Reliable Context

RELIABLE CONTEXT / RESEARCH & PRACTICAL GUIDANCE

Chain of Custody for Digital Evidence, Collection to Court

> Reliable Context is a kernel of truth: a system of record for organizations that fuse private and public information and must defend every value they act on. One canonical record per real thing, a cited source and an observation date behind every value, unknowns declared rather than left blank, and any past state of the record reproducible.

Published by Reliable Context · 2026-10-29 · chain of custody digital evidence · digital evidence chain of custody · chain of custody form · iso 27037 · digital forensics preservation

Original article: https://reliablecontext.com/articles/chain-of-custody-digital-evidence-explained



In this article

1. The short answer
2. What chain of custody is, and why gaps hurt
3. The handling stages: ISO/IEC 27037
4. Hash values as integrity anchors
5. The custody record
6. Authentication under the US federal rules
7. Cloud and SaaS evidence: custody you do not control
8. Applying custody to business facts, not only files
9. Custody record template

The short answer

A chain of custody for digital evidence is the documented, unbroken account of an item from the moment it is identified to the moment it is presented: what it is, where it came from, who held it, what was done to it, and how anyone can tell it has not changed. For digital items the last question is answered mainly with cryptographic hash values computed at collection and re-checked at every hand-off. In US federal courts, a well-kept custody record supports authentication under Federal Rule of Evidence (FRE) 901, and since 2017 a qualified person's certification of matching hash values can make copied data self-authenticating under FRE 902(14) (FRE 902 and Committee Notes, 2017 Amendment).

This article sets out the stages of evidence handling, the role of hashes, the fields a custody record needs, the US authentication rules, the particular problems of cloud and SaaS evidence, and how the same discipline applies to business facts that are not files. It is educational, not legal advice; rules outside US federal courts differ.

What chain of custody is, and why gaps hurt

NIST's guide to forensics in incident response describes the practice in one sentence: "keeping a log of every person who had physical custody of the evidence, documenting the actions that they performed on the evidence and at what time, storing the evidence in a secure location when it is not being used, making a copy of the evidence and performing examination and analysis using only the copied evidence, and verifying the integrity of the original and copied evidence". It adds that if it is unclear whether evidence needs preserving, "by default it generally should be preserved" (NIST SP 800-86, §3.1.2).

A gap in that account does not prove tampering. It gives an opponent room to argue tampering, and it forces the proponent to fill the gap with testimony. Digital evidence is especially exposed because, as NIST IR 8387 puts it, "digital files are very easy to change, so maintaining the integrity of the data is a critical concern" (NIST IR 8387, §3.2). A changed byte leaves no physical mark.

Every custody record has to answer five questions:

Question	What the record must show	Typical evidence
What is it?	A unique identifier and description of the item	Evidence number, file name, device serial, size
Where did it come from?	Original source and how it was obtained	Source system, custodian, collection method, tool and version
Who held it?	Every person or system with custody, in sequence	Signed or system-logged hand-offs with times
What happened to it?	Every action: copy, image, transfer, analysis	Action log with purpose and operator
How do we know it did not change?	Integrity verification at each step	Hash values at collection and at each verification

The handling stages: ISO/IEC 27037

ISO/IEC 27037:2012 "provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence that can be of evidential value". ISO says it aims to assist organizations in disciplinary procedures and to facilitate "the exchange of potential digital evidence between jurisdictions" (ISO/IEC 27037:2012). ISO's catalogue lists it as last reviewed and confirmed in 2018.

The four activities in the title give a usable sequence:

1. **Identification.** Recognize what might be evidence and where it resides: a laptop, a mailbox, a database table, a SaaS workspace.
2. **Collection.** Take physical items into custody, such as removing a device.
3. **Acquisition.** Create a copy of the data, such as a forensic image or an export, when taking the original is impossible or undesirable.
4. **Preservation.** Protect the item and copies from alteration or destruction for as long as they may be needed.

NIST SP 800-86 organizes forensic work into four phases, "collection, examination, analysis, and reporting" (NIST SP 800-86). In civil discovery, the Electronic Discovery Reference Model (EDRM) runs from identification through preservation, collection, processing, review, production and presentation; in the current model, EDRM 2.0, it defines preservation as "safeguarding relevant ESI and documents against alteration or destruction" (EDRM Model). The three frameworks use different words for overlapping steps. Custody documentation runs through all of them.

Hash values as integrity anchors

A **cryptographic hash function** maps any input to a fixed-length value, such that a change to the input produces a different value. NIST IR 8387 summarizes the practical consequence: "A file can be uniquely identified by its hash. Any change to a file will result in a different hash" (NIST IR 8387, §3.2). The Federal

Rules' 2017 committee note says the same in legal terms: "If the hash values for the original and copy are different, then the copy is not identical to the original. If the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical" (FRE 902, Committee Notes 2017).

