INVESTIGATION · FOUNDATIONS

The Chain of Custody and the Integrity of Evidence

How investigators show that evidence is what they say it is and has not been changed, from sealed bags and custody logs to forensic images and hash values, and what happens when the chain breaks.

ModQu research article · 2,472 words · 22 references (APA 7th edition)

An item of evidence is only useful if the people relying on it can trust two things: that it is the same item that was collected, and that it has not been altered, contaminated or substituted along the way. The **chain of custody** is the documented record that answers both questions. It shows who collected the item, when and where, how it was packaged, everyone who handled it afterwards, where it was stored, and what was done to it. Together with the practices that protect evidence from damage, it underpins the integrity of every investigation that relies on physical or digital material.

This article explains what the chain of custody is, why it matters, how it works for physical and digital evidence, and what happens when it fails. Although the concept comes from criminal justice, the same principles apply to corporate investigations, regulatory inquiries, laboratory testing and any setting where findings may be challenged.

Why integrity matters

Evidence can go wrong in four main ways. It can be **lost**, so that it is unavailable when needed. It can be **substituted** or mixed up with other items, so that what is examined is not what was collected. It can be **contaminated**, for example by DNA transferred from an investigator's gloves or by another sample in the laboratory. And it can be **altered**, deliberately or accidentally, as when a computer file's dates change because someone opened it on the original device.

Any of these can lead to a wrong conclusion. Even when nothing has actually gone wrong, an inability to show that the evidence was handled properly can be fatal to its use. Courts and tribunals ask whether the party offering evidence can show that it is what it purports to be. A gap in the record invites the argument that something might have happened during the gap, and the burden of answering that argument falls on the investigator (Giannelli, 1983; Roberts & Zuckerman, 2010).

Concerns about evidence handling extend beyond individual cases. The United States National Research Council (2009) report on forensic science identified inconsistent standards, limited oversight and a lack of independence in many laboratories as threats to the reliability of forensic evidence generally. Saks and Koehler (2005) argued that forensic identification needed to move towards the empirical testing and error measurement normal in other sciences. Good custody practice is one of the foundations on which such reliability is built.

The principle behind the chain

The idea that evidence must be protected rests on an observation attributed to the French forensic pioneer Edmond Locard: when two objects come into contact, material is transferred between them (Locard, 1930). The principle explains why trace evidence exists at all, but it also explains why evidence is vulnerable. Every person who touches an item, every bag it is placed in and every surface it rests on can add or remove material. The chain of custody does not prevent transfer. It records the handling so that the risk can be assessed, and it is combined with procedures that keep transfer to a minimum.

The stages of custody

Although details differ between fields and jurisdictions, custody follows the same broad stages.

