RAČUNALNA FORENZIKA

UVOD U RAČUNALNU FORENZIKU

Razvoj kompjuterske tehnologije

- Kompjuterska je tehnologija posljednjih godina veoma napredovala, što je rezultiralo njenim uvođenjem u različite aspekte našeg života.
  - osobna oprema (mobiteli i srodni uređaji, audio i video plejeri)
  - oprema u stanu (telefon, telefaks, video i sl. oprema, DTV, automatizirani kućanski aparati)
  - računalna i njoj srodna oprema u uredu i stanu (server, osobno računalo, prenosivo računalo, dlanovnici, žična i bežična infrastruktura)
  - identifikacijski dokumenti (e-indeks, "pametne kartice", e-socijalno)
  - kreditne i debitne kartice (American, Diners, Maestro, Visa i sl.)
  - e-informacije (vijesti, novine, forumi, društvene mreže, oglasnici)

Nove tehnologije u poslovanju

- Tvornice koriste tehnološki napredak i zamjenjuju stare strojeve sofisticiranijom opremom kako bi poboljšale svoju proizvodnju.
- Gdje je to god moguće papir se u arhivama zamijenjuje elektroničkom bazom podataka.
- Menadžeri u tvrtkama umjesto pairnatog rokovnika koriste različite elektroničke planere.
- Korisnici Interneta postali su sudionici online trgovine.
- Bolnice su kartone pacijenata zamijenile informacijama u elektroničkom obliku.
- Novi oblik pohrane podataka znači bitno poboljšanje u odnosu na prethodno stanje, ali i otvara vrata i skupini ljudi koja je te podatke zloupotrebljava. Podaci su postali lakše dostupni, a sama tehnologija donijela je moćnije alate i u njihove ruke.

Potreba zaštite podataka

- Primjena novih tehnologija stvorila je potrebu za različitim vrstama zaštite podataka, međutim, koliko god da je znanost uspješna u tom aspektu, onaj tko je htio doći do podatka uvijek je nekako pronalazio način da to i učini.
- Sudionici online trgovine shvatili su da im netko krade novac sa računa, tvrtke su uočile neautoriziran pristup važnim podacima, banke su oštećene transakcijama koje je izvršila nepoznata vanjska osoba.
- Postaje je očito da smo sve češće žrtve nove vrste kriminala koji prije svega treba prevenirati, a ako se već dogodi tada svoju ključnu ulogu ima danas relativno mlada znanost - računalna forenzika u otkrivanju počinitelja i dokazivanju njegove krivnje.

Definicija računalne forenzike

- Računalna forenzika je znanost koja se bavi
  - *sakupljanjem*
  - *pretraživanjem*
  - *analizom*
  - *prezentacijom*

  podataka koji se na neki način mogu dobaviti s dijelova elektroničkih uređaja koji imaju svojstvo da privremeno ili trajno mogu zapamtiti odrenu informaciju.

Predmet forenzičke analize

- Elektronički uređaj nad kojim je počinjena kriminalna radnja ili koji je bio alat za izvršenje takve radnje, ako je to moguće i ako se na taj način neće izgubiti dio dragocjenih informacija, transportira se u forenzički laboratorij u stanju u kojem je pronađen radi daljnje analize.
- Podaci s uređaja se kopiraju uporabom forenzičkih alata (hardvera i softvera) i ta kopija postaje dokaz, odnosno predmet daljnje istrage.
- Izvorni uređaj nikada ne bi trebao biti objekt nad kojim se neposredno vrši istraga jer mora služiti kao dokaz, te zbog toga niti jedan podatak na njemu ne smije biti izmijenjen, a što nažalost uvijek nije moguće izvesti (npr. zbog zloporabe Interneta rijetko se kao dokaz izuzima server na kojem osim relevantnog i za istragu interesantnog sadržaja postoji još mnogo irelevantnih sadržaja, ali se izuzimaju određeni podaci i pohranjuju na siguran medij).

Vjerodostojna kopija sadržaja

- Kopija podataka koja je načinjena mora biti vjerodostojna da bi uopće mogla biti objekt istrage.
- Ponekad elektronički uređaj nije moguće transportirati u laboratorij pa se kopiranje sadržaja mora obaviti na mjestu počinjenja.
- Nakon što se različitim metodama i postupcima dokaže vjerodostojnost kopije s nje se počinju prikupljati i ispitivati podaci koji se u slijedećoj fazi, tj. fazi analize povezuju da bi ispričali priču o prekršaju, zloporabi, tijeku događanja, zločinu.

Evidencija događanja

- Tijekom cjelokupnog procesa, najprije istrage, pa preko pretrage i analize svatko od sudionika treba detaljno zabilježiti radnje koje je obavio.
- Ponekad treba nekoliko godina da slučaj dođe na sud, a u tom vremenu forenzički stručnjaci mogu obaviti stotine novih pretraga i zaboraviti detalje o prvoj istrazi/pretragi. Upravo tu, glavnu će ulogu odigrati detaljno izvješće koje sadržava:
  - tko je sudjelovao u istrazi,
  - kada je ona obavljena,
  - kojim metodama su podaci obrađeni,
  - što je korišteno od hardverskih i softverskih alata,
  - kako prema sakupljenim dokazima izgleda rekonstrukcija kriminalne radnje,
  - te tko je i kada u međuvremenu imao pristup dokazima.

