CS-102 · Digital Forensics

Disk Imaging

Making an exact, verifiable copy of storage media so the original stays untouched.

Executive Summary

Disk imaging is the process of making a complete, bit-for-bit copy of storage media so that investigators can analyze the data without touching the original. A forensic image captures everything on the media, including deleted and unallocated areas, and its integrity is proven by matching cryptographic hashes. Done correctly, it preserves the original as evidence while giving examiners a faithful copy to work on.

What It Is

A forensic disk image is an exact duplicate of a storage device at the level of raw bits, not just the visible files. That means it includes active files, deleted-file remnants, slack space, unallocated space, and file system metadata, all of which can hold evidence. Imaging differs from an ordinary backup or file copy, which captures only visible data and may change timestamps. Images are typically stored in either a raw format that mirrors the media exactly or a forensic container format that also records hashes and case information. The purpose is to create a working copy that is provably identical to the source so analysis never risks altering the original.

Why It Matters

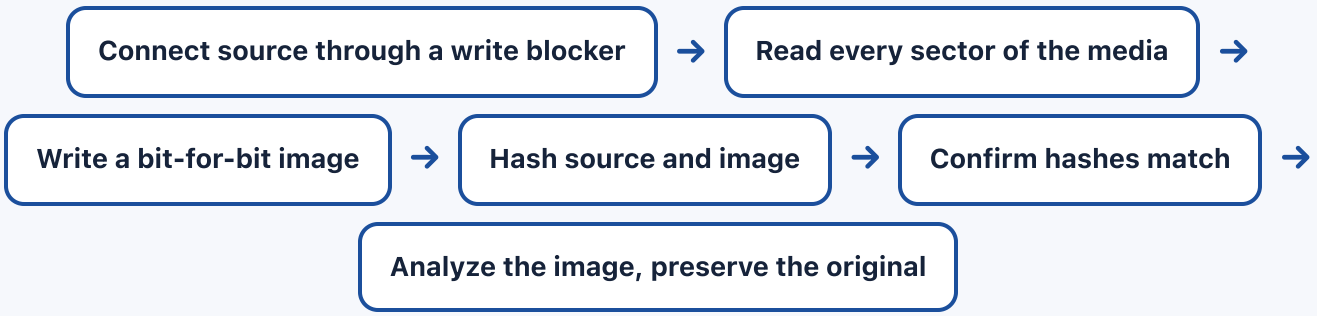
The original media is the evidence, and every analysis step carries some risk of changing it, so investigators image first and then work only on the copy. A verifiable image lets multiple examiners analyze the same data independently, supports reproducible results, and keeps the original safe for re-examination or court. Because a forensic image captures deleted and hidden areas, it often preserves evidence that a normal copy would lose. For organizations, sound

imaging underpins defensible breach investigations, litigation, and regulatory response. For professionals, it is a foundational, widely tested forensic skill.

How It Works

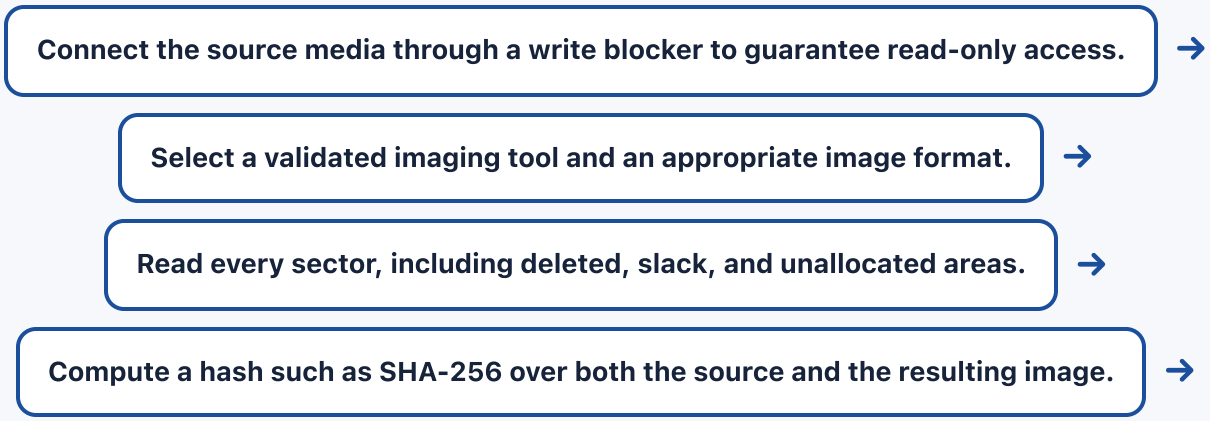
Imaging works by reading the source media in a way that cannot alter it and writing a faithful copy elsewhere. A write blocker sits between the source and the examiner's system to guarantee read-only access, so nothing is written back to the evidence. The imaging tool reads every sector and produces the image, and a cryptographic hash such as SHA-256 is computed over the source and the image. If the two hashes match, the copy is proven identical; that hash is then used later to confirm the image has not changed. All of this is documented, including tool versions and any bad sectors encountered. NIST maintains work on validating forensic tools, and guidance such as NIST SP 800-86 frames imaging within a sound overall process.

