REV 2 — 2026
LARS BLOMGAARD
www.defencia.dk

Steps for Acquiring Data

Digital Forensics & Incident Response — Evidence Acquisition & Chain of Custody

GOLDEN RULE	Acquisition is the foundation of all forensic work. A broken chain of custody can invalidate every finding. Document everything — before, during, and after. When in doubt: photograph it, write it down, and get a signature.

1 — Physical Surroundings & Scene Documentation

Document the physical environment thoroughly before touching anything. First responder actions at the scene define the integrity of all subsequent analysis.

1.1 Scene Documentation

- Photograph the entire scene before any equipment is moved or touched
- Photograph all screens (active sessions, open applications, current state)
- Photograph all physical connections: cables, USB devices, external drives, dongles, monitors
- Photograph any physical notes, sticky notes, or written passwords visible at the scene
- Note the date, time (UTC), and exact physical location
- Who was present? Record full names and roles:
  - HR representative
  - Manager / line manager
  - IT technician / DFIR analyst
  - Witness(es) — at least one independent witness is strongly recommended
  - Legal counsel / law enforcement (if applicable)
- Was the device in use at the time of collection?
  - If yes: document exactly what was visible, what the user was doing, and by whom
  - If a live session was running: consider live data acquisition before shutdown (see Live Data card)

1.2 Device State at Time of Collection

Device powered state	Was the device ON or OFF at time of collection? This drives the acquisition approach.
Screen state	Locked / unlocked / screensaver? Active session or logged out?
Network state	Connected (wired / Wi-Fi) or isolated? Any VPN active?
Encryption state	Was BitLocker / LUKS / FileVault active? Was the volume mounted (decrypted)?
Other effects	Any USB devices connected, external drives, other peripherals? List all.
Active processes	If screen was visible: note any running applications, open files, or browser tabs.
Memory dump possible?	Was a live memory dump performed before shutdown? If not — document why.

1.3 Collection & Retention of Physical Units

- Describe the collection method for each device
- Document date, time (UTC), and any prerequisites
- Under what conditions was the equipment retained? Any resistance, unusual behaviour?
- Device sealing — tamper-evident bags / seals applied?
- Photograph the device before sealing
  - Photograph the sealed package before transport
  - Photograph upon arrival at the forensic lab (break-in-transit detection)
- Anti-static bags for electronic storage media
- Faraday bag / cage for mobile devices to prevent remote wipe
- Transport: how was the device transported?
  - Was the transporting person trusted / vetted?
  - Chain of custody signed at every handover point
- Every change of hands must be documented: date, time, from person, to person, and signature

2 — Data Protection & Write Blocking

! CRITICAL NEVER connect forensic media to a live system without a write blocker. A single unprotected write to the original evidence invalidates its forensic integrity and may render it inadmissible.

2.1 Write Blocker

- Was a hardware write blocker used?
  - Make and model of write blocker (e.g. Tableau T35u, WiebeTech Forensic UltraDock, UFED)
  - Document the write blocker used, serial number, and firmware version
- Was a software write blocker used instead? (e.g. registry-based in Windows, hdparm in Linux)
- Document which method was used and why — hardware is always preferred
- Verify write blocker is functioning before connecting evidence media

2.2 Imaging & Data Securing

- Image format used: E01 (preferred for metadata + compression), DD/RAW, AD1, AFF4
- Software used for imaging — document name and exact version:
  - FTK Imager, Magnet ACQUIRE, Guymager, dc3dd, dcfldd, Paladin
- Who secured the data? Record full name, date, and time (UTC)
- Hash integrity calculated IMMEDIATELY after imaging:
  - SHA-256 — primary hash (MD5 and SHA-1 are deprecated for forensic use)
  - Hash both the source media AND the destination image — values must match
  - Re-verify hash after storage / transport to confirm integrity was maintained
- How was the data stored?
  - Which encryption was applied to the storage media? (BitLocker, VeraCrypt, LUKS)
  - Who holds the encryption key? Is it escrowed?
- Hash / integrity check log must be saved alongside the evidence image

2.3 Storage & Access Control

Where is data stored?	Physical location, server name, or cloud storage reference. Include path.
Storage media details	Make, model, serial number of the destination storage media.
Encryption applied	Encryption method and key holder. Is key escrowed with a second person?
Who has access?	List all persons with access to the evidence. Access must be need-to-know only.
Access log maintained?	Every access to evidence must be logged: who, when, and purpose.
Backup copy made?	A second verified copy should exist in a separate physical location.
Retention period	How long will evidence be retained? Per legal / organisational policy.

3 — Triangulation Data (Contextual Evidence)

Triangulation data is supporting evidence from surrounding infrastructure — firewalls, SIEM, DNS, AD, antivirus, proxies, cloud logs, etc. It does not replace forensic acquisition but contextualises and corroborates it.

IMPORTANT Triangulation data is highly valuable but must be treated with the same rigour as primary evidence. Document provenance, collection method, and integrity for every source.