Pristup prezentiranju rezultata pretrage

- Na posljetku, kada slučaj dođe na rapravu (sud, disciplinska komisija i sl.), rezultati istrage se prezentiraju odvjetnicima, sucima i sucima porotnicima (Nalaz i mišljenje sudskog vještaka).
- Izuzetno je važno da forenzički stručnjak na jednostavan način prezentira rezultate kako bi ga svi sudionici mogli razumjeti jer njegova uloga može biti ključna u rješavanju počinjene kriminalne radnje.

Protokoli postupanja

- Tradicionalna računalna forenzika odvija se u četiri faze:
  - Prikupljanje informacija, podataka, materijalnih dokaza
  - Pretraživanje/pregled relevantnih podataka
  - Analiza usmjerena na davanje odgovora na izravni nalog za vještačenje/ekspertizu
  - Prezentacija dobivenih rezultata analize i davanje osobnog mišljenja

Prikupljanje podataka

Prikupljanje podataka

- dolazak na mjesto počinjenja (vrlo često pod nadzorom suca zaduženog za osiguranje dokaza)
- dokumentiranje (uz dopuštenje suca, naručioca)
  - *zapisnik*
  - *fotografija i videozapisi*
  - *snimanje zvuka (diktafon)*
- upoznavanje s dokaznim materijalom
  - *stanje računala (prije isključenja, isključeno, nakon uključenja)*
  - *operacijski sustav i instalirani softver*
  - *hardver*

Dolazak na mjesto počinjenja

- Kada forenzički stručnjak dođe na mjesto počinjenja, odmah mora započeti sa dokumentiranjem.
- Dokumentiranje je pisanje natuknica, a uz dopuštenje naručioca ekspertize ili dežurnog suca i fotografiranje zatečenog stanja te snimanje razgovora diktafonom ili sličnim uređajima.
- Najprije treba utvrditi jeli računalo uključeno, te ukoliko je obavezno ga ostaviti u tom stanju dok se ne uvjerite da isključivanje koje uzrokuje izmjenu nekoliko stotina datoteka na koje djeluje operacijski sustav prilikom gašenja računala neće stvoriti štetu, tj. da se neće izgubiti relevantne informacije.
- Važno je uočiti i zapisati pod kojim operacijskim sustavom računalo radi, te kojom je vrstom hardvera opremljeno.

Prikupljanje podataka

- stvaranje forenzičke kopije tvrdog diska pretraživanog računala
  - *forenzičko čišćenje odredišnog diska*
  - *spajanje diskova na uređaj za snimanje*
    - *IDE kabel*
    - *crossover kabel*
  - *kopiranje*
  - *utvrđivanje autentičnosti dobivene kopije*

Stvaranje forenzičke kopije diska

- Sljedeći veoma važan korak je izrada kopije diska koja se još naziva **forenzička kopija diska** (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 prethodno bili "trajno"izbrisani.
- Kopiju treba načiniti na vlastiti nezavisni medij koji prije kopiranja mora biti potpuno prazan ("čist").
- Obično formatiranje diska ne osigurava “čisti” disk jer ono ne odstranjuje sve podatke s medija. Forenzička metoda formatiranja sastoji se u ispisivanju serija nula koje će ispuniti svaki sektor diska i tako ga u potpunosti "očistiti".

