CS-100 · Digital Forensics

Chain of Custody

The unbroken, documented record of who handled evidence, when, and why.

Executive Summary

Chain of custody is the continuous, documented history of every person who handled a piece of evidence, along with when, where, and why. It shows that evidence was controlled and unaltered from the moment it was collected to the moment it is presented. A gap in that record can cast doubt on everything the evidence is meant to prove.

What It Is

Chain of custody is the paper and digital trail that accounts for evidence at all times. Each time an item is collected, moved, stored, examined, or transferred, the action is logged with the identity of the person responsible, the date and time, the location, and the reason. For digital evidence this record usually pairs with cryptographic hashes so that the physical trail and the data integrity trail reinforce each other. The goal is simple to state and demanding to maintain: no unexplained gaps and no unaccounted access from acquisition through final disposition.

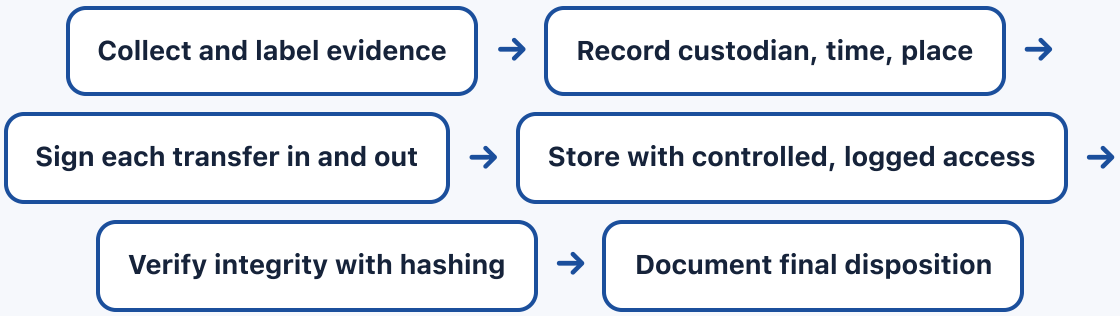
Why It Matters

Evidence with a broken or questionable custody record can be challenged as unreliable, and in legal proceedings it may be excluded entirely. Because digital data can be copied and edited invisibly, the custody record is often what convinces a court, regulator, or opposing expert that the evidence is authentic and unchanged. Beyond the courtroom, disciplined custody protects internal investigations, insurance claims, and regulatory findings from being second-guessed. For professionals, keeping a clean chain of custody is a hallmark of credible, defensible work and a skill that transfers across forensics, incident response, and audit.

How It Works

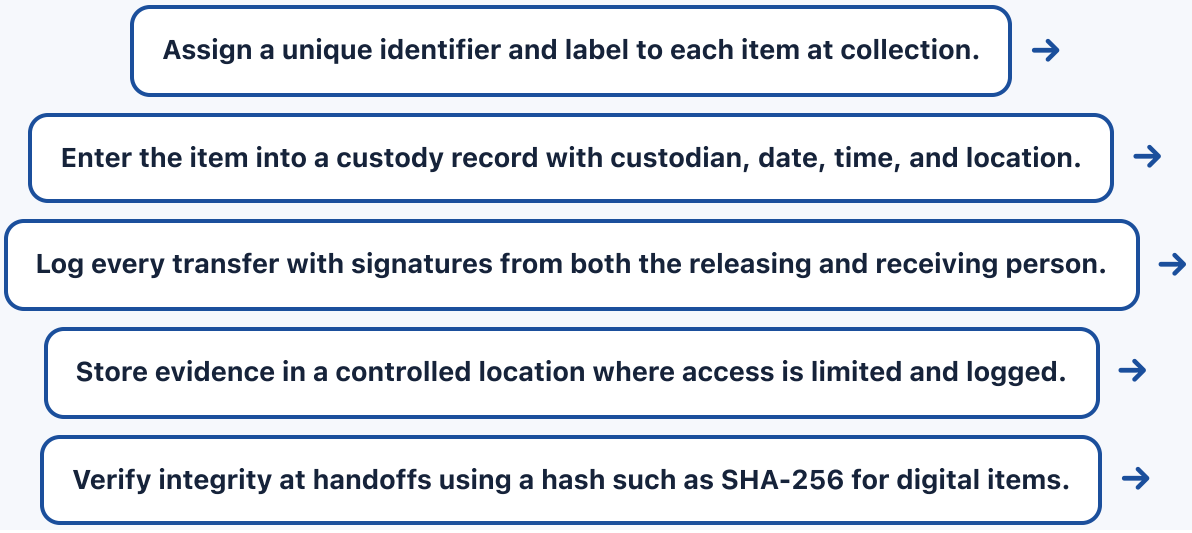
Chain of custody works by making handling transparent and accountable at every step. When evidence is collected, it is labeled with a unique identifier and entered into a custody record. Every subsequent transfer is signed for by the person releasing it and the person receiving it, so responsibility is never ambiguous. Storage is controlled with limited, logged access, and for digital items a hash such as SHA-256 is recorded so any change would be detectable. The record is contemporaneous, meaning it is written as events happen rather than reconstructed afterward. Guidance from NIST and standards bodies such as SWGDE stresses these documentation and control practices; NIST SP 800-86 discusses handling and documentation as part of a sound forensic process.

