Skupljanje dokaza

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,
- povezničke 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.

Redoslijed prikupljanja podataka

Ako je računalo upaljeno

1. 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.

2. 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.

Ako je računalo ugašeno (ili nakon prethodnog koraka)

1. Napraviti sliku tvrdog diska i pohraniti je na dokazni tvrdi ili USB disk. Napraviti [http://en.wikipedia.org/wiki/MD5|MD5]]/SHA1 sažetak slike, sačuvati ga i zapisati u bilježnicu.
2. Fotografirati računalo sa svih strana, slike sačuvati na dokazni disk. Napraviti MD5/SHA1 sažetke svih fotografija, pohraniti ih na disk i zapisati u bilježnicu.
3. 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.).
4. Otvoriti kućište računala i fotografirati unutrašnjost pod dobrim osvjetljenjem. Napraviti MD5/SHA1 sažetke fotografija, pohraniti ih na disk i zapisati u bilježnicu.

Checklista za analizu podataka

- 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).