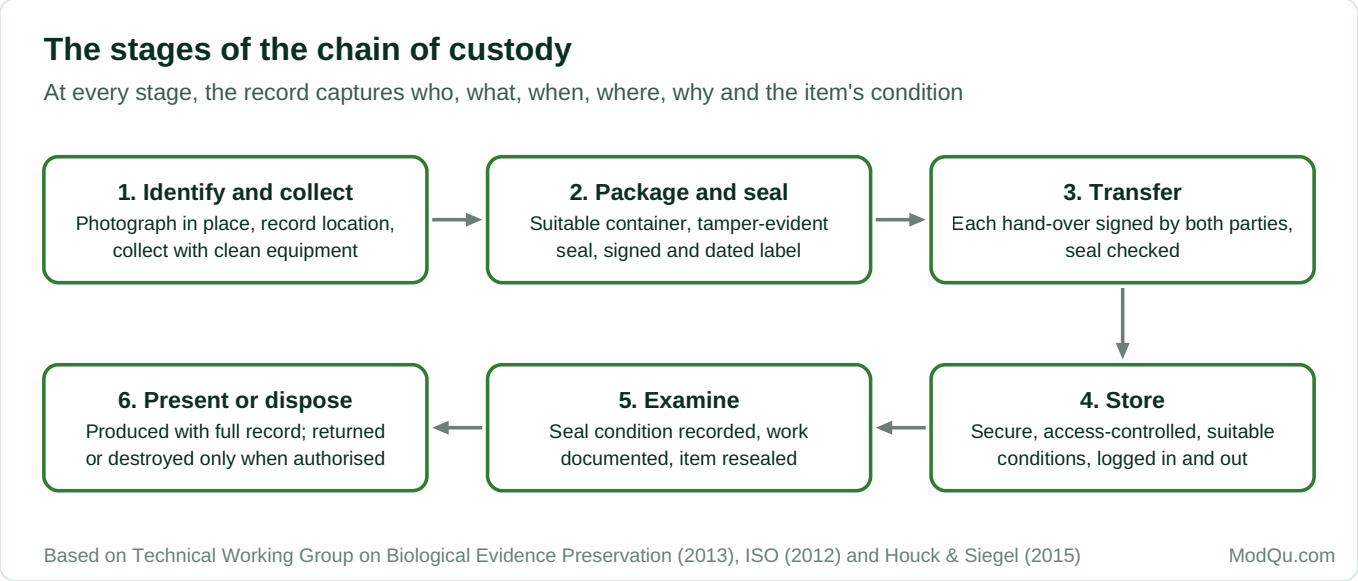


Figure 1. The six stages through which evidence typically passes. A gap in the record at any stage weakens the evidence, even if the item itself was not affected. Diagram by ModQu.

Identification and collection

Before anything is moved, the item is photographed and its position recorded, so that its original context can be reconstructed later. The person collecting it wears appropriate protective equipment, uses clean tools and handles it as little as possible. Each item receives a unique identifier, and the collector records what it is, where it was found, when it was collected and by whom (Houck & Siegel, 2015).

Packaging and sealing

Packaging protects the item and makes tampering visible. Biological material is usually packaged in breathable containers and dried, since moisture encourages degradation, while some liquids and volatile materials need airtight containers (Technical Working Group on Biological Evidence Preservation, 2013). The package is sealed with tamper-

evident tape, and the collector signs or initials across the seal and records the date. Items that could cross-contaminate one another, such as clothing from a suspect and from a victim, are packaged separately and often handled by different people.

Transfer

Each time an item changes hands, both the person releasing it and the person receiving it sign the custody record, note the date and time, and confirm that the seal is intact. The fewer transfers, the simpler the chain and the fewer opportunities for error.

Storage

Evidence is held in a secure store with controlled access, where every entry and exit is logged. Storage conditions should match the type of evidence: cool, dry and dark for many biological samples; protected from magnetic fields and static for some electronic media. Guidance on the preservation of biological evidence stresses tracking systems that can locate any item quickly and records that show its storage history throughout (Technical Working Group on Biological Evidence Preservation, 2013).

Examination

When an item is examined, the examiner records the condition of the seal before opening it, documents everything done to the item, and reseals it with a new signed seal afterwards. Laboratories accredited to ISO/IEC 17025 must have procedures for the receipt, handling, protection, storage and retention of test items, and for protecting their integrity (International Organization for Standardization [ISO], 2017). In England and Wales, the statutory code issued by the Forensic Science Regulator (2023) sets similar requirements for forensic science activities.

Presentation and disposal

Finally, the item is produced to a court, tribunal or decision-maker together with its custody record. Evidence is retained for as long as legal rules or organisational policy require. Premature disposal can prevent later re-examination, which has proved crucial in cases where new DNA techniques have exonerated wrongly convicted people.

Digital evidence

Digital evidence raises special problems. It is invisible without tools, easily changed, and often exists in many copies. Merely switching on a computer or opening a file can change dates, logs and other data that may later be relied on. The guiding principles used by police in the United Kingdom summarise the response (Association of Chief Police Officers [ACPO], 2012):

1. No action should change data held on a device or storage medium that may later be relied on in court.
2. Where it is necessary to access original data, the person doing so must be competent and able to explain the relevance and implications of their actions.

3. An audit trail of all processes applied to digital evidence should be created and preserved, and an independent third party should be able to repeat those processes and achieve the same result.
4. The person in charge of the investigation has overall responsibility for ensuring these principles are followed.

In practice, investigators make a **forensic image**, a bit-for-bit copy of a storage device, usually through a write-blocker that prevents any change to the original. They then calculate a **hash value** for both the original and the copy. A hash function, such as those in the Secure Hash Standard, produces a short fixed-length value from any input; changing even a single bit of the input produces a completely different value (National Institute of Standards and Technology [NIST], 2015). If the hash of the copy matches the hash of the original, the copy is exact. Re-calculating the hash at later stages shows that the evidence has not changed since it was acquired.

