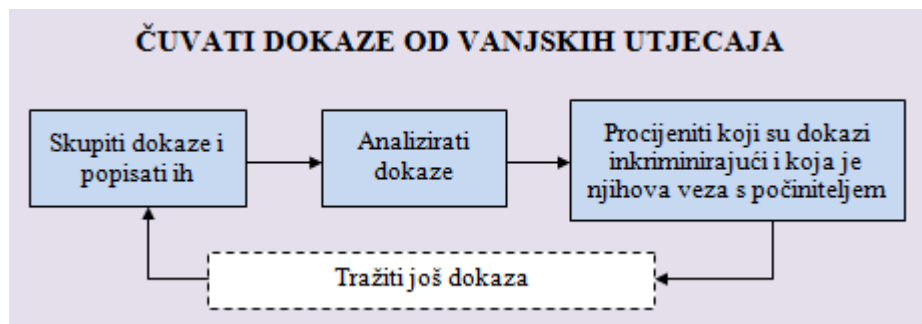
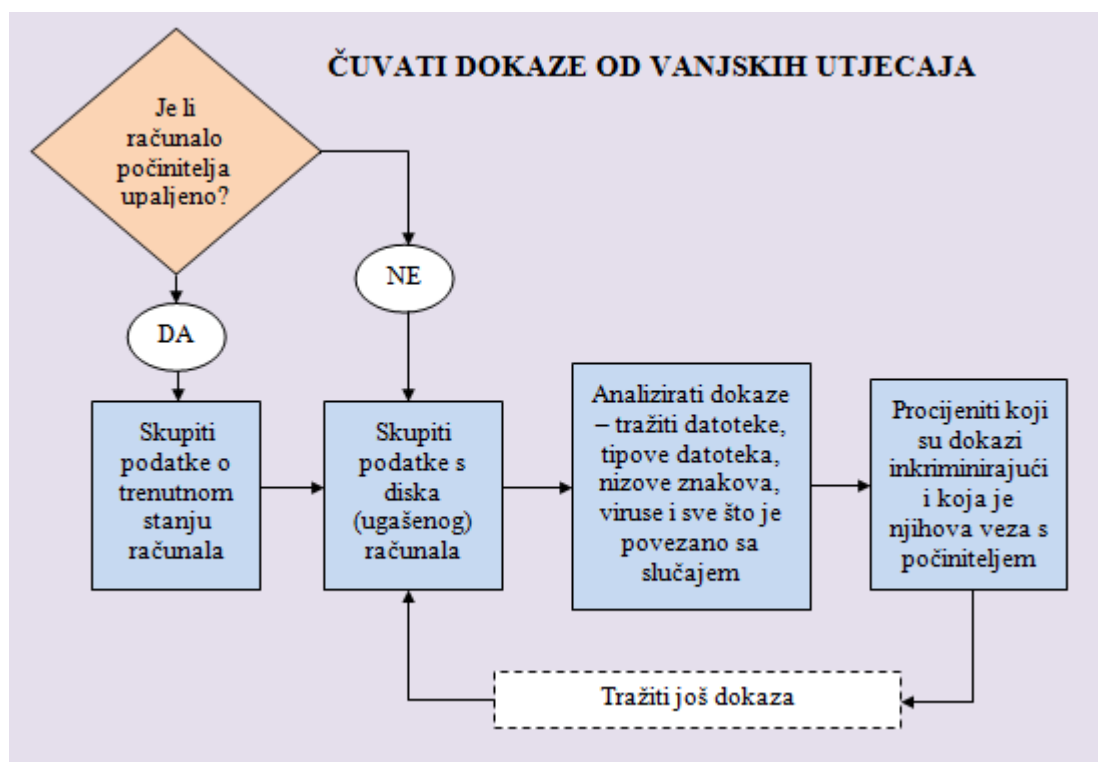


Tijek forenzičke istrage

Tijekom forenzičke istrage bitno se pridržavati određenih koraka. Oni nisu zakonski obvezujući već su oblikovani na temelju dugogodišnjeg iskustva forenzičkih istražitelja s ciljem da se smanji mogućnost previđanja bitnih detalja koji bi mogli utjecati na konačni ishod istrage. Slijedeća slika prikazuje dijagram forenzičkih postupaka. Riječ je o standardnom procesu primjenjivom u svim vrstama istraga, pa tako i u istragama računalnih zločina.



