Forenzika računala u teoriji

Upoznavanje s mogućnostima

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

Metodologija forenzičke istrage

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.
Metodologija forenzičke istrage...

Standardni forenzički zadaci

Iako je svaka istraga posebna na svoj način, generalni pristup je isti. Ovo poglavlje predstavlja pregled zadataka zajedničkih svim računalnim istragama.
Standardni forenzički zadaci...

Analiza dokaza

Ovaj korak oduzima najviše vremena. Nakon što su prikupljeni svi dokazi s mjesta zločina, potrebno ih je sve detaljno pregledati kako bi se osumnjičeni mogao inkriminirati ili osloboditi sumnje.
Analiza dokaza...

Vrste napada

Izvor: Network and Computer Security Tutorial Version 0.4.0 April 16, 2001
Vrste napada...

nadalje ...

- Poznavanje zakonskog okvira
- Okupljanje ekipe za odaziv
- POJMOVI

Forenzika u praksi

Skupljanje podataka

Skupljanje promjenjivih podataka

Skupljanje promjenjivih podataka

Uzimanje slike sustava (image)


Nakon skupljanja promjenjivih podataka, može se uzeti slika hard drive-a.
Forenzičko računalo (računalo F) se pomoću crossover ili ethernet kabla spoji na istraživano računalo (računalo X) te se oba računala smjeste u istu podmrežu. Da bi mogli međusobno komunicirati, moraju biti na istom mrežnom segmentu. Dobra praksa je koristiti 10.0.0.1 za računalo X, a 10.0.0.2 za računalo F.

Uzimanje slike sustava

Analiza skupljenih podataka

Analiza podataka je dijelom znanost, a dijelom umjetnost. Znanstveni dio analize nalaže dobru pripremu, detaljno ispitivanje klijenta te poznavanje alata kojima će se provoditi istraga. Umjetnički dio znači da istražitelj treba imati “osjećaj” za istragu - što je bitno i gdje to naći.

Analiza skupljenih podataka

Top 100 mrežnih alata

http://sectools.org/