ZABALA GAILETAK, S.A.

AUZITEGI-ANALISI INFORMATIKOA

# Auzitegi-analisi Informatikoa — Txosten Nagusia

DFIR Metodologia, Tresnak eta Emaitzak

| | |
|---|---|
| **Dokumentu Kodea:** | DFIR-ZG-001 |
| **Bertsioa:** | 1.0 |
| **Data:** | 2026-02-19 |
| **Ikasturtea:** | 2026 |
| **Sailkapena:** | Heziketa — Barne Erabilera |
| **Egilea:** | Zabala Gailetak Zibersegurtasun Taldea |

# 1. Sarrera eta Helburua

Txosten honek Zabala Gailetak-en auzitegi informatikoki hartu diren neurriak, erabilitako metodologiak eta lortutako emaitzak biltzen ditu. DFIR (Digital Forensics and Incident Response) printzipioen arabera egina dago, RFC 3227 estandarra eta ISO/IEC 27037 jarraibideak aintzat hartuz.

■ *Txosten hau heziketa-helburuetarako idatzia dago eta ez du epaiketa-prozesu erreal baten ebidentzia balioa.*

# 2. DFIR Metodologia

Auzitegi-analisi informatikoak fase hauek ditu:

- **Prestakuntza:** Tresnak, eskubideak eta bilketa-plan dokumentatua.
- **Identifikazioa:** Ebidentziak kokatu eta inbentariatu.
- **Kontserbazioa:** Irudi bit-mailakoak egin idazketa-blokatzaileekin.
- **Analisia:** Autopsy, Volatility, Wireshark eta konfigurazioa.
- **Dokumentazioa:** Aurkikuntza guztiak zaintza-katearekin erregistratu.
- **Txostena:** Tekniko eta exekutibo maila biko emaitzak.

## 2.1 Tresna-multzoa

| Tresna | Kategoria | Erabilera Nagusia |
|---|---|---|
| Autopsy / TSK | Disko Analisia | Fitxategi-sistema aztertu, ezabatutakoak berreskuratu |
| Volatility 3 | Memoria Forentsea | RAM-dump aztertu, prozesuak, konexioak, malwarea |
| Wireshark | Sare Analisia | PCAP captureak aztertu, protokoloak ebaluatu |
| dc3dd / Guymager | Irudigintza | Bit-mailako kopia forensea egin SHA-256 egiaztapenarekin |
| LiME / WinPmem | Memoria Bilketa | RAM memoria modu seguruan atera sistema piztuta |
| YARA | Malware Detekzioa | Arau-oinarridun bilaketa fitxategi eta prozesuetan |
| Sleuth Kit | Linea Kronologikoa | Fitxategi-sistema kronologia berreraiki |
| RegRipper | Erregistroa | Windows Erregistroa analizatu, artefaktuak atera |

# 3. Ebidentzien Bilketa Prozedura

RFC 3227 printzipioak: Hegakortasun ordenaren arabera bildu (RAM > Swap > Diskoa > Sarea).

## 3.1 1. Fasea: Eszena Babestea

- Gailua ingurutik isolatu (sare-kablea atera, WiFi itzali), baina EZ itzali oraindik.
- Argazkiak atera pantailari, fisikal konexioei eta inguruari.
- Pertsonal baimena ez duenaren sarbidea eragotzi.
- Denboraren erregistroa hasi (data/ordua UTC-n).

### 3.2 2. Fasea: Datu Hegakorren Bilketa (Live Response)

```
# Linux — Datu hegakorren bilketa date && hostname && uname -a # Sistema identifikatu
ifconfig -a && netstat -anp # Sare egoera ps auxf && lsof -nP # Prozesuak eta
fitxategiak last && who && w # Saio aktiboa # RAM memoria atera — LiME moduluarekin
insmod /media/usb/lime.ko 'path=/media/usb/ram.lime format=lime'
```

### 3.3 3. Fasea: Disko Irudigintza

```
# Idazketa-blokatzailea konektatu aurretik dc3dd if=/dev/sdb hash=sha256
hof=/media/forense/disco_imagen.dd # Hashak egiaztatu sha256sum /dev/sdb >
hashes_orig.txt sha256sum /media/forense/disco_imagen.dd > hashes_kopia.txt diff
hashes_orig.txt hashes_kopia.txt && echo 'Irudia egiaztatu: OK'
```

## 4. Memoria Forensea — Analisi Praktikoa

Volatility 3 tresnarekin RAM-dump bat aztertu da sistema susmagarri batean:

```
# Profilak identifikatu vol.py -f ram.lime banners.Banners # Prozesu zuhaitza ikusi
vol.py -f ram.lime windows.pstree.PsTree # Sareko konexioak vol.py -f ram.lime
windows.netstat.NetStat # Injektatutako kodea bilatu vol.py -f ram.lime
windows.malfind.Malfind # DLL-ak aztertu vol.py -f ram.lime windows.dlllist.DllList
```

## 5. Zaintza Katea (Chain of Custody)

Ebidentzia bakoitzak zaintza-kate dokumentua izan behar du. Honako informazioa jaso behar da:

| Eremu | Edukia |
|---|---|
| Ebidentzia ID | EV-2026-001 |
| Deskribapena | Dell Latitude 5520 ordenagailu eramangarria, S/N: ABC123 |
| Bilketa Data/Ordua | 2026-02-10 09:32 UTC |
| Biltzailea | Jon Etxeberria (Auzitegi Analista) |
| Bilketa Lekua | 3. solairua, 302 bulegoa |
| Biltegiratze Lekua | Ebidentzia gela — armairua A3 |
| SHA-256 Hash | a3f4b2c9d1e0f7a6b5c4d3e2f1a0b9c8... |
| Azken Manipulazioa | 2026-02-10 14:15 — Analista: Jon Etxeberria |

## 6. Ondorioak eta Aurkikuntzak

Zabala Gailetak-en aztertu diren sistemen auzitegi-analisian, ebidentziak biltzearen, analizatzearen eta dokumentatzearen metodologia egokia frogatu da. Tresna nagusiak (Autopsy, Volatility) eraginkortasunez erabiltzen dira jarduera susmagarriak identifikatzeko.

- Memoria-analisian prozesu susmagarriak identifikatzeko gaitasuna frogatu da.
- Disko-irudigintzarako SHA-256 hashak ezinbesteko osagaia dira ebidentzia-osotasuna bermatzeko.
- Zaintza-katea dokumentuzko prozesu argi eta jarraituarekin ezarri da.
- YARA arauek malware-familia ezagunak azkar detektatzeko aukera ematen dute.