Kad se koraci forenzičkih procesa prilagode računalima, gornji dijagram dobiva novi oblik (slika ispod). Ono što je bitno kod analize računala je da se puno dokaza može skupiti dok je računalo još upaljeno. Istražitelj ima samo jednu priliku za to jer se svakom dodatnom radnjom (npr. pokretanjem neke aplikacije, otvaranjem web preglednika, ...), kao i gašenjem računala uništavaju podaci iz radne memorije računala. Računalo se stoga mora ostaviti upaljeno dok se ne kopiraju svi podaci iz radne memorije.



Koraci navedeni u gornjim dijagramima su okvirni i mogu se razlikovati od istrage do istrage.

Tipovi podataka

Standardna forenzička analiza računala uključuje pregledavanje materijala na medijima (tvrdi disk, USB diskovi, CD diskovi, DVD diskovi, ...), pregledavanje Windows registra (za računala s Microsoft Windows operacijskim sustavom), otkrivanje lozinki (npr. za pristup računu e-pošte ili forumima i sličnim stranicama koje mogu otkriti nešto o korisnikovim navikama), pretraga po ključnim riječima, izdvajanje e-pošte i slika za pregled. Podaci na računalu mogu se s obzirom na vidljivost podijeliti u dvije skupine:

Vidljivi

- dokumenti, datoteke koje sadrže sliku programa ili operacijskog sustava (eng. *image files*), e-mail poruke, proračunske tablice (eng. *spreadsheets*),
- programi i aplikacije,
- poveznicičke datoteke (eng. *link files*) te
- dnevničke datoteke (eng. *log files*).

Nevidljivi

- izbrisane datoteke (dokumenti, *image* datoteke, e-mail poruke, proračunske tablice i sl.),
- namjerno skrivene (eng. *hidden*) datoteke i mape,
- zastarjeli sistemski podaci (eng. *file system artifacts*),
- povijest pregledavanja Internet stranica (eng. *history*),
- ispisivani dokumenti,
- radna memorija (RAM),
- zaštićena područja pohrane (npr. gdje se čuvaju brojevi kreditnih kartica uneseni u web preglednike),
- područja u memoriji računala iz kojih operacijski sustav ne čita podatke kao datoteke već kao naredbe sustava (osobe koje su ih tamo pohranile alatom poput [heksadecimalnog uređivača](#), znaju što traže, ali drugima to može predstavljati traženje igle u plastu sijena) te
- sistemski zapisnici (eng. *system log files*).

Dok neke od ovih podataka korisnik stvara vlastitom voljom, većina ih ipak nastaje zbog korisnikovih radnji, ali bez njegove suradnje.

Alati forenzičke istrage

Prilikom pristupa računalu koje je predmet istrage, svaki računalni forenzičar bi trebao sa sobom imati barem osnovni alat koji će mu pomoći u skupljanju dokaza. Tu se ubrajaju:

- forenzički programi s raznim funkcijama,
- digitalna kamera,
- USB uređaj od barem 4 GB memorije za pohranjivanje manjih komada dokaza,
- tvrdi disk (500 GB je dovoljno za većinu slučajeva) za pohranjivanje dokazne kopije cijelog diska,
- računalo za analizu (laptop), s uvjetom da ne sadrži bilo kakve maliciozne programe kako ne bi

ugrozilo dokaze (čak i ako se dokazi nisu oštetili, činjenica da je forenzičko računalo bilo ranjivo može rezultirati odbacivanjem dokaza na sudu),

- bilježnica i kemijska olovka za uzimanje bilješki o mjestu zločina i stanju računala ,
- program za pregledavanje preuzete slike sustava (eng. *mounting*),
- *Antivirus/Antispyware/Rootkit detector* programi na forenzičkom računalu.

Skupljanje dokaza

1. Ako je računalo upaljeno

- Napraviti sliku radne (RAM) memorije i pohraniti je na pripremljeni tvrdi ili USB disk za pohranjivanje dokaza. Napraviti **MD5/SHA1** sažetak (eng. *hash*) image datoteke, sačuvati je na disku i zapisati u bilježnicu.
- Popisati sve procese, mrežne veze, instalirane programe i sklopovlje. Sačuvati podatke u datoteci na dokaznom disku. Napraviti **MD5/SHA1** sažetak datoteke, sačuvati ga i zapisati u bilježnicu.