3.1 Triangulation Data Sources

- Firewall logs — inbound/outbound traffic, blocked connections, NAT translations
- SIEM / SOAR — correlated alerts, event timelines, detection rules triggered
- DNS logs — query history, resolution records, anomalous domains queried
- Active Directory / LDAP — authentication events, group changes, account creation/deletion
- Antivirus / EDR — detection logs, quarantine events, blocked executions (CrowdStrike, Defender for Endpoint, SentinelOne, etc.)
- Email gateway / spam filter logs — delivery records, attachment inspection results
- Proxy / web gateway — URL history, category blocks, user-agent strings
- VPN / remote access logs — session times, IP addresses, authentication events
- Cloud platform logs — Azure AD sign-in logs, AWS CloudTrail, GCP Audit Logs, M365 Unified Audit Log
- DHCP logs — IP address assignment history (correlate MAC to IP to hostname)
- Network flow / NetFlow / IPFIX — traffic volume, port usage, lateral movement indicators
- Physical access logs — badge/swipe records correlated to logon events

3.2 Triangulation Data Documentation Requirements

For each triangulation data source, the following must be documented. This is very important — describe as thoroughly as possible.

Data type & source	What type of data is it, and from which system/service was it collected?
Collection method	How was it exported or captured? API, direct log export, SIEM query, screenshot?
Who collected it?	Full name, role, date, and time (UTC) of collection.
Who has access?	List all persons with access to this data source and its export.
What does the data prove?	What specific facts or timeline events does this data establish?
Limitations	Any gaps, retention limits, clock skew, or known issues with this data source?
Integrity check	Hash of exported log files. Screenshot of query parameters / date range used.
Storage location	Where is this data stored? Encrypted? Access-controlled?

4 — Chain of Custody

LEGAL WEIGHT

The chain of custody is the legal backbone of a forensic case. Every break or undocumented handover weakens the admissibility of findings. Maintain it with absolute precision from first contact to final disposition.

4.1 Evidence Item Register

Complete one row per physical or logical evidence item collected.

Item #	Description	Make / Model / S/N	Collected by	Date & Time (UTC)	Hash (SHA-256)	Storage location
1						
2						
3						

4.2 Transfer Log

Record every transfer of evidence — physical or logical. Every handover requires a signature from both parties.

Transfer #	Date & Time (UTC)	From (Name / Role)	To (Name / Role)	Method / Location	Signature
1					
2					
3					
4					

4.3 Chain of Custody Principles

- Every person who handles evidence must be identified by name, role, and timestamp
- Handling must be minimised — only authorised personnel with documented purpose
- Original media must never leave the evidence bag without being logged
- Analysis is ALWAYS performed on verified forensic copies — never the original
- If original media must be accessed: document reason, who accessed it, and re-verify hash after
- Evidence must be stored in a locked, access-controlled, environmentally controlled location
- Electronic access log for evidence storage must be maintained
- Evidence disposition: document final outcome (returned, destroyed, submitted to court, archived)

5 — Special Acquisition Considerations

5.1 Live vs. Powered-Off Acquisition

Device is ON — memory acquisition needed	Prioritise live memory dump (DumpIt, Magnet RAM Capture, WinPmem). Then consider live disk acquisition. Refer to Live Data Acquisition card.
Device is ON — encryption concern	If BitLocker/LUKS is active and volume is mounted: image while live. Shutting down may lock the volume permanently if recovery key is unavailable.
Device is OFF	Standard dead-box acquisition. Apply write blocker, image with FTK Imager or Guymager. Verify hash immediately.
Device is a laptop on battery	Risk of shutdown during imaging. Plug in power before connecting. Monitor battery status throughout.
Mobile device	Place in Faraday bag immediately to prevent remote wipe. Use Cellebrite UFED, Magnet AXIOM, or Oxygen Forensic Detective. Document unlock method.
Server / RAID system	Do not pull drives without documenting RAID configuration. Image via network or hardware. Consult senior analyst before shutdown of production systems.
Virtual machine	Suspend VM (do not shut down) to capture memory state. Copy .vmdk / .vhdx + snapshot files. Document hypervisor version.
Cloud / SaaS	Legal process (warrant / court order) may be required. Use platform admin tools (eDiscovery, Content Search). Document scope and authorisation.

5.2 SSD & Flash Storage Considerations

SSD WARNING TRIM operations on SSDs may permanently destroy deleted file data. This can occur automatically while the drive is connected to a running OS. Always use write blockers and disconnect from live systems immediately.

- Document whether the target drive is SSD, HDD, NVMe, or eMMC
- Check if TRIM is enabled (fsutil behavior query DisableDeleteNotify on Windows)
- Prioritise acquisition speed — every minute of delay increases risk of TRIM activity
- Note: file carving from SSDs may yield fewer results than from HDDs due to TRIM
- For NVMe drives: ensure acquisition tool supports NVMe protocol (not all do)

5.3 Encryption Considerations

- BitLocker (Windows): obtain recovery key from Active Directory / Azure AD before imaging
- LUKS (Linux): passphrase or key file required — obtain from system owner with authorisation
- FileVault (macOS): recovery key from MDM or Apple ID — document source
- VeraCrypt / third-party: document software version, algorithm, and key source
- If encryption key cannot be obtained: image the encrypted volume — note limitation in report
- Never attempt brute-force without explicit legal authorisation

Acquisition done right is the difference between a case that stands and a case that collapses. There are no second chances — the scene exists only once.