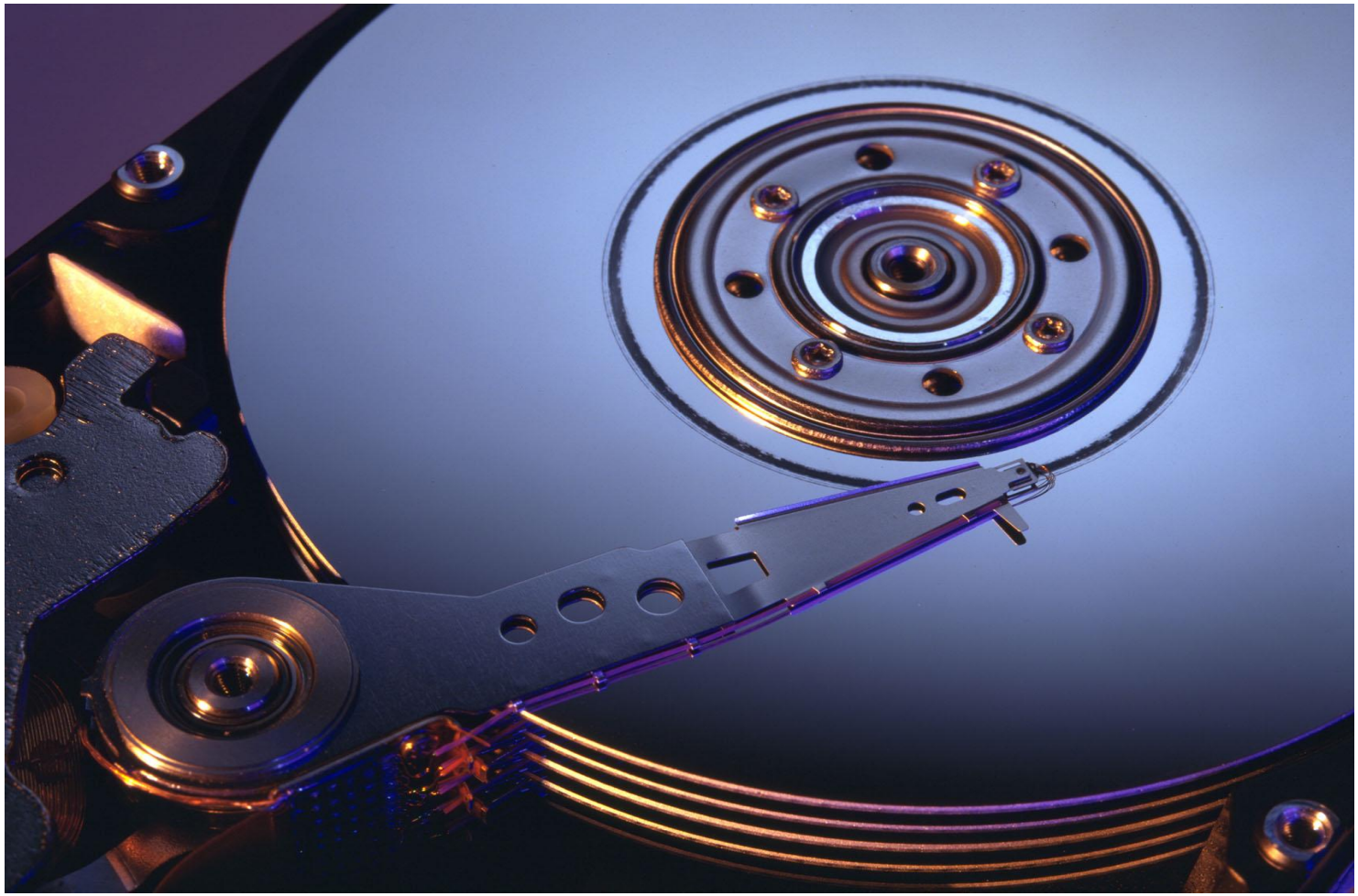
Kako načiniti kopiranje diska

- Kopiranje na disk može se izvršiti na nekoliko načina:
- Predmetni disk se može fizički odspojiti i prespojiti na radno računalo preko IDE kabela ili se mogu spojiti dva računala pomoću crossover kabela.
- Ukoliko se disk prespaja preko IDE kabela neophodno je blokirati pisanje po izvornom disku jer je pod nekim operacijskim sustavima (npr. Windows) disk definiran i za čitanje i za pisanje, a to bi moglo izmijeniti njegov trenutni sadržaj.

Što kada se disk ne može izuzeti

- 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 koji poduzmemo mijenja više od nekoliko stvari u sustavu.
- Budući da u takvom okruženju izmjene ne možemo spriječiti važno je svesti ih na minimum i to tako da se koraci pretraživanja sustava provode prema unaprijed određenom planu.

Pretraživanje podataka



Pretraživanje (1)

- hash analiza (hash analysis)
- potpis datoteke (file signature)
- pretraga po ključnoj riječi
- pretraga po tipu, veličini, datumu nastanka ili zadnje promjene
- zamjenska datoteka (swap)
- kanta za otpatke (Recycle Bin)
- obrisane datoteke (undelete)

Pretraga kopije tvrdog diska

- Nakon što su prikupljene osnovne informacije o predmetu pretrage, disk se “podiže” na testnom računalu samo za čitanje i pretraga može započeti.
- Kako će pretraga započeti ovisi o vrsti slučaja na kojem se radi. Na primjer:
  - da bi se pronašli dokazi o pedofilskim sklonostima korisnika računala logično je započeti pretragom svih fotografija i video zapisa.
  - za dokazivanje zlouporabe podataka neke korporacije, pretraga će biti usmjerena između ostalog i na pretraživanje e-pošte.
- Jednostavni slučajevi u kojima se točno zna što se traži oduzet će malo vremena, možda tek pola dana, dok će složeniji slučajevi u kojima treba kombinirati nekoliko diskova i za koje se ne zna točno što se traži oduzimaju mnogo više vremena.
- Veoma je važno efikasno iskoristiti vrijeme, jer ponekad sudski proces kreće prije no što je istraga zaključena, pa je za početak dobar korak eliminirati datoteke poput explore.exe, iexplore.exe, winword.exe i sl. za koje se zna da nisu potencijalni dokazi.

Izdvajanje podataka hash analizom

- Izdvajanje podataka može se, na primjer započeti sa **hash analizom** (hash analysis).
- Recimo da je disk koji se pregledava jedan od diskova iz velike tvrtke u kojoj se dogodilo curenje informacija. Vlasnici sumnjaju da je zaposlenik dao neke važne informacije konkurentskoj tvrtci. Tvrtka forenzičkom timu daje sve kritične podatke za koje se boje da su mogli biti proslijeđeni te ih oni pomoću hash algoritma uspoređuju sa podacima na disku. Pronađe li algoritam podudarne datoteke, ispisat će ih na ekranu računala. Na taj način radi velika većina forenzičkog softvera koji obrađuje podatke hash analizom.

Provjera potpisa datoteke

- Slijedeće što se može učiniti je provjeriti **potpis datoteke** (file signature) uobičajeno pomoću hex editora.
- Svaka datoteka ima svoj potpis i on govori u kojem je softverskom alatu datoteka nastala. Ova metoda veoma je korisna kada želimo provjeriti da li je korisnik računala promijenio ime i ekstenziju datoteke kako bi prikrio njezin pravi sadržaj.
- Datoteku u `.jpg` formatu (npr. *sexy_lady.jpg*) korisnik veoma lagano može preimenovati u `.doc` format (npr. `domaća zadaća.doc`). Obični korisnik nikada neće primijetiti da je to zapravo fotografija jer će Word svakoj `.doc` datoteci rado dodijeliti Word ikonu.
- Forenzički će stručnjak datoteku provesti kroz hex editor i ukoliko se pokaže da trenutna ekstenzija ne odgovara njezinom stvarnom formatu, datoteka ide na detaljniju analizu.