The international standard ISO/IEC 27037 sets out guidelines for identifying, collecting, acquiring and preserving digital evidence, and emphasises that the methods used should be auditable, repeatable, reproducible and justifiable (ISO, 2012). NIST guidance on integrating forensic techniques into incident response stresses that organisations should be ready to preserve evidence before an incident occurs, because evidence gathered hastily during a crisis is often incomplete or poorly documented (Kent et al., 2006). Casey (2011) and Mason and Seng (2017) discuss how courts have approached the authenticity and reliability of electronic records.

Live systems, cloud services and mobile phones complicate the picture. A running server cannot always be switched off without losing important data held in memory, so investigators may need to capture it while it runs, which inevitably changes some data. Cloud data may be held in another jurisdiction by a provider who controls the copying. In such cases the investigator cannot follow the ideal of leaving the original untouched, so the emphasis shifts to recording exactly what was done and why. Horsman (2019) argues that the field also needs better testing of the forensic tools themselves, since an unreliable tool can undermine the integrity of evidence even when custody procedures are followed perfectly.

Integrity of interpretation

Integrity is not only about the physical or digital item. It also concerns the information that reaches the person interpreting it. Research on cognitive bias has shown that forensic examiners who are told contextual details of a case, such as that a suspect has confessed, can be influenced in how they interpret ambiguous evidence (Kassin et al., 2013). Dror (2020) argues that bias can enter at many points, from the data itself and reference materials to the examiner's expectations and organisational pressures. Procedures such as limiting examiners to the information they need and documenting what they were told are a form of custody for the evidence's meaning, not just for the evidence itself.

When the chain breaks

A broken chain does not automatically make evidence worthless. Courts generally treat gaps as going to the weight of evidence rather than its admissibility, unless the gap is so serious that the item cannot be authenticated at all (Giannelli, 1983). The party offering the evidence may be able to fill gaps with testimony about routine practice or other records. Nevertheless, a weak chain gives the opposing side an opening, and in close cases it can be decisive.

The consequences can be severe when failures are systemic. Investigations into laboratory misconduct and contamination in several countries have led to the review of thousands of cases. Gill (2014) describes how errors in the handling and interpretation of DNA evidence, including contamination and transfer, have contributed to miscarriages of justice. In the United States, the Supreme Court's decision in *Melendez-Diaz v. Massachusetts* (2009) confirmed that the analysts who produce forensic reports can be required to testify, which in turn makes the reliability of laboratory practices, including custody, open to direct challenge.

The following table summarises common failures and their usual consequences.

Failure	Example	Typical consequence
Undocumented transfer	Item passed between officers without a signature	Authenticity challenged; testimony needed to fill the gap
Broken or missing seal	Package opened and not resealed	Possibility of tampering or contamination raised
Poor storage	Biological sample stored damp and warm	Degradation; results unreliable or impossible
Mixed packaging	Suspect and victim clothing in one bag	Transfer between items; findings undermined
Original device used directly	Investigator browses files on a seized laptop	Metadata altered; reliability challenged
Premature disposal	Samples destroyed after conviction	No possibility of later re-examination

Beyond criminal cases

The chain of custody is equally important in other settings. In anti-doping, athletes' samples are collected, sealed and transported under strict procedures because a positive result can end a career; the international standard for testing requires documentation of every stage from sample collection to laboratory receipt (World Anti-Doping Agency [WADA], 2021). Workplace drug testing, environmental sampling and product testing follow similar rules.

In corporate investigations, the evidence is more often documents, emails, financial records and devices than physical traces. The same principles apply: identify the material, collect it without changing it, record its source and handling, keep it secure and be able to show that what was analysed is what was collected. A company that dismisses an employee on the basis of emails that cannot be shown to be authentic and complete may face a successful claim for unfair dismissal, even if the employee was in fact guilty.

A hypothetical example shows how this works in practice. A finance manager is suspected of approving payments to a company owned by a relative. The investigator arranges for the manager's work laptop to be collected by the IT department in the presence of a witness, without being switched on, and placed in a sealed, labelled bag. A forensic specialist later makes an image of the hard drive through a write-blocker and records matching hash values for the original and the copy. Emails are exported from the company's server by an administrator who documents the search terms, date ranges and export tool used, and produces a hash value for the export file. Bank and payment records are obtained from the finance system with a report showing who ran the query and when.