2. Ako je računalo ugašeno (ili nakon prethodnog koraka)

- Napraviti sliku tvrdog diska i pohraniti je na dokazni tvrdi ili USB disk. Napraviti **MD5/SHA1** sažetak slike, sačuvati ga i zapisati u bilježnicu.
- Fotografirati računalo sa svih strana, slike sačuvati na dokazni disk. Napraviti **MD5/SHA1** sažetke svih fotografija, pohraniti ih na disk i zapisati u bilježnicu.
- Ako su vidljive ikakve fizičke promjene računala ili opreme (npr. u kućište je ugrađen još jedan ventilator za hlađenje ili je zamijenjen jedan zid kućišta i sl.), fotografirati ih zasebno i posavjetovati se s forenzičkim stručnjakom koji će potražiti dodatne tragove (otiske prstiju, tragove alata i sl.).
- Otvoriti kućište računala i fotografirati unutrašnjost pod dobrim osvjetljenjem. Napraviti **MD5/SHA1** sažetke fotografija, pohraniti ih na disk i zapisati u bilježnicu.

Analiza dokaza

- Prenijeti kopije dokaznih datoteka na forenzičko računalo i napraviti još jednu kopiju svih kopija. Potvrditi da imaju isti **MD5/SHA1** sažetak koji je sačuvan na disku i zapisan u bilježnici kako bi se uvjerilo da podaci nisu izmijenjeni na putu od mjesta zločina do laboratorija.
- Pretražiti izvorne slike radne memorije i diska, ako se nađu kakvi znakovni nizovi (eng. *string*) zapisati ih i pohraniti rezultate.
- Pregledati ispis svih nizova (eng. *string dump*), tražiti ključne riječi.
- Ukoliko su nađene ključne riječi koje se tiču istrage (npr. "plaća", "lozinka", "bomba"), potražiti te riječi u izvornim image datotekama. Pohraniti rezultate.
- Na forenzičkom računalu pregledati sliku diska uzetu s istraživanog računala (paziti da se datoteka otvori u načinu rada samo za čitanje (eng. *read-only*). Skenirati disk u potrazi za virusima, spyware i rootkit programima. Spremiti rezultate u obliku slike zaslona (eng. *screenshot*) ili log datoteke.
- Analizirati dnevnik događaja (eng. *event log*) računala osumnjičenika i tražiti nepravilnosti. Ako se nađu, pohraniti ih zajedno s vremenima kad su se nepravilnosti dogodile.
- Analizirati dnevnik izvršavanja procesa (eng. *running processes log*) računala osumnjičenika i tražiti sumnjive procese. Ako se nađu, provjeriti ispis sadržaja memorije (eng. *memory dump*) i istražiti proces (pomoću bilo kojeg **heksadecimalnog uređivača**)
- Naći slike, filmove, dokumente, pohranjenu e-poštu i dokumentirati njihove lokacije za kasniji pregled.

- Ako je potrebno, primijeniti programe za detekciju steganografije kako bi se našli skriveni podaci u slikama i glazbenim datotekama.
- Analizirati cookie zapise u web preglednicima kako bi se otkrilo da li je osumnjičenik posjećivao sumnjive ili neke određene stranice.
- Analizirati e-mail poruke.
- Istražiti datoteke u neiskorištenom prostoru na disku (eng. *slack space*). To su datoteke koje su izbrisane iz korisničkog prostora (naredbom delete ili shift+delete), ali su još uvijek fizički zapisane na disku.

Svi inkriminirajući dokazi (ovisno o kontekstu) se moraju zabilježiti i pohraniti zajedno s vremenskim oznakama i pripadajućim prikazima (slike zaslona, ispisi teksta, audio zapisi).

From:

<https://www.cis.hr/WikiS/> - **wikiS**

Permanent link:

https://www.cis.hr/WikiS/doku.php?id=old_zabrisati:istraga_forenzika

Last update: **2015/01/21 13:37**

