.

3.4. Prezentacija rezultata istrage

Izvještaj povezuje zaključke analize, dokaze i dokumentaciju, sadrži vrijeme i datum analize te detaljan opis rezultata. Stvaranje izvještaja je najvažnija faza računalne forenzike i treba sadržavati detaljnu dokumentaciju alata, procesa i metodologije. Složenost izvještaja ovisi o njegovoj namjeni. Ponekad se, osim za sudski proces, piše i poseban izvještaj za izvršnog menadžera kako bi tvrtka dobila zahtijevane odgovore. Kada je istraga zaključena i slučaj predan sudu, rezultati istrage se prezentiraju odvjetnicima, sucu i poroti. Forenzički stručnjak mora biti u stanju na jednostavan način obrazložiti rezultate, a nerijetko odvjetnici, suci i porota prolaze osnovne tečajeve računalne forenzike kako bi što kvalitetnije mogli sudjelovati u sudskom procesu.

4. Forenzički alati

Postoji nekoliko vrsta forenzičkih alata. Glavna podjela je na alate za analizu programskih paketa te alate za analizu fizičkih komponenti računala. Postoji nekoliko besplatnih alata, no većina su komercijalni.

Slika 5. Forenzički alati
Izvor: Google

4.1. Alati za analizu programa

Nakon obavljene istrage i predstavljanja njezinih rezultata, dokazi se temeljito proučavaju u sudskom procesu. Razvijeno je mnogo alata koji stručnjacima pomažu u pregledavanju, pretraživanju i analizi dokaza.

Programski alati za upravljanje podacima na čvrstom disku su:

- *PDBlock* – alat tvrtke Digital Intelligence koji sprječava pisanje po izvornom disku prilikom forenzičkog kopiranja diska,
- *DriveSpy* - alat temeljen na operacijskom sustavi DOS sa sučeljem sličnim istom, koji omogućuje stvaranje forenzičke kopije diska, obnavljanje obrisanih podataka i neiskorištenih dijelova sektora te analizu upotrebom kriptografskog sažetka,
- *Forensic Replicator*– alat tvrtke Parben Forensics Tools za forenzičko kopiranje različitih medija,
- *FTK Imager* – alat tvrtke AccessData Corporation za forenzičko kopiranje,
- *SnapBack Exact* – alat tvrtke SnapBack koji služi za forenzičko kopiranje diska,
- *DiskSig* – alat tvrtke NTI koji služi za provjeru autentičnosti forenzičke kopije diska i
- *GetFree* – alat tvrtke NTI koji služi za kopiranje oslobođenog prostora diska, spremanje tih podataka na drugi medij te njihovu analizu.

Alati za obnovu podataka su:

- *Ontrack* – program za obnavljanje podataka izbrisanih s diska,
- *AcoDisk* – program za obnovu podataka s optičkih medija i
- *MediaMerge* - alat tvrtke Computer Conversions koji služi za obnavljanje podataka s optičkih medija i tvrdih diskova.

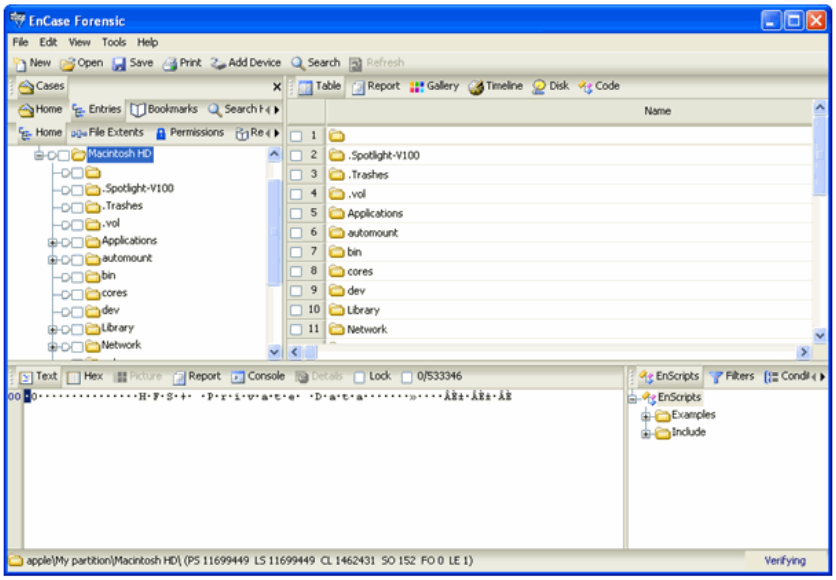
Preglednici binarnih datoteka:

- *010 Hex editor* – alat tvrtke SweetScape koji služi za pregledavanje binarnih datoteka te
- *Hex Workshop* – programski paket tvrtke BreakPoint koji služi za pregledavanje i upravljanje datotekama, predviđen za rad na operacijskom sustavu Windows.

