REV 2 — 2026
LARS BLOMGAARD
www.defencia.dk

Steps for Secure Replication

Digital Forensics & Incident Response — Evidence Preservation & Secure Transfer

PRINCIPLE Replication is not a copy — it is a forensically verified, integrity-protected duplicate of evidence. Every replication action must be documented, hashed, and logged. The destination copy is what analysts work from. The source is stored and never touched again.

1 — Replicating Hardware Media

Applies to: HDD, SSD, NVMe, USB drives, SD cards, eMMC, optical media, and other storage hardware.

1.1 Write Blocker Verification

! MANDATORY A write blocker MUST be used for all hardware media replication unless live acquisition conditions explicitly prevent it. Document the reason if no write blocker was used.

- Hardware write blocker (preferred)
  - Make, model, and serial number (e.g. Tableau T35u-R2, WiebeTech Forensic UltraDock v6)
  - Firmware version — confirm current and note in log
  - Connector type used: SATA, USB 3.x, NVMe, PCIe, SD, CF
  - Verify write blocker is active before connecting source media
- Software write blocker (only if hardware is unavailable)
  - Windows: registry-based (HKLM\SYSTEM\...\StorageDevicePolicies, WriteProtect = 1)
  - Linux: hdparm -r1 /dev/sdX or blockdev --setro /dev/sdX
  - Document exact command used and output confirming read-only state
- If no write blocker was used: document exact circumstances (e.g. live acquisition, cloud, network share)

1.2 Source Media Documentation

Make & model	Manufacturer, drive model name.
Serial number	Physical label serial number AND firmware-reported serial (may differ on some drives).
Interface / form factor	SATA / NVMe / USB / M.2 / 2.5" / 3.5" / SD / eMMC etc.
Storage capacity	Reported capacity (sectors × sector size). Note if disk reports less than labelled.
Drive condition	Any visible physical damage? S.M.A.R.T. status checked? Reallocated sectors?
Encryption state	Was hardware-level encryption (SED / TCG Opal) in place? Was it bypassed?
SSD / TRIM status	Is TRIM active? NVMe or SATA? Document — TRIM affects recoverability of deleted data.

1.3 Replication Process

- Software used for replication — document name and exact version:
  - FTK Imager, Magnet ACQUIRE, Guymager, dc3dd, dcfldd, Paladin, X-Ways Imager
- Image format selected and rationale:
  - E01 / Ex01: preferred — includes metadata, CRC verification per block, compression
  - DD / RAW: simple sector-by-sector copy, no metadata container — large file size
  - AD1: AccessData logical image format
  - AFF4: modern open format with built-in hashing and compression
- Who performed the replication? Full name, date, and time (UTC)
- Destination media: make, model, serial number, and path
- Segment size (if split image): note segment size used
- Errors during imaging: bad sectors logged? Note count and location ranges
- Time taken for replication: start time, end time (UTC)

1.4 Hash Integrity Verification

HASH RULE	Calculate hash on the SOURCE before imaging AND on the DESTINATION image after. Both values must match. Use SHA-256 as primary hash. MD5 is deprecated for forensic integrity — use only for legacy tool compatibility if required.

- Hash algorithm: SHA-256 (primary). MD5 / SHA-1 only for secondary / compatibility
- Hash the source media before imaging begins — record value
- Hash the destination image immediately after imaging completes — record value
- Values must match — if they do not: STOP and document the discrepancy
- Re-verify the destination hash after any transfer or storage event
- Hash log file must be saved alongside the evidence image in the same folder
- Segmented images: verify each segment hash AND the full image hash
- Tools that automatically generate hash logs: FTK Imager (.txt), Guymager (.log), dc3dd (stdout — redirect to file)

1.5 Storage of Replicated Image

- Where is the image stored? (Path, server name, physical location)
- Storage media details: make, model, serial number of destination drive
- Encryption applied to storage:
  - Full-disk: BitLocker, LUKS, FileVault
  - Container: VeraCrypt, Boxcryptor (AES-256 minimum)
  - Who holds the encryption key? Is it escrowed?
- Who has access to the stored image? List all persons — access must be need-to-know only
- Was a verified second (backup) copy created and stored at a separate location?
- Data was replicated to whom? Record recipient name, role, and organisation

2 — Replicating Files, Artefacts & Logs

Applies to: targeted file collections, triage outputs (KAPE, CyLR), log exports, triangulation data (firewall, SIEM, DNS, AV, EDR), and cloud data exports.

2.1 File Replication Documentation

Data type & source	What type of data? Which system / service / tool produced it?
Collection method	How was it exported or captured? CLI, API, GUI export, log forwarder?
Who collected it?	Full name, role, date, and time (UTC).
Volume of data	Total file count and total size (bytes). Note compression applied.
Who has access?	All persons with access. Need-to-know principle applies.
What does it prove?	What specific facts, timeline events, or hypotheses does this data support?
Storage location	Full path, server, or cloud reference. Encrypted? Access-controlled?
Retention period	How long will this data be retained? Per legal or organisational policy.

- Hash all collected files individually: SHA-256 of each file
- Generate a hash manifest file: one line per file, format: SHA256 filename
- Tools: sha256sum (Linux/macOS), Get-FileHash (PowerShell), HashMyFiles (Windows GUI)
- Manifest file must be timestamped and stored alongside the collected data
- For large collections: generate a hash of the entire folder archive (zip/tar + hash)
- Log the total number of files and total byte count — verify at destination after transfer

3 — Secure Sharing

When sharing evidence or artefacts with external parties — MSSP/retainer partners, legal counsel, law enforcement, or other organisations — secure transfer methods must always be in place. Never share forensic evidence via unencrypted email, consumer file sharing, or USB without encryption.