When the manager later claims that the incriminating emails were planted, the company can show that the laptop was not used after collection, that the image is an exact copy, and that the emails on the server match those on the laptop. Without that record, the dispute would turn on the credibility of individual staff members. With it, the integrity of the evidence can be demonstrated rather than merely asserted.

The standards governing expert evidence reinforce these demands. Under *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993), courts in the United States consider whether the methods an expert relies on are reliable, and evidence that cannot be shown to have been handled properly undermines any method applied to it.

Good practice in summary

The literature and standards discussed here point to a short set of practical rules:

- Plan for evidence before an investigation begins, with procedures, packaging, storage and trained staff in place (Kent et al., 2006).
- Record each item at the point of collection with a unique identifier, and photograph it in place.
- Use tamper-evident packaging and sign across seals.
- Keep transfers to a minimum and record every one.
- Store evidence securely, in suitable conditions, with logged access.
- For digital evidence, work on verified copies, not originals, and use hash values to show integrity.
- Document every examination so that an independent person could repeat it.
- Control the information given to examiners, as well as the items themselves.
- Retain evidence for as long as it might be needed, and dispose of it only with proper authority.

Implications for research and data

The same logic applies to research data. A survey dataset passes through many hands: collection, cleaning, weighting, analysis and reporting. Each step can introduce errors or unrecorded changes. Keeping raw data unaltered, recording every transformation in scripts rather than manual edits, using checksums to confirm that files have not changed, and keeping a log of who did what and when are the research equivalents of a chain of custody. They allow anyone who later questions a finding to trace it back to the original responses, and they protect the organisation that produced it. Evidence that can be traced is evidence that can be trusted.

References

Association of Chief Police Officers. (2012). *ACPO good practice guide for digital evidence* (Version 5). ACPO.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet* (3rd ed.). Academic Press.

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

Dror, I. E. (2020). Cognitive and human factors in expert decision making: Six fallacies and the eight sources of bias. *Analytical Chemistry, 92*(12), 7998–8004. https://doi.org/10.1021/acs.analchem.0c00704

Forensic Science Regulator. (2023). *Forensic science regulator code of practice*. Home Office.

Giannelli, P. C. (1983). Chain of custody and the handling of real evidence. *American Criminal Law Review, 20*(4), 527–568.

Gill, P. (2014). *Misleading DNA evidence: Reasons for miscarriages of justice*. Academic Press.

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. *Digital Investigation*, *28*, 163–175. https://doi.org/10.1016/j.diin.2019.01.009

Houck, M. M., & Siegel, J. A. (2015). *Fundamentals of forensic science* (3rd ed.). Academic Press.

International Organization for Standardization. (2017). *General requirements for the competence of testing and calibration laboratories* (ISO/IEC Standard No. 17025:2017).

International Organization for Standardization. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC Standard No. 27037:2012).

Kassin, S. M., Dror, I. E., & Kukucka, J. (2013). The forensic confirmation bias: Problems, perspectives, and proposed solutions. *Journal of Applied Research in Memory and Cognition*, *2*(1), 42–52. https://doi.org/10.1016/j.jarmac.2013.01.001

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response* (NIST Special Publication 800-86). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Locard, E. (1930). The analysis of dust traces. Part I. *American Journal of Police Science, 1*(3), 276–298. https://doi.org/10.2307/1147154

Mason, S., & Seng, D. (Eds.). (2017). *Electronic evidence* (4th ed.). Institute of Advanced Legal Studies, University of London.

Melendez-Diaz v. Massachusetts, 557 U.S. 305 (2009).

National Institute of Standards and Technology. (2015). *Secure hash standard (SHS)* (FIPS PUB 180-4). https://doi.org/10.6028/NIST.FIPS.180-4

National Research Council. (2009). *Strengthening forensic science in the United States: A path forward*. National Academies Press. https://doi.org/10.17226/12589

Roberts, P., & Zuckerman, A. (2010). *Criminal evidence* (2nd ed.). Oxford University Press.

Saks, M. J., & Koehler, J. J. (2005). The coming paradigm shift in forensic identification science. *Science, 309*(5736), 892–895. https://doi.org/10.1126/science.1111565

Technical Working Group on Biological Evidence Preservation. (2013). *The biological evidence preservation handbook: Best practices for evidence handlers* (NISTIR 7928). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.7928

World Anti-Doping Agency. (2021). *International standard for testing and investigations*. WADA.