Višenamjenski programski paketi:

- *EnCase* – programski paket tvrtke Guidance Software, jedan od najpotpunijih forenzičkih programskih paketa,

- *Maresware* – alat tvrtke Mares and Company koji sadrži kolekciju korisnih alata za forenziku na mjestu zločina i
- *Access Data*.



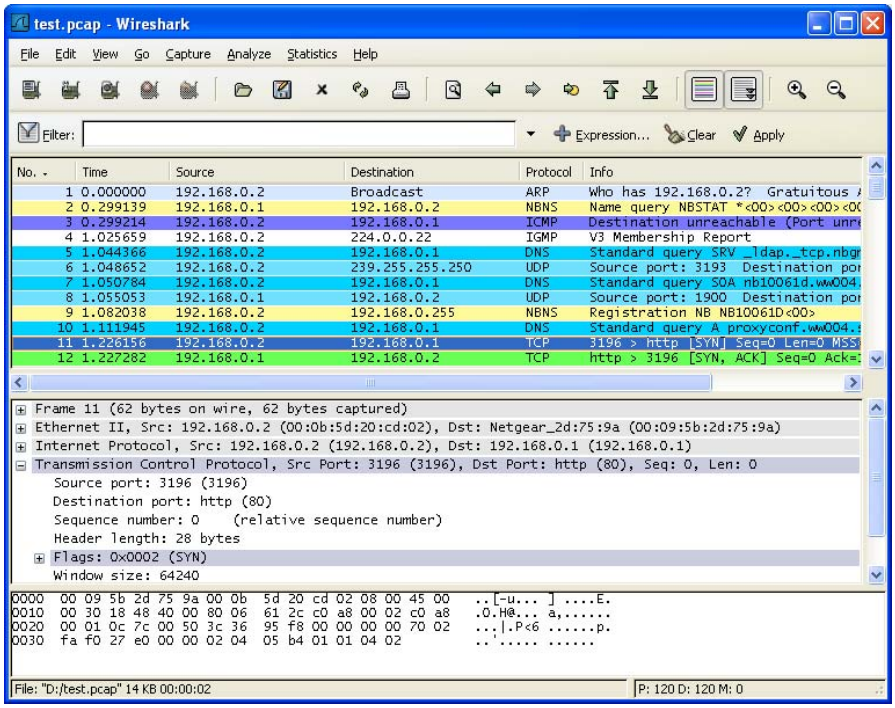
Slika 6. Primjer grafičkog sučelja programa EnCase
Izvor: EnCase

Besplatni forenzički alati:

