REV 2 — 2026
LARS BLOMGAARD
www.defencia.dk

Steps for Acquiring Live Data

Digital Forensics & Incident Response — Evidence Collection Procedure

! IMPORTANT Time-sync all collection systems to NTP before starting. Document UTC offset. Ensure write-blockers and adapters are prepared. Never alter original evidence.

1 — Case Preparation

1.1 Prepare Evidence Data from Acquisition

Before any collection begins, ensure the following case metadata is recorded:

Case description	Short, factual description of the case and suspected incident type.
Analyst responsible	Full name, role, and contact information.
Start date & time	Date/time collection commenced (UTC). Include UTC offset.
Time on evidence	Track time spent on each piece of evidence for chain of custody.
Number of evidence items	Total count of items acquired in this case.
Tools & versions	List all tools used (e.g. KAPE, Magnet AXIOM, Velociraptor). Include exact version numbers.
Additional information	Any supplementary notes, access restrictions, or special circumstances.
NTP / Timezone	CRITICAL: Record NTP server used and timezone of target system.
Setup photographs	Photos of the acquisition setup (physical connections, screen, environment).

1.2 Limitations

Document any constraints that affect the scope or completeness of collection:

- Time limitation — legal deadlines, on-call windows, or business continuity requirements
- Physical limitations — access to hardware, connectors, power, or physical location
- Circumstances inhibiting full collection — encrypted volumes, running VMs, locked systems, remote-only access
- Legal / scope limitations — court orders, NDAs, restricted data types (PII, GDPR, etc.)

2 — Tools in Toolbox

2.1 Triage & Collection

KAPE Fast triage & targeted artefact collection	**CyLR** Live response collection (cross-platform)	**Velociraptor** Endpoint query & large-scale collection
Binalyze IREC Automated enterprise IR collection	**Eric Zimmerman Tools** Artefact parsing (EZ Tools suite)	

2.2 Memory Acquisition

DumpIt Fast, lightweight Windows memory dump	**Magnet RAM Capture** Free GUI-based memory acquisition	**FTK Imager** Memory + disk imaging (GUI)
WinPmem Open-source Windows memory driver	**LiME** Linux memory acquisition (kernel module)	

2.3 Disk Imaging

FTK Imager DD / E01 / AD1 disk imaging	**Paladin / CAINE** Linux forensic boot environments	**Kali Linux** Versatile forensic & IR platform
dd / dcfldd CLI imaging on Linux/macOS	**Guymager** Fast GUI imager for Linux	

3 — Analysis on Evidence

This is not an exhaustive list. Document all actions performed during analysis.

- Tools installed and run on the system
  - Version number
  - Timeframe (when tool was run)
  - Actions performed by the tool
  - Memory dump performed or not
- Commands executed on the system
  - Full command-line syntax and parameters used
  - Output files generated and their location
  - Hash values of all output files (SHA-256)

4 — Data Collection by Scenario

4.1 Network Drive

- Tools: Teamspy, Windows Memory, FTK
- Filetree in text
- Import data from ex folder or files to AD1
- Screenshot of files / folders (File > to > AD1)
- Hash tool (AD Bintools, Domain)

4.2 Computer (Workstation / Laptop)

- Tools
  - Teamspy
  - Windows Memory
  - FTK
- Filetree in text
- Import data from ex folder or files to AD1
- Screenshot of files / folders
- Documentation
  - Screenshot of files
  - Rename in clear text
  - Camera / mobile (if system is locked)
- Agent utilities: AFF, GoLd, Security, Files, Memorydump
- Copy of artefact (logs, malware, files, hives)
- Remote Endpoint
  - Velociraptor
  - EDR (Falcon, Carbon Black, etc.)
  - Detection and Response
  - Contact local support for agreement on course of action to collect data
- Timeframe to have data in hand
- Anti-malware solution
  - Logs
  - Detection
  - Network activity
  - Detection (according to vendor)
- NADS
- Online resources from vendor or others

4.3 Server

- Documentation
  - Screenshot of files
  - Rename in clear text
  - Camera / mobile (if system is locked)
- Logs
  - From app server (Accesslogs)
  - Application
  - Any logs / information
  - Files / artefacts
- Test HASH against service (VT, Any.run, sandbox, MISP, etc.)
- If password infected: document and hash

4.4 Malware (Generic Handling)

Connect to an external device — preferably Linux.

- If screenshot and password infected: document and hash
- Test HASH against service (VT, Any.run, sandbox, MISP, etc.)
- Logs
  - System logs
  - Application logs
  - Any logs / information
- Files / artefacts

4.5 Cloud Systems

- Specific information
  - Changes of files
  - Data portability (MS, Google, etc.)
  - Export AD data (Azure)
  - Export M365 data security
- Define what to collect — be aware of large data volumes
  - Takeouts
  - File activity
  - Sharing history
  - Login and traffic information
  - Files deleted / changed
  - Logs of the above
- Virtual machines
  - If on-premise: collect memory by hibernating VM (VMware)

4.6 Live Collection (Applies to All Scenarios)

- Simply copy the files if applicable
- Tools for live collection
  - Velociraptor
  - KAPE
  - CyLR
  - Binalyze IREC
  - Volatility (memory analysis)
- Memory dump (if possible — BE CAREFUL)
  - DumpIt
  - Magnet RAM Capture
  - FTK Imager
  - WinPmem / LiME (Linux)
- netstat -NAOB (capture active network connections)
- Image of hard drive
  - Verify you have the correct tools and adapters (SATA, NVMe, M.2)
  - Boot environments: CAINE, Paladin, Kali etc.
  - Output formats: DD / RAW / E01 / AD1
  - Hash and timestamp immediately after imaging
  - Store original copy — do not work from the original
- Documentation
  - Describe the files collected
  - Hash / Integrity calculation (SHA-256)
  - Describe the course of action
  - Screenshots from system
  - File tree (screenshot or cleartext — 'tree' command)
  - Photos (camera / mobile phone) of physical environment
- Encryption (check before imaging)
  - LUKS (Linux)
  - FileVault (macOS)
  - BitLocker (Windows) — obtain recovery key
  - Boxcryptor / VeraCrypt

5 — Tips & Reminders

TIP 1	Know your servers and endpoints before deployment. Are you sure virtualization is in place?
TIP 2	Know your 'copy' time — large datasets take longer than expected. Plan accordingly.
TIP 3	Know where to obtain codes for encryption recovery in the organisation (BitLocker, LUKS, FileVault).

5.1 Browser Evidence

- Portable browser — collect data from the collection media
- Favourite browser extensions to preserve web session context
- HTA Track browser extension — capture browsing history
- HTTPS Everywhere / uBlock: note any active privacy extensions on suspect browser

HASH	Always use SHA-256 for integrity verification. MD5 and SHA-1 are deprecated for forensic use. Calculate hash before and after collection.

CHAIN OF CUSTODY	Every transfer, copy, or analysis action must be documented with analyst name, timestamp (UTC), and purpose. If you didn't document it — it didn't happen.

This document is a living reference. Update tool versions and procedures as the threat landscape evolves.