Pretraga prema ključnoj riječi

- Pretraga se može nastaviti **prema ključnoj riječi** (keyword analysis).
- Stvara se `.txt` datoteka i u nju se upisuju ključne riječi.
- Pomoću određenih alata moguće je pronaći sva pojavljivanja riječi iz naše datoteke te na taj način izdvojiti datoteke koje nas sadržajno zanimaju.
- Ukoliko se zna što se otprilike traži moguće je datoteku izdvojiti i po određenim specifikacijama kao što su npr. **tip, veličina i datum nastanka datoteke**.
- Nakon što se izdvoje sve datoteke koje su bile dostupne čak i običnom korisniku, kreće se na pregledavanje izbrisanih podataka, zamjenske datoteke (swap file), neiskorištenih dijelova klastera na disku.

Zamjenske (swap) datoteke

- Nakon što smo izdvojili sve datoteke koje su bile dostupne čak i običnom korisniku, kreće se na pregledavanje izbrisanih podataka, zamjenskih datoteka (swap file), neiskorištenih dijelova klastera na disku.
- **Zamjenska datoteka** (swap file) je binarna datoteka koja predstavlja virtualnu memoriju u koju 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 čak i podatke koji su forenzički izbrisani s diska, pa je stoga veoma koristan izvor informacija.

“Kanta za smeće” – Recycle Bin

- Sljedeće mjesto na kojemu možemo tražiti dokaze je “**kanta za smeće”** (Recycle Bin).
- Netko je možda u strahu pokušao prikriti dokaze i odlučio ih izbrisati, no obrisani podaci najprije završavaju tamo, a otkuda mogu veoma lako biti vraćeni na mjesto gdje su izvorno stajali.
- Ukoliko je korisnik malo informiraniji, izbrisati će podatke i iz kante za otpatke. No, i tada je moguće rekonstruirati podatke, jer se datoteke ne brišu s diska u potpunosti.
- Operacijski sustav u tablici datoteka samo obilježi prostor koji su one zauzimale kao slobodan i tek kada mu taj prostor bude trebao za nove podatke, preko njih će prepisati novi sadržaj preko starog. To znači da će još neko vrijeme obrisane datoteke biti na disku, baš kao i njihovi metapodaci (podaci o podacima): ime, vrijeme nastajanja, vrijeme izmjene, autor i sl.

Pretraživanje (2)

- neiskorišteni prostor u klasteru na tvrdom disku (slack space)
- privremene datoteke (temporary files)
- elektronička pošta (e-mail)
- web pošta (web-mail)
- "kolačići" (cookies)
- datoteke zapisa (log files)

Neiskorišteni prostor prostor na tvrdom disku (slack space)

- **Slack space** je zanimljiv fenomen koji postoji na disku, a koji nam može u nekim slučajevima pružiti korisne dokaze.
- Najmanja podatkovna jedinka na disku naziva se klaster. Zamislimo da je on veličine 32.000 bajta, a mi trebamo spremiti datoteku veličine 20 bajta. Budući da je klaster najmanja veličina prostora koju je moguće rezervirati za određenu datoteku to znači da će 31.980 bajta klastera ostati potpuno neiskorišteno. Prisjetimo li se činjenice iz prethodnog odlomka, a ta je da obrisani podaci ostaju na disku dok ih ne prepišemo drugima, znači da će neiskorišteni dio klastera biti bogat dokazima.

Privremene (temporary) datoteke

- Bitni dokazi mogu biti pronađeni i u **privremenim datotekama** (temporary files).
- Razne aplikacije prilikom korištenja stvaraju takve datoteke, koje bi trebale nakon po završetka rada biti automatski obrisane, ali …
- Microsoft Word će na primjer stvoriti takvu datoteku svaki puta kada snimimo načinjene izmjene na njoj.
- To znači da će forenzički stručnjak vidjeti kada i kako se mijenjao dokument i na taj način imati gotovu priču o nastajanju određene datoteke, s obzirom na to da izbrisane datoteke ne nestaju odmah s diska.

Korištenje e-pošte

- Sljedeće mjesto gdje se mogu tražiti dokazi je sandučić **e-pošte** (e-mail).
- Pregleda li se sadržaj sandučića može se utvrditi s kime je i kada osoba komunicirala te kakve su podatke izmijenili.
- Ponekad se korisnici služe **web-poštom** (webmail), pa se prilikom skidanja pošte s Interneta poruke spremaju u **privremene internet datoteke** (temporary Internet files).
- Budući da se tu spremaju i različite druge aktivnosti vezane za korištenje interneta, moguće je pronaći i podatke poput:
  - koje je web-stranice korisnik posjećivao,
  - kojeg datuma je to bilo,
  - koliko često odlazi tamo,
  - što je skidao s Interneta i sl.