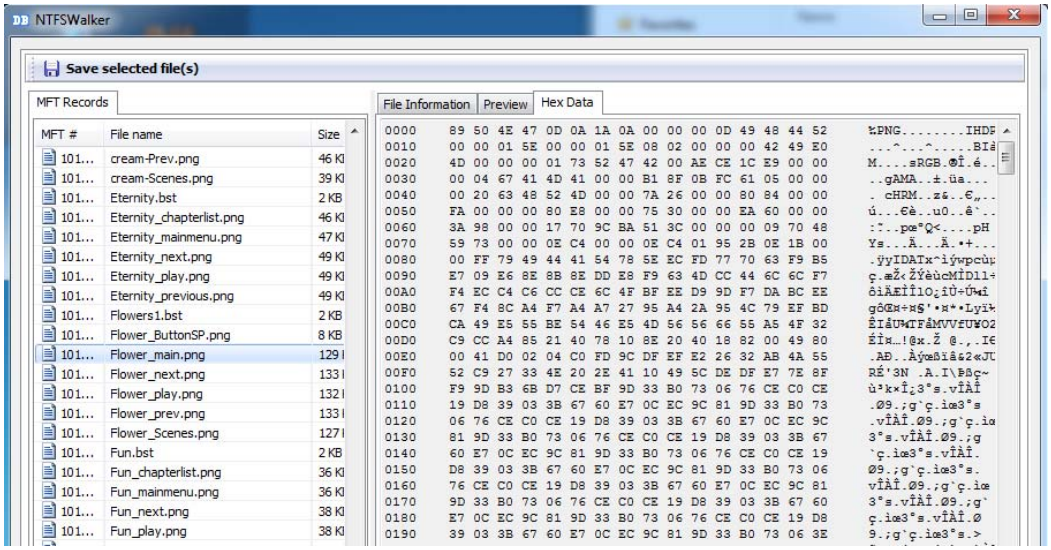
- *Sleuth Kit* –biblioteka i kolekcija komandno-linijskih alata koji omogućuju pretraživanje diska i datotečnog sustava (http://www.sleuthkit.org/),
- *Helix* – skupina forenzičkih alata koja uključuje Sleuth Kit i mnoge druge aplikacije (http://www.e-fense.com/helix/),
- *Foremost* – alat za pretraživanje slikovnih datoteka i različitih datotečnih sustava, kao što su Linux ext2/ext3, Linux swap, UFS, JFS, NTFS, FAT12, FAT16, FAT32,

  (http://sourceforge.net/projects/foremost)
- *F.I.R.E.* (eng. *Forensic and Incident Response Environment*) – samostalna skupina alata koja se pokreće kada se upali računalo (http://fire.dmzs.com/)
- *Forensic Toolkit, BinText, Galleta, NTLast, Pasco, Patchit, Rifiuti, i ShoWin* – alati posebno namijenjeni operacijskom sustavu Windows (http://www.foundstone.com/),
- *WinHex* – alat za upravljanje datotekama, diskovima i radnom memorijom u heksadekadskom formatu (http://www.x-ways.net/winhex/),
- *SMART Linux* – Linux distribucija posebno osmišljena za forenzičku analizu dokaza. Sadrži alate za analizu podataka, pretraživanje i odgovor na sigurnosni incident. (http://www.asrdata2.com/),
- *Wireshark* – alat za analizu mrežnog prometa (http://www.wireshark.org/),
- *NTFSWalker* – alat za analizu NTFS datotečnog sustava (http://www.brothersoft.com/ntfswalker-262095.html)

Sljedeće slike prikazuju primjer rada alata Wireshark i NTFSWalker.



Slika 7. Primjer rada programa Wireshark koji presreće mrežni promet i priprema ga za analizu. Izvor: Wireshark



Slika 8. Prikaz podataka na disku u heksadekadskom formatu alatom NTFSWalker. Izvor: Softpedia

Iako postoji mnogo forenzičkih alata, besplatnih i komercijalnih, bez stručnog nadzora moguće je uništiti dokaze, a time i sudski proces. Potrebno je naglasiti da forenzičku istragu prema tome može kvalitetno i pravovaljano voditi isključivo forenzički stručnjak.

4.2. Alati za analizu diska

Čvrsti disk je sastavni dio računala i obično se na njemu nalazi operacijski sustav koji sadrži različite programske pakete. Većina forenzičkih alata može se pokrenuti s jednog takvog sustava, odnosno običnog računala. No, ukoliko je potrebno zasebno analizirati dijelove računala, kao što su čvrsti diskovi, optički mediji, USB memorijske kartice, mobilni uređaji i slično, potrebna je posebna oprema. Postoji nekoliko proizvođača takvih forenzičkih uređaja za analizu dokaznog materijala (dijelova računala za pohranu podataka) i najvažniji među njima su Digital Intelligence i Vogon International.

Proizvodi tvrtke Digital Intelligence su:

- forenzički sustavi - Fred, Freddie, Fred SR, Fred-M, Fred-C,
- uređaji za prikupljanje podataka - Forensic Talon Kit, Forensic Talon, Forensic MD5 Kit, Forensic MDP, Clone Card PRO, OmniPort,
- prijenosni uređaji - CellDEK, Mobile Response Kit, Wireless Stronghold Bag, STE3000F RF Enclosure, Remote Charger,
- uređaji za obradu optičkih medija (CD, DVD) - FAR LITE, FAR PRO i
- uređaji za kopiranje (kloniranje) podataka - Echo Plus, Sonix, OmniClone 2Xi, OmniClone 5Xi, OmniClone 10Xi, OmniSCSI 1, OmniSCSI 4, OmniWipe.