Architecture Diagram



Custody stays unbroken when every transfer is identified, timed, signed, and logged from collection to disposition.

Visual Workflow



Record final disposition, whether retained, returned, or destroyed.

Common Attacks

- Tampering with stored evidence when access controls are weak
- Substitution of media when items are not uniquely identified
- Undocumented access that creates an unexplained gap in the record
- Timestamp or log manipulation to disguise when handling occurred
- Loss of evidence during transfer when handoffs are not signed

Common Mistakes

- Leaving gaps in the record where an item cannot be accounted for
- Reconstructing the log after the fact instead of recording contemporaneously
- Sharing storage access broadly without logging who entered
- Failing to uniquely label items, making substitution hard to disprove
- Recording the physical trail but neglecting to hash digital contents

Best Practices

- Give every item a unique identifier from the moment of collection
- Record custody events as they happen, not later from memory
- Require dual signatures on every transfer of possession
- Limit and log physical and logical access to stored evidence
- Pair the physical custody record with cryptographic hashes for digital items
- Retain the record for as long as the matter and policy require

Quick Checklist

- [x] Each item uniquely labeled and identified
- [x] Custody record shows an unbroken sequence of custodians

- [x] Every transfer signed by releasing and receiving parties
- [x] Storage access is restricted and logged
- [x] Digital integrity hashes recorded and verifiable
- [x] Final disposition documented

Recommended Tools

Custody log or tracking system
Records custodians, transfers, times, and locations over the evidence lifecycle

Evidence labels and tamper-evident bags
Uniquely identify items and reveal unauthorized access

Hashing utility
Fixes and verifies digital integrity alongside the custody record

Access-controlled storage
Limits and logs who can reach stored evidence

Industry Standards

NIST SP 800-86
Guide to integrating forensic techniques, including handling and documentation

SWGDE best practices
Community guidance on documentation and evidence control

ISO/IEC 27037
Guidelines that address preservation and continuity of digital evidence

Career Relevance

Chain of custody discipline is essential for forensic investigators, DFIR analysts, and incident responders, and it is expected of SOC analysts who may collect the first artifacts. It is equally relevant to legal, audit, and compliance professionals who must vouch for how records were kept, and to privacy and AI governance practitioners who evaluate the defensibility of evidence and data trails, the audience AI-Governance-Jobs.com serves.

Interview Questions

- What is chain of custody and why does a gap in it matter?
- What information should be recorded at each transfer of evidence?
- How does hashing complement the physical custody record for digital evidence?
- Describe how you would store evidence to keep access controlled and logged.
- How do you keep a custody record defensible when many people touch an incident?

Related Certifications

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

Further Reading

- NIST SP 800-86: Guide to Integrating Forensic Techniques into Incident Response
- SWGDE Best Practices
- CISA: Incident Response

Key Takeaways

- Chain of custody is the unbroken, documented history of who handled evidence and when.
- A gap or unexplained access can make evidence unreliable or inadmissible.
- Every transfer should be signed by both the releasing and receiving person.
- For digital evidence, hashing reinforces the physical custody record.
- Contemporaneous records and controlled storage keep the chain defensible.

FAQ

▶ **What breaks a chain of custody?**

▶ **Does chain of custody apply to copies as well as originals?**

▶ **How long should custody records be kept?**

Related Careers

RELATED ROLES

Dfir Analyst · Forensic Investigator · Incident Responder · Soc Analyst

RELATED CERTIFICATIONS

GIAC Certified Forensic Analyst (GCFA) · GIAC Certified Forensic Examiner (GCFE) · 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: **Chain of Custody**
3. Go deeper: Digital Evidence
4. Go deeper: Memory Forensics
5. Validate it: work toward **GIAC Certified Forensic Analyst (GCFA)**
6. Find the role: browse current openings

RELATED SHEETS

CS-099 Digital Evidence | CS-101 Memory Forensics | CS-102 Disk Imaging | CS-103 Log Analysis | CS-094 Incident Response: Identification | CS-095 Incident Response: Containment | CS-001 Cybersecurity