“Kolačići” - Cookies

- Podaci koji su također vezani uz Internet aktivnost, a mogu biti od velike koristi su “kolačići” (**cookies)**. To su informacije koje server šalje web pregledniku, a koje preglednik neizmijenjene vraća svaki puta kada pristupi tom serveru.
- Spremaju se na računalo u obliku tekstualnih datoteka i služe kako bi korisniku optimizirali pristup informacijama na Internetu.
- Njihova primjena je veoma široka:
  - Omogućavaju korisniku online kupovinu, točnije omogućavaju mu spremanje i vađenje proizvoda u i iz virtualne košarice.
  - Omogućavaju mu prijavljivanje na razne web stranice, tako što pamte da je on već autorizirani korisnik te ne traže ponovno upisivanje korisničkog imena i lozinke.
  - Pomoću cookie-ja je moguće pratiti i koje stranice korisnik posjećuje.

Log datoteke

- Izuzetno važan izvor forenzičkih dokaza mogu biti **datoteke zapisa** (log files) nekog servera.
- One mogu sadržavati informacije o raznim sistemskim sredstvima, procesima i aktivnostima od strane korisnika.
- Ukoliko administrator sustava ne omogući evidentiranje aktivnosti na mreži, moguće je da neće postojati dokazi potrebni da se počinitelj zločina poveže sa incidentom.
- Nažalost, iskusni kriminalci znaju da je jedno od prvih pravila pri upadu u sustav obrisati ili modificirati datoteku zapisa tako da njihova aktivnost na sustavu ne bude zabilježena.

Analiza

Analiza

- Analiza je proces tumačenja dokaza prikupljenih tokom procesa pretraživanja podataka.

- vrste analize:
  - *vremenska analiza*
  - *analiza skrivenih podataka*
  - *analiza datoteka i aplikacija*

Vremenska analiza

- Vremenska analiza određuje kada se određeni događaj zbio, te tako stvara sliku o razvoju nedozvoljenih radnji korak po korak.
- Moguće ju je provesti pregledavajući:
  - vremenske metapodatke (posljednja izmjena, posljednji pristup, vrijeme nastanka, promjena statusa …) ili
  - datoteke zapis**a** (evidencija pogreški, evidencija instalacija, evidencija prijava na sustav…).
- Pomoću vremenskih metapodataka može se na primjer saznati kada je datoteka zadnji puta izmijenjena, a iz dnevničke datoteke može se saznati kada se korisnik sa svojom kombinacijom korisničkog imena i lozinke prijavljivao na sustav.

Analiza skrivenih podataka

- Ova analiza korisna je u rekonstrukciji skrivenih podataka, te može ukazati na vlasništvo, vještinu ili namjeru.
- Ukoliko su pretraživanjem pronađeni podaci koji imaju izmijenjenu ekstenziju, to odmah upućuje na namjerno skrivanje podataka.
- Pronalazak šifriranih te komprimiranih informacija zaštićenih lozinkama upućuje na skrivanje podataka od neautoriziranih korisnika, ali može ukazivati i na zaštitu korisnika računala od moguće pretrage računala u svrhu pronalaženja dokaza.

Analiza datoteka i aplikacija

- Analiziranjem datoteka i aplikacija može se izvesti zaključak o sposobnosti sustava i vještini korisnika. Rezultati ove analize mogu uvjetovati sljedeće mjere koje moraju biti poduzete da bi se analiza izvršila do kraja:
  - pregledavanje sadržaja datoteka
  - korelacija podataka s aplikacijama
  - identificiranje serijskog broja i vrste operacijskih sustava
  - utvrđivanje povezanosti između datoteka (pr. veza između privremenih internet datoteka i cookie-a, te sadržaja e-pošte i privitka)
  - pregledavanje standardnog korisnikovog spremnika podataka te utvrđivanje da li su podaci spremljeni tu ili na nekom drugom mjestu
  - pregledavanje korisničkih postavki

Prezentacija rezultata

Prezentacija rezultata

- rezultati istrage prezentiraju se onome tko je pretragu zatražio i to na primjeren način
- u sudskom procesu forenzički stručnjak (stalni sudski vještak, ekspert) postaje svjedok
- bez obzira tko je Nalaz i mišljenje zatražio forenzički stručnjak mora na jednostavan način obrazložiti rezultate istrage vodeći računa o tome da se isti mogu ponoviti ili da netko drugi može doći do istih zaključaka

Izvješće

- Izvješće predstavlja sjedinjenje prikupljene dokumentacije, utvrđenih dokaza i rezultata provedene analize.
- Izvješće treba sadržavati vrijeme i datum analize i detaljno opisane rezultate, a treba biti pisan jednostavno kako bi bio razumljiv godinama kasnije.
- On je najvažnija faza digitalne forenzike, pa ako je nepotpun ili ne prati pomno dokumentaciju alata, procesa i metodologije, sav posao učinjen je nizašto.
- Složenost izvještaja ovisi o njegovoj namjeni, no u većini slučaja minimum koji mora biti ostvaren je dokumentacija o pregledavanom objektu, upotrijebljeni alati i činjenični nalazi.
- Ponekad se izvještaj osim za sud izrađuje i za potrebe pojedinih pravnih subjekata (procjena kvalitete izvedbe i vrijednosti softvera, procjena stupnja dovršenosti, procjena mogućih štetnih učinaka korištenja, utvrđivanje opsega plagiranja nečijeg softvera i sl.)

