Standardni zadaci istrage

Poanta računalne forenzike je dolazak do istine. Do istine se dolazi identificiranjem i skupljanjem dostatnih dokaza za dokazivanje identiteta ili aktivnosti računalnog korisnika. Ono što zanima istražitelja su rezultati zabranjenih aktivnosti ili ono što podupire druge zabranjene aktivnosti.
Skoro sve forenzičke istrage imaju zajedničke osnovne korake. Prilikom dolaska na mjesto zločina, potrebno je odrediti sve dokaze koji bi mogli biti bitni. Nakon identifikacije dokaza, potrebno ih je prikupiti i pohraniti na način koji će sačuvati njihovo stanje pri čemu se isprva potrebno prema SVIM dokazima ponašati kao da će biti od važnosti na sudu. Nakon što su dokazi u ovlasti istražitelja, može se započeti s analizom.
Ovo poglavlje predstavlja pregled zadataka zajedničkih svim računalnim istragama.

4 osnovna principa

1. **Minimizirati gubitak podataka**
   Sustav ni u kojem slučaju ne može ostati nepromijenjen u procesu skupljanja podataka. Cilj dobrog istražitelja je da minimizira gubitak i maksimizira količinu prikupljenih podataka.
2. **Bilježiti sve o svemu**
   Istražitelj mora snimati, slikati, zapisivati i bilježiti apsolutno sve svoje postupke i pronađene podatke.
3. **Analizirati sve prikupljene podatke**
   Nakon što je utvrđeno da je stvarno došlo do incidenta, istražitelj treba početi duplicirati sve podatke, počevši od onih najsklonijih izmjenama koji će se izgubiti gašenjem računala.
4. **Izvjestiti o nalazima**
   Izvještaj treba biti jasan i precizan te sadržavati nalaze, zaključke i postupke koji su doveli do zaključka. Izvještaj bi trebao biti jasan i ljudima koji nisu stručnjaci u tom području.

Identificiranje dokaza

Početak posla za istražitelja je skupljanje dokaza. Generalno pravilo je da se sve smatra dokazom. Najbolja opcija bi bila da se uzme sve što zakon i situacija dopušta. Možda važnost nekog podatka isprva nije očita, ali kasnije bi mogao biti presudan.

- **Obratiti pažnju na okolinu.**
  Presudno je uzimati bilješke, fotografirati, skicirati i na sve moguće načine dokumentirati mjesto zločina u što više detalja.

  ```
  Don't get too caught up in finding specific evidence. Rather, treat an investigation like a large puzzle. Avoid fixating on the picture (on the puzzle's box); instead, look at the shapes and how the pieces fit together. When you focus on the end product too much, you can miss important evidence that may lead you in a different direction. Try to avoid looking only for evidence you expect to exist. Be on the lookout for any evidence that would be of interest to your case.
  ```

- **Hardware.**

Osim što pruža mogućnost pronalazaka otisaka prstiju, *hardware* je mjesto gdje će forenzičar tražiti većinu dokaza. Potrebno je obratiti pažnju na sve uređaje na mjestu zločina i pokušati stvoriti realnu sliku o njihovom korištenju. Npr. ako osumnjičeni ima skener priključen na računalo, istražitelj može zaključiti da će na računalu pronaći skenirane dokumente ili slike. Ako ih ne nađe, potrebno je zapitati se gdje bi mogli biti. Pogotovo ako je riječ o skupom skeneru, malo je vjerojatno da ga osumnjičeni nikad nije koristio. Malo više o čestim vrstama hardvera...

```
After you have the proper authorization, you will need to start
cataloging the physical evidence. Different people choose different
starting points. Some examiners start with the most prominent computer,
normally the one in the center of the workspace. Others choose a point
of reference, such as the entry door, as a starting point. Regardless of
where you start, you should move through the scene carefully and
document your actions as you proceed. Start where you are most
comfortable. The goal is to consider all physical evidence. Choosing a
starting point and moving through the scene in a methodical manner makes
it more unlikely that you will miss important evidence.
```

- **Komunikacijske veze.**
  Ako je istraživano računalo spojeno na mrežu, potrebno je obratiti pažnju na druga računala u mreži. Istraga se možda neće trebati proširiti na sva ta računala, ali potrebno je znati za sve mrežne veze.

