

Ebidentzia Digitalen Bilketa eta Analisi Prozedura (Forentsea)

1. Helburua

Intzidentzia baten ondoren ebidentzia digitalak modu seguruan biltzea, zaintza-katea bermatuz, ondoren auzitegi-analisia egiteko.

2. Printzipioak (RFC 3227)

- Hegakortasun Ordena:** Biltzen hasi memoria hegakorrenetik iraunkorrenera (CPU Cache -> RAM -> Swap -> Diskoa -> Babeskopiak).
- Ez aldatu:** Jatorrizko ebidentzia inoiz ez manipulatu. Egin irudi bat (bit-bit kopia) eta horren gainean lan egin.

3. Procedura

Fase 1: Eszena Babestea

- Isolatu gailua (saretik deskonektatu, baina ez itzali oraindik).
- Eragotzi baimenik gabeko pertsonen sarbidea.
- Argazkiak atera pantailari eta konexio fisikoei.

Fase 2: Datu Hegakorren Bilketa (Live Response)

- Sistema piztuta badago, exekutatu bilketa tresnak USB seguru batetik (ez instalatu ezer sisteman).
- Komandoak (Linux):** date, hostname, uname -a, ifconfig, netstat -anp, ps aux, lsof.
- RAM Memoria:** Erabili LiME edo WinPmem memoria-dumpa egiteko.

Fase 3: Diskoaren Irudia (Dead Acquisition)

- Itzali sistema (araututako moduan edo kabletik tiraka, egoeraren arabera).
- Erabili idazketa-blokeatzaleak (Write Blockers) diskoa konektatzean.
- Egin irudia: dd edo Guymager erabiliz.
- Kalkulatu HASH-a (SHA-256) jatorrizko discoan eta irudian. Biak berdinak izan behar dute.

Fase 4: Zaintza Katea (Chain of Custody)

- Dokumentatu pauso guztiak Zaintza Katearen Orria-n:
 - Ebidentziaren deskribapena (Marka, Eredua, Serie zenbakia).
 - Nork bildu du? Noiz? Non?
 - Nork dauka orain? Non gordetzen da?

Fase 5: Analisia

- Erabili Autopsy edo Volatility (RAM-erako) sortutako irudiaren gainean.
- Bilatu: Ezabatutako fitxategiak, nabigazio historia, log susmagarriak, malwarea.