Architecture Diagram



A write blocker guarantees read-only access; matching hashes prove the image is an exact, defensible copy.

Visual Workflow



Confirm the source and image hashes match to prove the copy is exact. →

Store the original securely and perform all analysis on the verified image.

Common Attacks

- Anti-forensic wiping that destroys data before it can be imaged
- Full-disk encryption that renders an image unreadable without the key
- Hidden areas of a drive used to conceal data from casual copying
- Timestamp and metadata manipulation to mislead later analysis
- Deliberate corruption of sectors to disrupt acquisition

Common Mistakes

- Booting or mounting the original media read-write and altering it
- Skipping the write blocker and writing back to the evidence
- Making a normal backup that misses deleted and unallocated data
- Not verifying that source and image hashes match
- Failing to document tool versions, formats, and any read errors

Best Practices

- Always acquire through a write blocker or a verified read-only method
- Capture a full bit-for-bit image, not just visible files
- Hash the source and image and confirm they match before analysis
- Store the image in a format that records hashes and case details when possible
- Keep the original in secure storage and work only from the copy
- Document tools, versions, formats, and any errors encountered

Quick Checklist

- [ ] Write blocker or read-only method confirmed before acquisition

- [x] Full bit-for-bit image captured, including unallocated space
- [x] Source and image hashes recorded and matching
- [x] Image stored with case details and integrity information
- [x] Original media secured and untouched after imaging
- [x] Imaging tool, version, format, and errors documented

Recommended Tools

Write blocker
Enforces read-only access so the source media cannot be altered

Forensic imaging tool
Reads every sector and produces a verifiable bit-for-bit image

Hashing utility
Computes and compares hashes such as SHA-256 to prove the image is exact

Forensic image format
Stores the copy along with hashes and case metadata for defensibility

Industry Standards

NIST SP 800-86
Guide that frames acquisition and integrity within a sound forensic process

NIST Computer Forensics Tool Testing (CFTT)
Program that validates the behavior of forensic imaging tools

ISO/IEC 27037
Guidelines for acquisition and preservation of digital evidence

Career Relevance

Disk imaging is a foundational skill for forensic investigators, DFIR analysts, and incident responders, and SOC analysts benefit from understanding it when systems must be preserved. E-discovery and litigation-support professionals rely on defensible imaging, and the concepts

inform auditors and AI governance professionals evaluating how digital records are preserved, the audience AI-Governance-Jobs.com serves.

Interview Questions

- What is the difference between a forensic disk image and an ordinary backup?
- How does a write blocker protect the integrity of an investigation?
- How do you prove that a disk image is an exact copy of the original?
- Why does a forensic image include deleted and unallocated space?
- How would you handle imaging a drive that is fully encrypted?

Related Certifications

GIAC Certified Forensic Examiner (GCFE) | GIAC Certified Forensic Analyst (GCFA) | EnCase Certified Examiner (EnCE)

Further Reading

- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- NIST Computer Forensics Tool Testing (CFTT)
- SWGDE Best Practices

Key Takeaways

- A forensic image is an exact, bit-for-bit copy, not just the visible files.
- A write blocker guarantees the original is never altered during acquisition.
- Matching hashes prove the image is identical and later prove it is unchanged.
- Imaging captures deleted and unallocated areas where evidence often hides.
- Preserve the original as evidence and analyze only the verified copy.

FAQ

▶ **Why not just copy the files I need?**

▶ **What does a write blocker actually do?**

▶ **Can you image an encrypted drive?**

Related Careers

RELATED ROLES

Dfir Analyst · Forensic Investigator · Incident Responder · Soc Analyst

RELATED CERTIFICATIONS

GIAC Certified Forensic Examiner (GCFE)
GIAC Certified Forensic Analyst (GCFA)
EnCase Certified Examiner (EnCE)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides · Role roadmaps · Salary data · Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Disk Imaging**
3. Go deeper: Digital Evidence
4. Go deeper: Chain of Custody
5. Validate it: work toward **GIAC Certified Forensic Examiner (GCFE)**
6. Find the role: browse current openings

RELATED SHEETS

CS-099 Digital Evidence | CS-100 Chain of Custody | CS-101 Memory Forensics | CS-103 Log Analysis | CS-094 Incident Response: Identification | CS-095 Incident Response: Containment | CS-001 Cybersecurity