- **Prijenosni uređaji za pohranu.**
  Prijenosni uređaji, poput USB stickova, su često nalazište dokaza. Potrebno je detaljno pretražiti sve pronađene prijenosne uređaje. Iako taj postupak zna biti dugotrajan i naporan, postoji mogućnost da će se na njima pronaći podaci koji se ne mogu pronaći nigdje drugdje. Korisno je imati na umu za što se najčešće koriste takvi uređaji:
    - arhiviranje podataka/rezervnih kopija,
    - prijenos podataka te
    - instalacija programa.

- **Dokumenti.**
  Hard-copy dokument je bilo što napisano što se može dotaknuti. Dokazi koji se sastoje od dokumenata se zovu dokumentarni dokazi (eng. *documentary evidence*). Podaci pohranjeni u datotekama na računalu se isto tako smatraju dokumentarnim dokazima.

  ```
  The most important characteristic of documentary evidence is that it
  cannot stand on its own. It must be authenticated. When you find
  suspicious files on a hard drive (or removable media), you must prove
  that they are authentic. You must prove that the evidence came from the
  suspect's computer and has not been altered since it was collected.
  ```

  Potrebno je slikati sve ploče za pisanje i ostale pronađene zapise. Svi papiri na mjestu zločina se trebaju smatrati dokazima. Samoljepljivi papirići (eng. *post-its*, *sticky notes*) se često koriste kao podsjetnici za lozinke i slično. Potražiti okolo, ispod i na hardverskim komponentama, kao i u ladicama radnog stola. Zapisani podaci će često usmjeriti istragu brže nego što bi to napravila detaljna pretraga cijelog diska. Podaci koji se često nalaze na “pomoćnim” papirićima su:
    - lozinke,
    - enkripcijski ključevi ili kodovi,
    - URL adrese,

- IP adrese,
- e-mail adrese,
- telefonski brojevi,
- imena,
- (fizičke) adrese,
- imena dokumenata,
- imena mapa na računalu...

Čuvanje dokaza

- **Slika sustava.**
  Kako bi istražitelj mogao “kopati” po podacima na preuzetim medijima, a ipak na sudu mogao dokazati da nije ništa promijenio, potrebno je napraviti “sliku” sustava. To se može postići računanjem *hash* vrijednosti. *Hash* algoritam nepovratno stvara sažetak fiksne duljine (ovisno o tipu algoritma). Ako istražitelj napravi jedan sažetak sustava prije nego što poduzme išta drugo te jedan nakon analize, može dokazati da ništa nije promijenjeno (ako su sažeci jednaki).

- **Write blockers**
  Kako bi spriječio slučajno mijenjanje podataka, istražitelj može koristiti *write-blocking* uređaj prilikom analize sustava. Može birati između softverskog i hardverskog rješenja. Softverski, onemogućava se operacijski sustav od pisanja na medij. Hardverski, fizički se onesposobljava kabel koji prenosi instrukcije pisanja. Drugu opciju je lakše opravdati na sudu.
  Ako se ne može koristiti ni jedno od dva spomenuta rješenja, medij se može *mountati* u *read-only* načinu. U tom slučaju je potrebno u detalje opisati korištene postupke i opcije kako bi se na sudu moglo dokazati da nije bilo dopušteno pisanje na disk.

- **Očuvanje stanja dokaza**
  Nakon *mountanja* istraživanog medija, prvi korak je računanje MD5 *hash* sažetka. To pruža referentnu točku inicijalnog stanja medija. Drugi korak je *bit-by-bit* kopija medija. Sve daljnje akcije će biti obavljane na kopiji medija, ne na originalu. Nakon toga je original potrebno pohraniti na sigurno mjesto.

  ```
  Take extra precautions to protect the original media and the initial
  hash. You will need both at the time of trial so that you can ensure
  that evidence you find is admissible. Even if your investigation does
  not lead to court, being able to prove that your activities made no
  changes to a disk drive is extremely helpful. You'll need the initial
  hash to prove such a claim.
  ```