

Preserve Digital Evidence Without Damaging the Original

The strongest file is not the most edited or dramatic copy. It is the original byte stream preserved with enough context to explain where it came from and what happened next.



A digital evidence preservation workspace with drives and archival storage. Original TargetedArmy editorial image generated for this guide.

FIRST PRINCIPLE

Stop changing the source

When a file may matter, pause before opening it in an editor, uploading it to a social platform, or sending it through an app that may compress or rewrite it. Preserve the original file exactly as the device produced it. If the item is a message or web record, export it through the service when possible and also capture the surrounding context.

Create a case folder with separate directories for originals, working copies, exports, notes, and shared copies. Originals should be read-only in practice: do not crop, enhance, rename, transcode, or add annotations inside that folder.

COLLECTION NOTE

Describe how the bytes reached your custody

For each item, record the original filename, source device or account, date and time collected, person who collected it, transfer method, displayed timestamps and time zone, and any known clock error. Note whether the file was downloaded, copied by cable, exported by an application, received as an attachment, or captured from a screen.

This collection note is as important as the file. Metadata can be changed by normal software, cloud synchronization, or transfer. A preserved account of the collection process helps another reviewer understand which values came from the source and which may have been introduced later.

- Never ask a checksum to prove authorship or cause
- Keep the source device when lawful and safe
- Document clock settings and time zone
- Retain export instructions and application version
- Record every copy shared outside your custody



A practical detail view supporting the article procedure.

INTEGRITY

Calculate a checksum and verify every backup

Use a reputable SHA-256 tool to calculate a checksum after collection. Save the value in a plain-text inventory outside the original file. Copy the originals to at least one additional device, calculate the checksum of the backup, and confirm that it matches.

A matching checksum demonstrates that two files contain the same bytes. It does not establish when an event occurred, whether the content is authentic, or who controlled the source device. Those questions depend on the collection record, surrounding evidence, system logs, testimony, and qualified examination.

WORKING COPIES

Analyze, redact, and share from a derivative

Duplicate the original into the working folder before changing it. Name the derivative so its relationship is obvious, and record the operation performed: volume normalization, frame extraction, redaction, transcript, or format conversion. Never overwrite the source.

Public sharing creates additional risk. Remove private addresses, account identifiers, medical details, and unrelated faces only from a derivative. Keep a private cross-reference that identifies the original and the redaction method. A social-media upload is a distribution copy, not a preservation system.

HANDOFF

Give qualified reviewers a complete, bounded package

Provide the original file, checksum inventory, collection note, relevant device and software information, and the specific question you want examined. Avoid flooding a reviewer with unrelated material. A small package with a documented chain is easier to assess than an unstructured archive.

NIST describes collection, examination, analysis, and reporting as distinct forensic phases. A personal preservation workflow does not replace a qualified forensic examiner or legal advice, but it can prevent avoidable damage before professional help is available.

Sources

1. NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology 2006

<https://csrc.nist.gov/pubs/sp/800/86/final>

2. NIST SP 800-101 Rev. 1: Guidelines on Mobile Device Forensics. National Institute of Standards and Technology 2014

<https://csrc.nist.gov/pubs/sp/800/101/r1/final>

Editorial Notice

TargetedArmy presents information, testimony, research, historical material, and analysis from the perspective of targeted individuals and this community. Some readers, institutions, or organizations may dispute portions of the material presented. Readers are encouraged to review the supporting materials and reach their own conclusions.

Published 2026-07-17 · <https://targetedarmy.maxisrichards.chatgpt.site/content/defense/preserve-digital-evidence>