3.1 Who Is the Recipient?

Internal colleague	Encrypted shared drive or internal evidence management system. Document access grant.
MSSP / retainer partner	Encrypted container via secure file transfer (SFTP, FTPS, managed file transfer platform). Signed NDA / retainer in place?
Legal counsel	Encrypted email (S/MIME or PGP) or secure legal file sharing platform (e.g. NetDocuments, ShareFile). Document authorisation.
Law enforcement	Follow legal process (warrant / court order). Use law enforcement-approved transfer method. Document every item shared with evidence receipt.
Threat intelligence sharing	STIX/TAXII, MISP, or sector ISAC platform. Strip identifying information unless explicitly authorised. Use TLP markings.

3.2 Encryption Methods for Sharing

Encrypted containers must be used for all external evidence sharing. AES-256 is the minimum acceptable standard.

Method	Use Case	Notes
Full-disk encryption	Physical drive handover	BitLocker, LUKS, FileVault — key shared via separate secure channel (never same email as drive)
VeraCrypt container	File/folder transfer — any platform	AES-256-XTS. Password via separate channel. Version-independent and open-source.
7-Zip AES-256 archive	Smaller collections, email attachment	Strong password required (16+ chars). Simpler than VeraCrypt. Widely compatible.
PGP / GPG encrypted file	Analyst-to-analyst transfer	Asymmetric encryption. Verify recipient public key fingerprint before use.
Encrypted email (S/MIME)	Legal / HR communications	Requires certificate infrastructure. Suitable for metadata and reports, not large evidence.
Managed File Transfer (MFT)	Large evidence packages to MSSP / LE	SFTP/FTPS with audit log. Examples: GoAnywhere, IBM SEAS, AWS Transfer Family.

3.3 Sharing Checklist

- Written authorisation obtained before any sharing — who authorised? Reference the document
- NDA / retainer agreement / legal order in place and referenced
- Data classification confirmed — does the recipient have clearance for this classification level?
- Personal data (PII / GDPR) handling reviewed — is GDPR Article 28 processor agreement required?
- Hash manifest provided with all shared data — recipient must verify on receipt
- Encryption key / password transmitted via a separate secure channel (never the same as the data)
- Evidence receipt obtained from recipient — signed acknowledgement of items received and hash values
- Log of sharing event: who shared, to whom, what, when (UTC), method, and reference number
- TLP (Traffic Light Protocol) marking applied if sharing threat intelligence:
  - TLP:RED — named recipients only, no further distribution
  - TLP:AMBER — limited to recipient organisation, need-to-know
  - TLP:GREEN — community sharing permitted
  - TLP:CLEAR — unrestricted

4 — Handling Malicious Artefacts

! DANGER Malicious artefacts (malware samples, exploit payloads, weaponised documents) are active threats. They must be handled as hazardous material. Mishandling can trigger execution, AV deletion, or contamination of analysis systems.

4.1 Containment of Malicious Files

- NEVER store or transfer malware samples in unprotected form on a connected system
- Password-protect all malicious artefacts immediately on collection
- Standard forensic community convention: password = infected
- Archive format: ZIP (most compatible) or 7-Zip with AES-256
- Naming convention: infected_<SHA256_first8chars>_<YYYYMMDD>.zip
- Store in a dedicated, clearly labelled folder: /malware_samples/ or /infected/
- Include a README.txt inside the archive:
  - SHA-256 hash of each contained file
  - Source: where/when/how the file was collected
  - AV detection name (if known)
  - Warning label: MALICIOUS CONTENT — DO NOT EXECUTE
  - Analyst name and date

4.2 Why Password Protection Matters

- Prevents accidental execution by the analyst or automated systems
- Prevents antivirus / EDR from quarantining or deleting the sample before analysis
- Prevents accidental detonation during transfer or backup
- Ensures sample integrity — AV alteration of samples destroys forensic value
- Industry-standard password 'infected' is recognised by malware repositories (MalwareBazaar, VirusTotal) and is universally understood by DFIR analysts

4.3 Sharing Malicious Artefacts

- Obtain explicit written authorisation before sharing any malware sample externally
- Never upload to public sandboxes (VirusTotal, ANY.RUN) without authorisation — samples may alert the adversary or leak sensitive metadata
- When sharing with MSSP / law enforcement: use encrypted container (VeraCrypt / 7-Zip AES-256)
- Provide SHA-256 hash to recipient in advance via a separate secure channel
- Recipient must verify hash on receipt before opening the container
- Maintain a malware sample registry: one row per sample with hash, source, recipient, date, and authorisation reference

5 — Replication Log

Complete one row per replication action. Retain this log as part of the case file. Both source and destination hashes must be recorded and must match.

Item #	Source media / path	Destination	Tool & version	Analyst	Date/Time (UTC)	SHA-256 (source)	SHA-256 (dest.)	Match?
1								
2								
3								

MISMATCH If source hash ≠ destination hash: STOP immediately. Do not use the destination copy. Investigate the cause (bad sectors, transfer error, write blocker failure). Re-image from source. Document the failure in the case file.

A replicated image that has not been hash-verified is not evidence — it is an unknown. Verify everything. Every time.