Računalna forenzika

Uvod

Porastom broja korisnika osobnih računala povećala se i mogućnost iskorištavanja ljudi putem računala. Računalna forenzika je znanost koja se bavi otkrivanjem, sprječavanjem, analiziranjem i istraživanjem računalnih zločina. Područja istraživanja računalne forenzike uključuju web forenziku, forenziku podataka, forenziku dokumenata, mrežnu forenziku te forenziku mobilnih uređaja.

Pregled stranice

Teorija oko forenzike

ZAKONSKI OKVIR

Zločin počinjen pomoću bilo kakvog računala naziva se kibernetičkim ili računalnim kriminalom (eng. *cybercrime*) i u posljednjih je nekoliko desetljeća bilo potrebno stvoriti nove odnosno prilagoditi postojeće zakone ovoj vrsti zločina. U Hrvatskoj je prihvaćena Konvencija o kibernetičkom kriminalu, preuzeta u sklopu prilagodbe hrvatskih zakona pravnoj stečevini Europske unije.

Saznaj više o zakonskom okviru

CERTIFICIRANJE

U svijetu postoje organizacije koje izdaju certifikate za pojedina područja računalne forenzike. Ispitni postupak za dobivanje certifikata se standardno sastoji od pitanja vezana uz *hardware*, *software* te zakone u državi u kojoj se polaže ispit. U Hrvatskoj se obrazovanjem budućih forenzičara bavi samo INsig2 u Zagrebu, ovlašteni forenzički centar za regiju bivše Jugoslavije.

Neki od dostupnih certifikata u svijetu su:

- GIAC certificiran forenzički analitičar (GCFA, *The GIAC (Global Information Assurance Certification) Certified Forensics Analyst*), ANSI/ISO/IEC 17024 akreditiran certifikat,
- ISFCE CCE (*The International Society of Forensic Computer Examiners Certified Computer Examiner*)
- IACRB CCFE (*Information Assurance Certification Review Board Certified Computer Forensics Examiner*)
- IACIS CFCE (*The International Association for Computer Information Systems Certified Forensic Computer Examiner*)

- indijski IFS (*Intense Forensic Services*) *Cyber Forensic, Cyber Law, Cyber Crime* i *Cyber Security* certifikati
- EC-Council *Certified Ethical Hacker*
- Certifikati pojedinih tvrtki, npr. EnCE Certification Program softverskog alata EnCase

Pogledaj primjere pitanja na ispitu za CCE certifikat

Forenzika u praksi

GRANE RAČUNALNE FORENZIKE

Računalna forenzika je obitelj forenzičkih znanosti koja se bavi istraživanjem računalnih sustava, kao što su osobna i prijenosna računala, mobilni telefoni, digitalne kamere, vanjski diskovi, GPS uređaji, mrežni uređaji pa čak i uređaji za kopiranje ukoliko imaju internu memoriju. Standardno se dijeli na slijedeće grane:

- forenzika podataka (eng. *data forensics*)
- forenzika dokumenata (eng. *document forensics*)
- mrežna forenzika (eng. *network forensics*)
- forenzika mobilnih uređaja (eng. *mobile forensics*)
- e-mail i web forenzika

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.

Alati koje svaki forenzičar mora imati.

Računalna forenzika je više od analize blokova podataka. Riječ je o efektivnom skupljanju, analizi i izvještavanju o korištenim postupcima i nalazima. Iskusni istražitelj zna da je svaki korak bitan kako bi njegov slučaj imao željeni kraj.

Saznaj više o tijeku forenzičke istrage

PRIPREMA PRIJE IZLASKA NA TEREN

Prije same analize, istražitelj mora biti upoznat sa svim mogućnostima koje ga možda čekaju u stvarnom svijetu. To znači da mora znati kakvi uređaji sve postoje i kakvu potporu zahtjevaju te posebnosti različitih operacijskih sustava.

- **Hardware**
  Danas postoji toliko različitog sklopovlja da ga je nemoguće cijelog pokriti u ovom članku. Stoga će se pružiti generalni pregled tipova sklopovlja koji se može očekivati u forenzičkim istragama.

Pregled sklopovlja

- **Software**
  Iako većina korisnika danas koristi operacijski sustav Windows, nikako se ne smiju zaboraviti druge opcije, prvenstveno Linux i Mac OS. Istražitelj mora znati kako koji sustav radi, gdje pohranjuje podatke i što se sve može izvući s njega. Operacijski sustav se ponaša kao redatelj i tumač između korisnika i softvera i hardvera na računalu. Različiti operacijski sustavi drugačije funkcioniraju i istražitelj će koristiti drugačije metode i alate za pojedini OS.

  Pregled operacijskih sustava

VRSTE NAPADA

Vrste napada

SKUPLJANJE PODATAKA

Prilikom dolaska na mjesto zločina/istrage, prvo što istražitelj treba napraviti je zaključiti što bi sve moglo poslužiti kao dokaz. Nakon toga se identificirani podaci skupljaju te se poduzimaju mjere kako bi ostali nepromijenjeni prije i za vrijeme analize. Ključni koraci su dakle:

- IDENTIFIKACIJA DOKAZA
- SKUPLJANJE PODATAKA
  - Skupljanje promjenjivih podataka
  - Uzimanje slike sustava
- ČUVANJE SKUPLJENIH PODATAKA
- ANALIZA PODATAKA
  - Alati za mrežnu analizu