Prezentacija rezultata istrage

- Jednom kada je cijela istraga zaključena i slučaj ode na sud, rezultati istrage koju je proveo forenzičar trebaju osim u pisanom obliku biti prezentirani odvjetnicima, sucu i poroti i usmeno (ispitivanje svjedoka).
- Forenzički stručnjak mora biti u stanju na jednostavan način obrazložiti dobivene rezultate, a nerijetko odvjetnici, suci i porota prolaze osnovne tečajeve računalne forenzike kako bi što kvalitetnije mogli sudjelovati u sudskom procesu i postavljati forenzičaru suvisla pitanja.

Nalaz i mišljenje

- Krajnji korak provedenog prikupljanja informacija i obavljene analize je dokument koji se obično naziva Nalaz i mišljenje vještaka čiji je važni dio jasno napisan zaključak u kojemu se povezuju do sada prikupljeni i analizirani podaci u cjelovitu priču.
- sadržaj Nalaza i mišljenja
  - *prikupljena dokumentacija*
  - *popis dokaza*
  - *rezultati analize*
- složenost izvještaja
  - *Nalaz i mišljenje koje je svojim nalogom zatražio sud*
  - *eventualno posebni izvještaj za tvrtku*

Forenzički softverski alati

- Nakon što je obavljena istraga i nakon što su predstavljeni njezini rezultati, dokazi postaju subjekt temeljitog proučavanja u sudnici.
- Kako bi se osigurala pravovaljanost dokaza razvijeno je mnoštvo softverskih alata koji pomažu forenzičkim stručnjacima u pregledavanju, pretraživanju i analizi dokaza.
- Ugled pojedinih proizvođača forenzičkog sofvera može dodatno pojačati dokaznu snagu prezentiranog Nalaza, te se preporuča koristiti autorizirane inačice softvera čija se licenca onda spominje i u Nalazu.

Softver za manipulaciju diskom

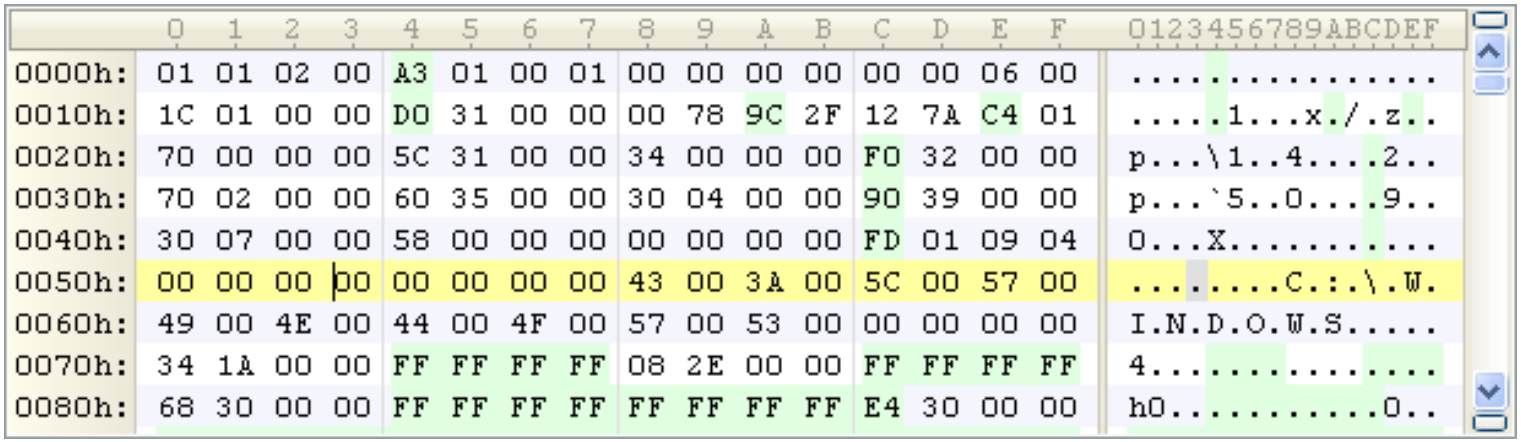
- **PDBlock** – softver tvrtke Digital Intelligence koji sprečava pisanje po izvornom disku prilikom forenzičkog kopiranja diska
- **DriveSpy** – softverski alat tvrtke Digital Intelligence baziran na DOS-u, sa sučeljem sličnim istom, a koji omogućava stvaranje forenzičke kopije diska, obnavljanje obrisanih podataka, neiskorištenih dijelova sektora, hash analizu
- **Forensic Replicator** – softver tvrtke Parben Forensics Tools za forenzičko kopiranje različitih medija
- **FTK Imager** – softver tvrtke AccessData Corporation za forenzičko kopiranje
- **DiskSig** – softver tvrtke NTI koji služi za provjeru autentičnosti forenzičke kopije diska
- **SnapBack® Exact** – softver tvrtke SnapBack koji služi za forenzičko kopiranje diska
- **GetFree** – softver tvrtke NTI koji služi za kopiranje svog oslobođenog prostora diska, spremanje tih podataka na drugi medij te njihovu analizu
- **GetSlack** – softver tvrtke NTI koji radi na istom principu kao GetFree, samo što kopira slack space

Softver za obnavljanje podataka

- **Ontrack** – softver za obnavljanje podataka izbrisanih sa diska
- **AcoDisk** – softver za obnavljanje podataka sa CD-a
- **MediaMerge for PC** – softver tvrtke Computer Conversions koji služi za obnavljanje podataka s optičkih, tvrdih diskova, CD-a