A one-character change is enough. The SHA-256 value of the fictional sample text `Halden Therapeutics AG - board minutes 2026-02-11 (fictional sample)` begins `63e5eb7e`…; adding a final full stop changes it to `55d5488a`….

NIST IR 8387 sets out working rules for hashes (§3.2 and §9):

- **Hash as close to collection as possible.** The guidance lists the weaknesses a hash does not cover, including changing "the evidence before it is hashed" and changing the evidence, re-hashing it and overwriting "a stored hash".
- **Store hashes separately.** Hashes "should be stored separately from the image or file in a secure location", so that people with access to the evidence cannot alter the record of its hash. Hash chains are mentioned as "a useful technology for securing hashes".
- **Prefer current algorithms.** Older algorithms such as MD5 or SHA-1 are acceptable "if needed but newer algorithms are preferred"; the guidance points to FIPS 180-4, the Secure Hash Standard, for examples.
- **Plan for mismatches.** Because "the change of even one bit will cause the hash to be completely different", keep more than one copy, and consider block hashes to limit the amount of data under suspicion.

During acquisition, NIST SP 800-86 recommends write-blockers, which prevent the analysis system from writing to the source media, and computing message digests of the original and the copy and comparing them (NIST SP 800-86, §3.1.2 and §4.2.2).

The custody record

A custody record is an append-only log. Each entry should capture who, what, when, where, why and the integrity check. The example below is fictional. **Halden Therapeutics AG is a fictional company**; the matter, people and devices are invented. The hash values are real SHA-256 digests of the stated sample text, shortened for display.

Item E-0007: board minutes, 11 February 2026, PDF exported from Halden's document management system, 412 KB.

#	Time (UTC)	Who	Action	Location	Purpose	SHA-256	Verified
1	2026-03-02 09:14	P. Lindqvist, IT admin	Identified in DMS folder /Board/2026	DMS, Basel	Litigation hold notice LH-12	—	—
2	2026-03-02 09:40	P. Lindqvist	Exported native file and system metadata using DMS export v7.2	DMS to evidence share	Collection	63e5eb7e… bedae	Computed at export

#	Time (UTC)	Who	Action	Location	Purpose	SHA-256	Verified
3	2026-03-02 10:05	P. Lindqvist to R. Asante, forensic analyst	Transfer of export on encrypted drive D-31	Evidence room 2	Hand-off	63e5eb7e… bedae	Match
4	2026-03-03 08:30	R. Asante	Working copy made; original sealed	Forensic workstation FW-4	Examination on copy only	63e5eb7e… bedae	Match (original and copy)
5	2026-03-09 14:20	R. Asante	Text extracted for review platform	FW-4	Processing	63e5eb7e… bedae	Match before processing
6	2026-06-15 09:00	R. Asante	Integrity re-check of sealed original	Evidence room 2	Pre-production verification	63e5eb7e… bedae	Match

The hash recorded at entry 2 is also written to a case-management system to which neither Lindqvist nor Asante has write access, following the NIST IR 8387 recommendation that the hash record be beyond the control of the people handling the evidence.

Common failures, and what they cost:

Failure	Consequence
Hash computed only after transfer to the analyst	Cannot show the item was unchanged between collection and transfer
Analysis performed on the original	Original's integrity becomes an argument rather than a fact
Hash stored in the same folder as the file	Anyone who could alter the file could alter the hash
Export without system metadata (author, created, modified)	Distinctive characteristics for FRE 901(b)(4) are lost
Shared account used for collection	Custody entry is not attributable to a person
Collection tool and version not recorded	The process cannot be described under FRE 901(b)(9)

Authentication under the US federal rules

Authentication is a threshold question: is the item what its proponent says it is? FRE 901(a) requires "evidence sufficient to support a finding that the item is what the proponent claims it is" (FRE 901). Rule 901(b) lists examples, "not a complete list". Three matter most for digital evidence:

- **901(b)(1), testimony of a witness with knowledge**, such as the person who performed the collection.
- **901(b)(4), distinctive characteristics**: "the appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances". Metadata and hash values are distinctive characteristics.
- **901(b)(9), evidence about a process or system**: "Evidence describing a process or system and showing that it produces an accurate result."

The 2017 amendments added two self-authentication routes that replace a live foundation witness with a written certification (FRE 902):

Rule	Covers	Mechanism
902(13)	"A record generated by an electronic process or system that produces an accurate result"	Certification of a qualified person, complying with the certification requirements of 902(11) or (12), plus notice
902(14)	"Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification"	Certification of a qualified person, plus notice

The committee note to 902(14) explains that copied data is "ordinarily authenticated by 'hash value'", and that the rule "allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original". It is also "flexible enough to allow certifications through processes other than comparison of hash value". The note to 902(13) says the certification must contain information "sufficient to establish authenticity were that information provided by a witness at trial" and that the rule allows the 901(b)(9) foundation to be established by certification.