Sljedeća slika prikazuje uređaj Fred.

Slika 9. FRED - Forensic Recovery of Evidence Device
Izvor: Digital Intelligence

Proizvodi tvrtke Vogon International su:

- prijenosni i laboratorijski sustavi,
- uređaji za forenzičko kopiranje te
- prijenosne i laboratorijske radne stanice.

5. Certifikacija forenzičkih istražitelja

Forenzika je multidisciplinarno i interdisciplinarno područje. U razvijenim zemljama, naročito SAD-u, postojanje diplomskih studija forenzike dovelo je do kvalitetnog i učinkovitog rada pravosuđa. U Hrvatskoj je 2009. osnovan Studij forenzičkih znanosti na Sveučilištu u Splitu. Do tada nije postojala jedinstvena škola ili fakultet na kojem je bilo moguće izučiti forenzičku znanost. U Hrvatskoj postoje sljedeći forenzički laboratoriji:

- Zavod za sudsku medicinu zagrebačkog Medicinskog fakulteta,
- MUP-ov Centar za kriminalistička vještačenja Ivan Vučetić te
- Splitski forenzički laboratorij.

U SAD-u postoji nekoliko forenzičkih certifikata koje istražitelji moraju imati kako bi mogli svjedočiti na sudu. Jedan od certifikata koji nije vezan uz proizvođača programskih alata je GIAC (eng. *Global Information Assurance Certification*), a forenzičar koji posjeduje taj certifikat postaje certificirani GIAC forenzički analitičar

(eng. *GIAC Certified Forensic Analyst - GCFA*). U siječnju 2010. spomenuti certifikat je akreditiran po programu ANSI/ISO/IEC 17024 za certifikaciju osoblja. Slika 10. prikazuje logo koji koriste certificirani istražitelji.

Slika 10. GCFA (*GIAC Certified Forensic Analyst*).
Izvor: www.giac.com

Organizacija IACRB (eng. *Information Assurance Certification Review Board*) sponzorira CCFE (eng. *Certified Computer Forensics Examiner*) certifikaciju. Kandidati moraju proći pismeni ispit na kojem moraju imati 70% ili više točnih odgovora. Kandidati koji prođu spomenuti ispit dobivaju dokazne datoteke u obliku kopije čvrstog diska. Datoteke moraju analizirati i predati na ocjenjivanje.

IACIS (eng. *International Association of Computer Investigative Specialists*) nudi obavljanje certifikacije računalnih forenzičara od 1994. godine. U početku je to bio „MS-DOS Processing Certificate" (DPC), a kasnije CFCE (eng. *Certified Forensic Computer Examiner*) koji osposobljava kandidate za rad s forenzičkim kopijama te rješavanje problema koji se javljaju pri analizi digitalnog dokaznog materijala.

Različite računalne tvrtke nude certifikate posebno namijenjene za rad s njihovim programskim paketima. Na primjer, za rad s alatom EnCase izdaje se EnCE certifikat (eng. *Encase Certified Examiner*), a za alat AccessData ACE certifikat. EnCE certifikacija se obavlja od 2001. godine.

Forenzički istražitelji obično počinju svoju karijeru u policiji i sličnim vladinim organizacijama ili u tvrtkama koje se bave računalnom sigurnošću. U današnje vrijeme za forenzičke stručnjake se zahtjeva da imaju barem završeni preddiplomski ili diplomski studijski program iz područja društvenih i humanističkih znanosti, medicine, biomedicine i zdravstva, biotehnologije, tehničkih znanosti ili prirodnih znanosti.