Softver za pregled binarnih datoteka

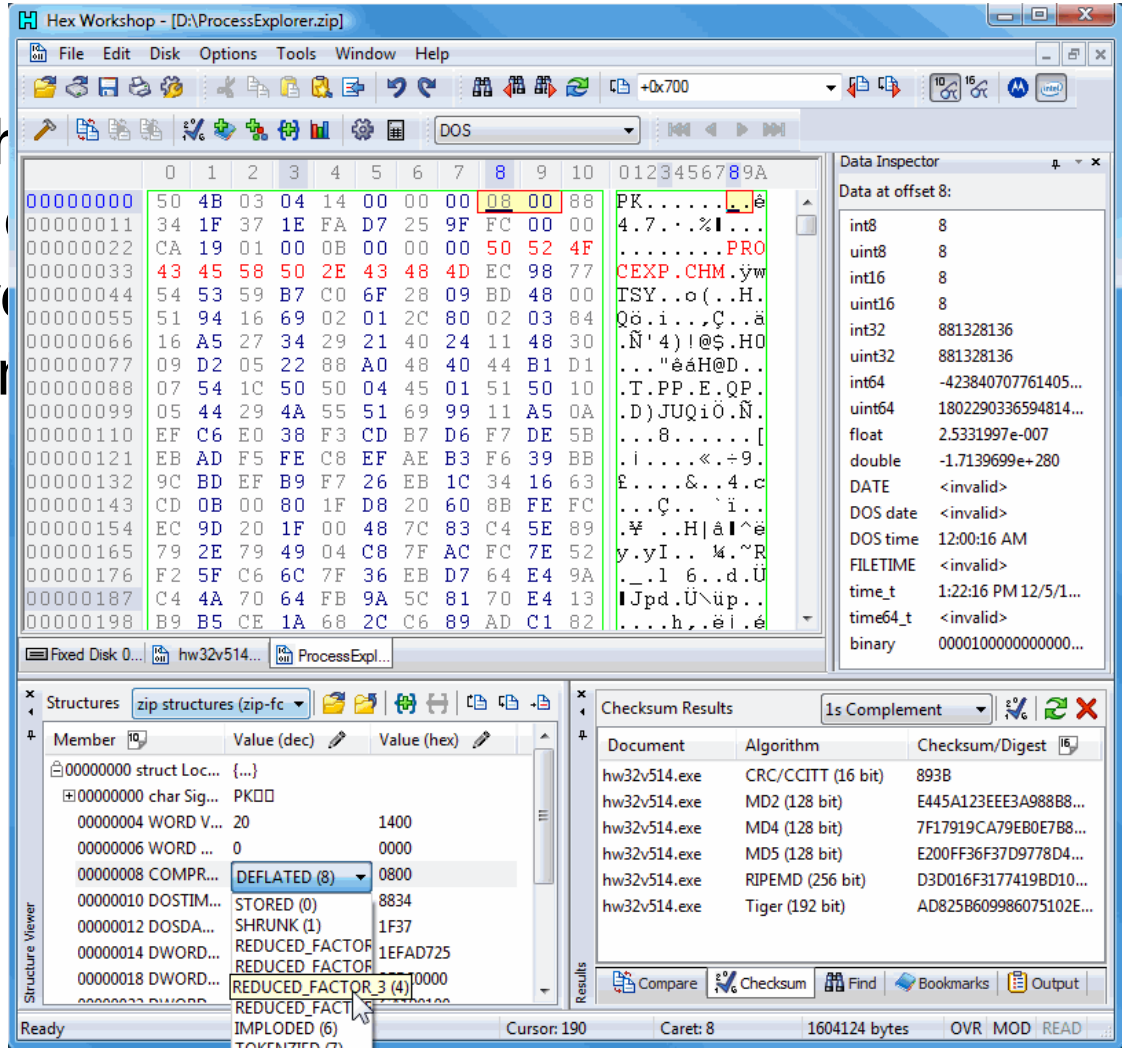
- **010 Hex editor** – softver tvrtke SweetScape koji služi za pregledavanje binarnih datoteka



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	01	01	02	00	A3	01	00	01	00	00	00	00	00	00	06	00	.....
0010h:	1C	01	00	00	D0	31	00	00	00	78	9C	2F	12	7A	C4	01	.....1...x./.z..
0020h:	70	00	00	00	5C	31	00	00	34	00	00	00	F0	32	00	00	p...\1..4....2..
0030h:	70	02	00	00	60	35	00	00	30	04	00	00	90	39	00	00	p...`5..0....9..
0040h:	30	07	00	00	58	00	00	00	00	00	00	00	FD	01	09	04	0...X.....
0050h:	00	00	00	00	00	00	00	00	43	00	3A	00	5C	00	57	00	....C.:.\.W.
0060h:	49	00	4E	00	44	00	4F	00	57	00	53	00	00	00	00	00	I.N.D.O.W.S.....
0070h:	34	1A	00	00	FF	FF	FF	FF	08	2E	00	00	FF	FF	FF	FF	4.....
0080h:	68	30	00	00	FF	FF	FF	FF	FF	FF	FF	FF	E4	30	00	00	h0.....0..

