INVESTIGATION · METHOD AND THE FUTURE

The Role of Audit Trails in Reproducible Investigations

An audit trail records who did what, when and why during an investigation. This article explains what a good audit trail contains, how it makes findings reproducible and defensible, how to protect it from tampering, and common gaps.

ModQu research article · 777 words · 8 references (APA 7th edition)

An investigation's findings are only as credible as the record of how they were reached. An audit trail is that record: a chronological log of the actions taken during an investigation, who took them, when, with what tools and for what reason. It allows another person to retrace the steps, check that evidence was handled properly and, ideally, reproduce the results. Without one, even a correct finding can be impossible to defend.

Why audit trails matter

Reproducibility is a central value in science. Peng (2011) argues that when full replication of a study is not possible, making the data and code available so that others can reproduce the analysis is the minimum standard. Sandve et al. (2013) recommend recording every step that produced a result, keeping the exact versions of tools, and avoiding manual changes that leave no trace. The same principles apply to investigations. A reviewer, regulator, court or the person investigated should be able to see how each finding was reached and to check it.

Audit trails also protect the investigator. Guidance on digital evidence requires that an audit trail of all processes applied to evidence be created and preserved, so that an independent third party could examine those processes and achieve the same result (Association of Chief Police Officers [ACPO], 2012). International standards make the same point for the identification, collection and preservation of digital evidence (International Organization for Standardization [ISO], 2012). In criminal cases in England and Wales, investigators must record and retain information that may be relevant, so that it can be reviewed for disclosure (Criminal Procedure and Investigations Act 1996).

What to record

What an investigation audit trail should record

Each entry answers who, what, when, how and why

	What to record	Why it matters
Decisions	Lines of enquiry opened or closed, and the reasons	Shows that alternatives were considered
Evidence handling	Collection, transfer, storage, copying, hash values	Proves integrity and chain of custody
Analysis	Tools, versions, settings, queries and filters	Allows the analysis to be repeated
Contacts	Interviews, requests, who was present	Shows fairness and completeness
Changes	Corrections to records and the reason	Prevents silent alteration

Based on ACPO (2012), ISO (2012) and Sandve et al. (2013) ModQu.com

Figure 1. The main categories of entries in an investigation audit trail, and the purpose each serves. Diagram by ModQu.

Entries should be made at the time, not reconstructed later, and should be specific. "Searched email" is not enough; "Searched the mailbox export of 12 March, version 2, for the terms 'invoice' and 'Supplier X', using tool Y version 4.1; 312 results; 27 reviewed as relevant" allows the step to be repeated.

Protecting the trail

An audit trail is useful only if it can be trusted. Electronic systems should generate logs automatically, record the identity of each user, and prevent entries from being edited or deleted without a further logged entry. Regulations for electronic records in some industries require exactly this: secure, computer-generated, time-stamped audit trails that record changes without obscuring the earlier information (Electronic Records; Electronic Signatures, 2023). Schneier and Kelsey (1999) describe cryptographic techniques that make it impossible to alter earlier log entries without detection, even if an attacker gains control of the system. Guidance on log management stresses protecting logs, synchronising clocks and retaining logs for a defined period (Kent & Souppaya, 2006).

Common gaps

Typical weaknesses include decisions made in meetings or phone calls that are never recorded, analysis done in spreadsheets with no record of the formulas or filters used, evidence copied without hash values, and reasons for closing a line of enquiry left unstated. Investigators also often fail to record negative results, such as a search that found nothing, even though these are part of the evidence. Each gap makes the investigation harder to review and easier to challenge.

Practical steps

Organisations can build reliable audit trails by using case management systems that log activity automatically, adopting a standard decision log format, recording tool versions and settings as a matter of routine, hashing evidence on receipt, and reviewing the trail at key stages. Small teams without specialist systems can keep a dated, numbered log in a write-protected document, and save copies of analysis files at each stage.

A short example

The following hypothetical case shows the value of a good trail. A company dismisses an employee for falsifying expense claims, and the employee brings a claim for unfair dismissal. At the tribunal, the employee's lawyer argues that the investigator selected only the claims that looked suspicious and ignored others that would have explained the pattern. Because the investigator's log records the full export of 420 claims, the filters applied, the 38 claims selected for review and the reasons each was selected or excluded, the company can show that the selection was systematic. A second analyst repeats the steps from the log and obtains the same 38 claims. The tribunal accepts that the investigation was fair. Without the log, the same findings might have been rejected as one-sided.

Conclusion

An audit trail turns an investigation from a set of conclusions into a process that others can check. By recording decisions, evidence handling, analysis, contacts and changes at the time they occur, and protecting that record from alteration, investigators make their findings reproducible and defensible.

References

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

Criminal Procedure and Investigations Act 1996, c. 25 (UK).

Electronic Records; Electronic Signatures, 21 C.F.R. pt. 11 (2023).

International Organization for Standardization. (2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence* (ISO/IEC 27037:2012).

Kent, K., & Souppaya, M. (2006). *Guide to computer security log management* (NIST Special Publication 800-92). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

Peng, R. D. (2011). Reproducible research in computational science. *Science, 334*(6060), 1226–1227. https://doi.org/10.1126/science.1213847

Sandve, G. K., Nekrutenko, A., Taylor, J., & Hovig, E. (2013). Ten simple rules for reproducible computational research. *PLoS Computational Biology, 9*(10), Article e1003285. https://doi.org/10.1371/journal.pcbi.1003285

Schneier, B., & Kelsey, J. (1999). Secure audit logs to support computer forensics. *ACM Transactions on Information and System Security, 2*(2), 159–176. https://doi.org/10.1145/317087.317089