6. Zakon i računalna forenzika

Zakon ima presudan utjecaj na računalnu forenziku jer ima stroga pravila o prihvaćanju prikupljenih podataka kao dokaza. Da bi se prikupljene informacije uistinu smatrale dokaznim materijalom, mora se održati visoka razina formalnosti u postupanju s računalom i njegovim spremnicima. Posebna briga se mora voditi kada se pristupa podacima osumnjičenika, virusima, elektromagnetskim i mehaničkim oštećenjima, a ponekad i računalnim zamkama (eng. *booby- traps*). Postoji nekoliko pravila kojih se treba pridržavati kako se ne bi ugrozila pravna upotrebljivost dokaza:

- koristiti samo alate i metode koje su prethodno ispitane i ocjenjene. Ispitivanje alata provode institucije poput proizvođača programskih paketa, vladinih organizacija (na primjer Defense Cyber Crime Institute iz SAD-a) i druge,
- originalne dokaze treba što manje mijenjati i odložiti na sigurno mjesto,
- zapisivati sve što je napravljeno jer je dokumentacija na kraju dio izvještaja,
- istražitelj treba poštovati vlastito znanje ili neznanje, tj. raditi samo ono u što je siguran da zna.

Također, potrebno je paziti na osjetljivost informacija do kojih se došlo pretragom, a koje nisu vezane za one podatke koji nas zanimaju. Zakoni nisu isti u svim državama, ali su im namjene i namjere jednake. U istragama kod kojih vlasnik digitalne opreme nije dao pristanak za inspekciju, a to su krivične istražne radnje, posebno se mora paziti da stručnjak za računalnu forenziku ima sve dozvole i zakonski autoritet za pregledavanje, kopiranje, otuđivanje i korištenje svih uređaja i njihovog sadržaja (odgovarajući sudski nalog). Ako to nije slučaj, osim odbacivanja dokaza na sudu, teško je očekivati izbjegavanje pravne tužbe. Koliko god da je forenzička obrada bila vođena ispravnim principima, uvijek je moguće doći u situaciju u kojoj će dokaz biti odbačen. Isto tako, ponekad izostanak stvaranja forenzičke kopije čvrstog diska neće biti otežavajuća

okolnost pri prezentaciji dokaza. Digitalna forenzika je relativno nova znanstvena disciplina i zakoni koji su temelj za priznavanje elektroničkih dokaza na sudovima još su uvijek u stanju nedorečenosti. Konstantan napredak tehnologije dovodi do većeg broja dokaza i alata, a time i dokaznog materijala, što u nekim slučajevima može biti i loše jer dokazi nisu jasni. Ipak, računalna forenzika se ne koristi samo u svrhe kriminalističke istrage. Alati i metode specifične za digitalnu forenziku koriste se i u svrhu povratka izgubljenih podataka kod običnih korisnika računala. Također, koriste se i u velikim tvrtkama za zaštitu računalnih mreža. Novije zakonske legislative u zapadnim državama drže odgovornim tvrtke koje ne uspiju spriječiti otkrivanje i zlouporabu osobnih podataka svojih klijenata pa je bavljenje računalnom forenzikom ponekad način da se tvrtki sačuva ugled i novac.

Uzimajući za cilj usuglašavanje međunarodnih zakona iz područja „cyber – zločina“ , Vijeće Europe je, kao najstarije tijelo Europske Unije, postavilo temelje dokumenta nazvanog „Konvencija o kibernetičkom kriminalu“ (eng. *Convention on cybercrime*). Konvencija je prvi međunarodni dokument koji želi skrenuti pažnju na rastuću stopu informatičkog kriminala, obrativši posebnu pažnju na prijestupe koji su nastali putem Interneta ili drugih komunikacijskih mreža, kršenje autorskih prava, dječju pornografiju i računalnu prijevaru. Hrvatska je taj dokument ratificirala 2002. godine.

Kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava uključuju:

- nezakoniti pristup,
- nezakonito presretanje,
- ometanje podataka,
- ometanje sustava,
- zloporabu uređaja,
- računalno krivotvorenje,
- kaznena djela vezana uz dječju pornografiju,
- kaznena djela povrede autorskih i srodnih prava te
- pokušaj, pomaganje ili poticanje na zločin.

6.1. Primjer primjene računalne forenzike

U SAD-u je računalna forenzika imala veliku ulogu u hvatanju i osudi serijskog ubojice kojeg su popularno zvali „BTK Killer“ ili „BTK ubojica“. Dennis Rader je osuđen za niz serijskih ubojstava koja su se dogodila u vremenskom razmaku od šesnaest godina. Prije uhićenja Rader je slao pisma policiji na *floppy* disku. Metapodaci u dokumentima ukazali su da se autor zove Dennis i da je povezan sa luteranskom crkvom (eng. *Christ Lutheran Church*). Ovi su dokazi pomogli istražiteljima i doveli do Raderovog uhićenja.