Softver za pregled binarnih datoteka

- **Hex Worksh**
  služi za pregl
  nad njima, pr
  sustavom Wi



Višenamjenski forenzički softver

- **EnCase** – proizvodna linija tvrtke Guidance Software, jedna od najpotpunijih forenzičkih softverskih alata
- **Maresware** - softverski alat tvrtke Mares and Company koji je kolekcija korisnih alata za forenziku na mjestu zločina
- *Access Data*
- *ASR*
- *Digital Intelligence*

Ostali forenzički softver

- softver za hash analizu
  - *Drive Spy (Digital Intelligence)*
  - **Hash, Crckit, Discat** – softver tvrtke Mares and Company
- ostalo
  - **DtSearch** – tvrtka koja ima cijelu liniju softverskih alata za pretraživanje podataka pomoću ključnih riječi
  - **Net Treat Analyzer** – softverski alat za identifikaciju Internet aktivnosti i pregledavanje zamjenskih datoteka

Hardverski alati

- Softverski alati moraju biti pokrenuti na određenom hardveru. lako dio njih može biti pokrenut na osobnim računalima, većina zahtjeva snažniju i kompleksniju hardversku podlogu koja će isto tako omogućavati i priključivanje hardvera koji je dio dokaznog materijala.
- Postoje razni opskrbljivači forenzičke hardverske opreme, no jedni od najvažnijih su:
  - Digital Intelligence (http://www.digitalintelligence.com/)
  - Vogon International (http://www.vogon-investigation.com/index.htm)

- *forenzički sustavi*
- *hardver za prikupljanje podataka*
- *prijenosni hardver*
- *hardver za obradu CD-a i DVD-a*
- *blokeri*
- *hardver za dupliciranje podataka*

- prijenosni i laboratorijski **forenzički sustavi**
- prijenosni i laboratorijski **hardver za forenzičko kopiranje**
- prijenosne i laboratorijske **radne stanice**

Zaključak

- razvoj tehnologije →
  - *porast kompjuterskih zločina*
  - *porast potrebe za osiguravanjem sustava*
  - *porast potražnje za forenzičkim stručnjacima*
  - *potreba za širenjem i usavršavanjem računalne forenzike*

Zaključno

- Razvojem tehnologije porastao je broj kompjuterskih zločina. Izvjesno je da će se taj trend nastaviti s obzirom na tehnologiju koja se i dalje razvija. Više zapravo i nije pitanje da li ćemo postati žrtve kompjuterskog zločina, već kada ćemo to postati. Stoga je neizmjerno važno da forenzički stručnjaci i provoditelji zakona postupaju sa digitalnim dokazima s osobitom pažnjom, te ih predstave temeljito.
- Danas već mnoge agencije pružaju izobrazbu o prikupljanju, ispitivanju i korištenju digitalnih dokaza. Uskoro će biti potrebno ne samo to, nego i šire profesionalno obrazovanje u polju računalne forenzike, jer će zajedno s napretkom tehnologije i porastom kriminala rasti potreba za osiguravanjem podataka i rješavanjem kompjuterskih zločina. U želji za podizanjem razine sigurnosti naših sustava, računalna će forenzika proširiti svoje granice.

Oprez kod korištenja softverskih alata

- Iako postoji mnoštvo alata za prikupljanje i analizu dokaza, bez stručnog nadzora mnoge stvari mogu poći krivo i uništiti dokaze, a samim time i slučaj.
- Stoga valja naglasiti da forenzičku istragu ne može provesti bilo tko služeći se putem interneta dostupnim alatima, nego nju može kvalitetno i pravovaljano voditi jednino forenzički stručnjak.
- za privatnu uporabu u funkciji održavanja vlastitog računarskog sustava se, naravno, treba poticati korištenje raznih programskih alata, kako onih "free ware" tako i onih koji uz malu naknadu ("share ware" mogu u potpunosti zadovoljiti potrebe vlasnika računala u njihovoj potrazi za izgubljenim datotekama, e-poštom i sl.

Literatura (1)

- Reyes, A. Cyber Crime Investigations: Digital Forensics and Analysing Data. Rockland: Syngress Publishing Inc., 2007.
- Schweitzer, D. Incident Reponse: Procedures for Collectiong and Preserving Evidence. Indianapolis: Wiley Publishing Inc., 2003.
- Solomon, M. G. Computer Forensics Jump Start™. Alameda: SYBEX Inc., 2005
- Ashcroft, J. Forensic Examination of Digital Evidence: A Guide for Law Inforcement. Special Report. U.S. Department of Justice, 2004.
- Craiger, J.P. Computer Forensics Procedures and Methods. Scientific paper. Nacional Center for Forensic Science & Demartment of Engineering Technology University of Central Florida, 2004.

Literatura (2)

- Oseles, L. Computer Forensics: The Key to Solving the Crime. Scientific paper., 2001.
- ComputerForensics.pdf, 2006., *An Introduction to Computer Forensics*, http://www.dns.co.uk/NR/rdonlyres/5ED1542B-6AB5-4CCE-838D-D5F3A4494F46/0/ComputerForensics.pdf, 23. travanj 2007.
- forensichardware.php, 2007., *Computer Forensics, Forensic Hardware and Software, Computer Investigation*, http://www.vogon-forensic-hardware.com, 5. svibanj 2007.
- computer-forensic-hardware.php, 2007., *Computer Forensic Hardware – Get Digital and Forensic Hardware from H-11*, http://www.h11-digital-forensics.com/computer-forensic-hardware.php, 4. svibanj 2007.

web literatura

- Branimir Radić: Osnove računalne forenzike (http://sistemac.srce.hr/fileadmin/user_root/seminari/Srce-Sys-Seminari-Osnove_racunalne_forenzike.pdf
- Carnet: Osnove računalne forenzičke analize (http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2006-11-174.pdf