HORIZONSHIELD

Securing Your Digital Future, Today.

BLUE TEAM SERIES · BOOK 14 OF 16

Digital Forensics Guide

Investigation, Evidence & Chain of Custody — 2026

End-to-end digital forensics covering evidence acquisition per ISO 27037, disk forensics, memory analysis, network forensics, log analysis, and expert witness reporting. Built on ACPO principles with legal admissibility focus.

EVIDENCE TYPES	TOOLS	STANDARD	LEVEL
6	35+	ISO 27037/ACPO	Intermediate

Contents

DIGITAL FORENSICS 2026

01	Forensic Principles — ACPO & ISO 27037	PRINCIPLES	4
02	Evidence Acquisition — Order of Volatility	ACQUISITION	8
03	Disk Forensics — Imaging & Analysis	DISK	12
04	Memory Forensics — Volatility 3 Reference	MEMORY	16
05	Network Forensics & Log Analysis	NETWORK	21
06	Windows Forensic Artefacts	WINDOWS	25
07	Expert Witness Reporting	REPORTING	29

CHAPTER 01

Forensic Principles

Forensic evidence is only useful if it is admissible and defensible. Follow established principles from the moment you engage.

ACPO PRINCIPLES | ISO 27037 | CHAIN OF CUSTODY | LEGAL ADMISSIBILITY

ACPO Principles for Digital Evidence

PRINCIPLE 1

No Alteration of Original Data

No action taken by investigators should change data held on a computer or storage media that may be relied upon in court. Write-blockers must be used for all forensic imaging. All hash values recorded before and after acquisition.

PRINCIPLE 2

Competence to Access Original Data

In circumstances where access to original data is necessary, the person accessing it must be competent to do so and must be able to give evidence explaining the relevance and implications of their actions.

PRINCIPLE 3

Audit Trail

An audit trail or other record of all processes applied to digital evidence must be created and preserved. It must be possible for an independent third party to examine the processes and achieve the same result. Contemporaneous notes are essential.

PRINCIPLE 4

Overall Responsibility

The person in charge of the investigation has overall responsibility for ensuring the law and these principles are adhered to. All investigators must understand their legal obligations.

Evidence Collection — Order of Volatility (RFC 3227)

Priority	Evidence Type	Volatility	Collection Method	Retention in Memory
1 (MOST VOLATILE)	CPU registers, cache, ARP table	Seconds to minutes	Live system only — specialised tools	Lost on context switch
2	RAM / physical memory	Minutes to hours	WinPmem (Windows), LiME kernel module (Linux), osxpmem (macOS)	Lost on shutdown or sleep
3	Active network connections	Minutes	netstat -anob, ss -tunap, TCPView	Lost on disconnect/timeout
4	Running processes	Minutes	Process list, process memory dump	Lost on termination
5	Logged-in users, open files	Hours	who, lsof, handle.exe	Lost on logout
6 (LEAST VOLATILE)	Disk / storage media	Days to indefinite	FTK Imager, dd with write-blocker	Persistent until overwritten
7	Backup media, offline storage	Weeks to years	Standard acquisition	Persistent

MEMORY ACQUISITION MUST HAPPEN BEFORE SHUTDOWN

All volatile evidence — running processes, network connections, encryption keys in RAM, attacker tools not written to disk — is permanently lost on system shutdown or reboot. In ransomware incidents: memory may contain the decryption key, making acquisition critical for key-escrow decryption of encrypted files.

CHAPTER 04

Memory Forensics — Volatility 3

Memory forensics reveals malware, credentials, and attacker activity that leaves no disk artefacts.

VOLATILITY 3 | PROCESS INJECTION | CREDENTIAL EXTRACTION | MALWARE DETECTION

Volatility 3 — Complete Command Reference

```
# ── SYSTEM INFORMATION ──────────────────────────
python3 vol.py -f memory.dmp windows.info
python3 vol.py -f memory.dmp windows.envars  # Environment variables

# ── PROCESS ANALYSIS ────────────────────────────
python3 vol.py -f memory.dmp windows.pslist  # Process list (normal view)
python3 vol.py -f memory.dmp windows.pstree  # Process tree (parent/child)
python3 vol.py -f memory.dmp windows.psscan  # Pool tag scan — finds hidden processes
python3 vol.py -f memory.dmp windows.cmdline  # Command line arguments per process

# COMPARE pslist vs psscan — discrepancies = hidden processes
# diff <(python3 vol.py -f memory.dmp windows.pslist) \
#      <(python3 vol.py -f memory.dmp windows.psscan)

# ── FIND INJECTED CODE (malfind) ────────────────
python3 vol.py -f memory.dmp windows.malfind
# Finds: RWX memory regions with PE headers (hallmark of process injection)
# Dump suspicious regions:
python3 vol.py -f memory.dmp windows.malfind \
  --dump --pid 1234  # Replace 1234 with suspicious PID

# ── NETWORK CONNECTIONS ─────────────────────────
python3 vol.py -f memory.dmp windows.netstat
python3 vol.py -f memory.dmp windows.netscan  # Includes closed connections

# ── CREDENTIAL EXTRACTION ───────────────────────
```

```
python3 vol.py -f memory.dmp windows.hashdump  # SAM database hashes
python3 vol.py -f memory.dmp windows.lsadump  # LSA secrets
python3 vol.py -f memory.dmp windows.cachedump  # Cached domain credentials

# ── REGISTRY & PERSISTENCE ──────────────────────
python3 vol.py -f memory.dmp windows.printkey \
  --key 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'
python3 vol.py -f memory.dmp windows.printkey \
  --key 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run'

# ── FILE & DLL ARTEFACTS ────────────────────────
python3 vol.py -f memory.dmp windows.dlllist --pid 1234  # DLLs loaded by process
python3 vol.py -f memory.dmp windows.dumpfiles --pid 1234  # Dump process files
python3 vol.py -f memory.dmp windows.handles --pid 1234  # Open handles
```

MEMORY ACQUISITION TIMING IS CRITICAL

Acquire memory BEFORE running any remediation tools. Running antivirus scans, restarting services, or isolating the machine via software (vs physical network disconnect) can overwrite valuable memory artefacts before acquisition. Physical network disconnect (pull cable) → memory acquisition → then software-level investigation.

HS

H O R I Z O N S H I E L D

Securing Your Digital Future, Today.

Digital Forensics Guide 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.