Osim što računalna forenzika može pomoću u hvatanju i osudi ubojica, u današnje doba gotovo svaki kriminalistički slučaj sadrži digitalne dokaze koji se koriste u sudskom procesu.

7. Zaključak

U današnje vrijeme javlja se porast broja zločina počinjenih upotrebom računala. Razvoj tehnologije je s jedne strane olakšao mnoge poslove i riješio različite probleme, no s druge strane ta ista tehnologija se može zlouporabiti u zločinačke svrhe. Više nije pitanje hoće li netko postati žrtvom zlouporabe računala već kada će to postati. Stoga je neizmjerno važno da forenzički stručnjaci i provoditelji zakona postupaju s digitalnim dokazima s pažnjom te ih analiziraju i predstave temeljito i transparentno. Mnoge agencije u svijetu pružaju izobrazbu o prikupljanju, ispitivanju i korištenju digitalnih dokaza. U Hrvatskoj postoji nekoliko ustanova koje se bave osposobljavanjem kadrova računalne forenzike. Uskoro će biti potrebno i šire profesionalno obrazovanje u području računalne forenzike jer će zajedno s napretkom tehnologije i porastom kriminala rasti potreba za osiguravanjem podataka i rješavanjem računalnih zločina. U postupku forenzičke istrage koriste se mnogi računalni alati i uređaji koji pomažu istražiteljima u očuvanju, pretraživanju i analizi digitalnih dokaza. Mnogi alati i uređaji su komercijalni i skupi, no postoji i nekolicina besplatnih alata koji omogućuju i običnom korisniku njihovu upotrebu. Obični korisnik takve alate može koristiti za obnovu obrisanih podataka, praćenje, presretanje i analizu mrežnog prometa te druge aktivnosti.

Računalna forenzika važno je područje forenzičke znanosti ne samo zbog hvatanja i osude cyber-kriminalaca, već i ubojica te drugih zakonskih prijestupnika. Računalni sigurnosni incidenti su postali svakodnevica i neizbježni su. Kako bi se otkrili krivci iza incidenata potrebno nužno je upotrijebiti tehnike računalne forenzike. Osim u rješavanju slučajeva u kojima su kriminalci iskoristili slabosti računala, računalnih programa i mreža, računalni forenzičari koriste svoja znanja u praćenju i otkrivanju različitih kriminalaca i ubojica. Čini se kako budućnost rješavanja kriminalnih slučajeva leži upravo u računalnoj forenzici i sličnim metodama otkrivanja informacija o kriminalu.

8. Reference

[1] Računalna forenzika, http://en.wikipedia.org/wiki/Computer_forensics, svibanj 2010.

[2] Računalna forenzika, http://www.cromwell-intl.com/security/security-forensics.html, siječanj 2010.

[3] Open Source Digital Forensics, http://www.opensourceforensics.org/, travanj 2010.

[4] Five Essential Computer Forensics Tools, http://www.enterpriseitplanet.com/security/features/article.php/3786046/Five-Essential-Computer-Forensics-Tools.htm, studeni 2008.

[5] Studij forenzičnih znanosti, http://forenzika.unist.hr/Naslovnica/tabid/475/Default.aspx, svibanj 2010.

[6] Digital Intelligence, http://www.digitalintelligence.com/, svibanj 2010.

[7] Smart Linux, http://www.asrdata2.com/, svibanj 2010.

[8] Firewall Forensics, http://www.linuxsecurity.com/resource_files/firewalls/firewall-seen.html, svibanj 2010.

[9] Vogon Investigation, http://www.vogon-investigation.com/, svibanj 2010.

[10] Access Data, http://www.accessdata.com/forensictoolkit.html, svibanj 2010.

[11] „Dragan Primorac: Split i Hrvatska postaju centar forenzičkog svijeta!", http://zastita.info/hr/clanak/2009/10/dragan-primorac-split-i-hrvatska-postaju-centar-forenzickog-svijeta!,105,3494.html, časopis Zaštita, broj 6, 2009.