Two limits are stated in the notes. A certification under either rule establishes only authenticity; "the opponent remains free to object to admissibility of the proffered item on other grounds—including hearsay, relevance, or in criminal cases the right to confrontation". And the reference to 902(11) is to procedure only: these rules do not prove the business-records requirements of Rule 803(6). A perfectly hashed spreadsheet can be authentic and still inadmissible, or authentic and wrong.

Cloud and SaaS evidence: custody you do not control

Most organizational evidence now lives on infrastructure owned by someone else: hosted email, collaboration suites, CRM and ticketing systems. Three practical consequences follow.

1. **There is often no original medium to image.** Acquisition means an export through an API or an admin console. The custody record should describe the export method, tool version, account used, query or scope, and time window, because the process itself is what 901(b)(9) or 902(13) will need described.
2. **The provider's records are part of the chain.** Audit logs of the SaaS platform (who accessed or exported the data) are evidence of custody before collection. Preserve them alongside the content, under the same legal hold.
3. **Hashes start at export.** A hash computed on an export proves the export has not changed since, not that it matches what the user saw in the application. Keep the platform's own identifiers and version numbers (message IDs, revision IDs) so the export can be tied back to the source state.

Retention settings in the platform can delete data on a schedule, so preservation under a hold usually has to be configured in the platform itself, not only by collecting a copy.

Applying custody to business facts, not only files

The same five questions apply to an individual fact an organization relies on, such as a supplier's registered address, a product's authorization status or a counterparty's ultimate parent. When such a fact is later disputed, a regulator or court will ask where it came from, when it was read, who recorded it, and whether it has changed since. A fact with a retained copy of its source, a verbatim excerpt, a read date and a hash of the retained source has, in effect, a chain of custody. A fact typed into a master-data screen has none. The site's chain of custody glossary entry, its method note on retaining source copies and its study of preserving evidence when cited sources change work through that case.

Custody record template

At minimum, for each item:

- **Item:** unique ID, description, original location, custodian, size, and native format.
- **Source system:** name, version, and account used for collection.
- **Collection:** method, tool and version, scope or query, start and end time, operator.
- **Integrity:** algorithm (for example SHA-256), value at collection, where the value is stored, who can modify that store.
- **Hand-offs:** from, to, time, location, purpose, integrity check result.
- **Actions:** each copy, image, processing step or analysis, with operator, time, purpose and whether it touched the original.
- **Storage:** location, access controls, and environmental or retention conditions.
- **Disposition:** release, return or destruction, with authority and date.

And four rules: hash at collection, store hashes out of the handlers' reach, analyse copies only, and never leave a hand-off unlogged.

The same discipline is what Reliable Context's published guarantee describes for organizational facts: a cited, verbatim, dated source behind every value, and any past state reproducible.

This article summarizes US federal rules and international guidance as of 28 October 2026 and is not legal advice.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.law.cornell.edu/rules/fre/rule_902
2. https://csrc.nist.gov/pubs/sp/800/86/final
3. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf
4. https://www.iso.org/standard/44381.html
5. https://edrm.net/edrm-model
6. https://www.law.cornell.edu/rules/fre/rule_901

THE PUBLISHER

About Reliable Context

Reliable Context is a system of record for organizations that fuse private and public information and must defend every value they act on.

The guarantees

One canonical record per real thing: duplicates resolve by rule, ambiguity is shown rather than hidden, and related organizations relate without ever being merged. A verbatim, cited source and an observation date sit behind every value. Unknowns are declared as not found, blocked or not applicable with a reason, never left as an empty cell. Any past state of the record is reproducible, together with what changed since.

Where it runs

It runs inside the customer's perimeter, one database per organization. Permitted sources, model routing, reader clearance and retention are set as the customer's own policies, and every value is exportable with its chain of custody for an auditor or regulator.

What it is not

It is not a vector database or a RAG framework, not a data catalog, MDM or data-quality suite, not a CRM or data-enrichment vendor, and not a chatbot or AI assistant. Where a reader needs one of those, the honest answer is to say so and point them there.

Visit

See Reliable Context.

Reliable Context is in production use in two sectors; more than six thousand of its identity decisions were made by rule and none has been reversed. Articles published here explain general practice, cite their primary and academic sources, and name the jurisdiction of any regulatory rule they describe. They are not legal, regulatory or compliance advice for a specific organization, and requirements change.

Website: https://reliablecontext.com

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.