INVESTIGATION · DIGITAL INVESTIGATION

Digital Forensics: Principles and Process

Almost every investigation now involves digital evidence. This article explains the principles that make digital evidence reliable, the stages of a forensic examination, the challenges of phones, cloud services and volume, and the limits that investigators and courts must keep in mind.

ModQu research article · 2,358 words · 23 references (APA 7th edition)

Phones, laptops, servers, cloud accounts, cars, doorbells and fitness trackers record what people do, where they go and whom they contact. Almost every investigation, whether criminal, corporate, regulatory or civil, now involves some digital evidence. Digital forensics is the discipline of identifying, preserving, examining and presenting that evidence in a way that can withstand scrutiny.

Digital evidence has unusual properties. It is invisible without tools, it can be changed without trace by the simple act of looking at it, it exists in many copies across many devices and services, and its meaning often depends on how software recorded it. These properties shape the principles and methods of the discipline. This article explains those principles, sets out the stages of a forensic examination, describes the main challenges facing the field and considers how digital evidence should be interpreted.

Origins and scope

Digital forensics grew out of efforts by law enforcement agencies in the 1980s and 1990s to examine computers seized in criminal cases (Pollitt, 2010). Early work focused on recovering files from hard drives. The field now covers computers, mobile devices, networks, cloud services, memory, vehicles, embedded devices and more. A research agenda set out at the first Digital Forensic Research Workshop defined digital forensics as the use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence (Palmer, 2001).

Casey (2011) emphasises that digital evidence should be treated like any other forensic evidence: subject to the same requirements of reliability, documentation and scientific method, and interpreted in light of the case as a whole.

Core principles

Guidance for practitioners rests on a small number of principles. The good practice guide used by police in the United Kingdom sets out four (Association of Chief Police Officers [ACPO], 2012):

1. No action should change data held on a device 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, so that an independent third party could repeat them and reach the same result.
4. The person in charge of the investigation is responsible for ensuring that the law and these principles are followed.

The international standard ISO/IEC 27037 expresses similar ideas, emphasising that the handling of digital evidence should be auditable, repeatable, reproducible and justifiable (International Organization for Standardization [ISO], 2012).

These principles translate into a few core practices. Investigators work on verified copies rather than originals wherever possible. They use write-blocking hardware or software to prevent changes when copying storage devices. They calculate cryptographic hash values, using standard algorithms such as those in the SHA-2 family (National Institute of Standards and Technology [NIST], 2015), to show that a copy is identical to the original and has not changed since it was made. And they document every step.

The process

Models of the digital forensic process differ in detail but share a common structure (Reith et al., 2002; Kent et al., 2006).

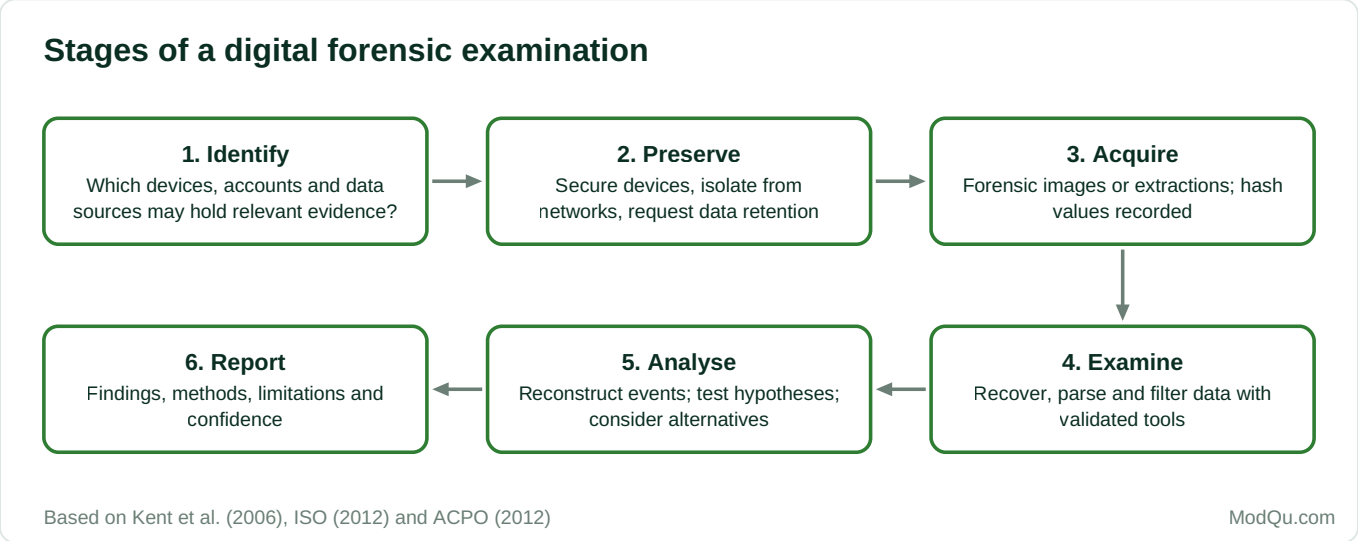


Figure 1. The main stages of a digital forensic examination. Documentation runs through every stage, so that another examiner could repeat the work. Diagram by ModQu.

Identification

The first task is to work out where relevant evidence may be. A modern case may involve a suspect's phone and laptop, a company's email server, cloud storage, messaging applications, social media accounts, payment records, security cameras and records held by telecommunications providers. Identification should be guided by the questions the investigation needs to answer, not by a desire to collect everything.

Preservation

Digital evidence can be lost quickly. A phone can be wiped remotely, cloud data can be deleted, logs can be overwritten, and data in a computer's memory disappear when it is switched off. Preservation may involve isolating a phone from networks, photographing a screen before touching a device, asking a service provider to preserve an account, or capturing data from a running system. Guidance on evidence collection recommends gathering the most volatile data first, since it will be lost soonest (Brezinski & Killalea, 2002).

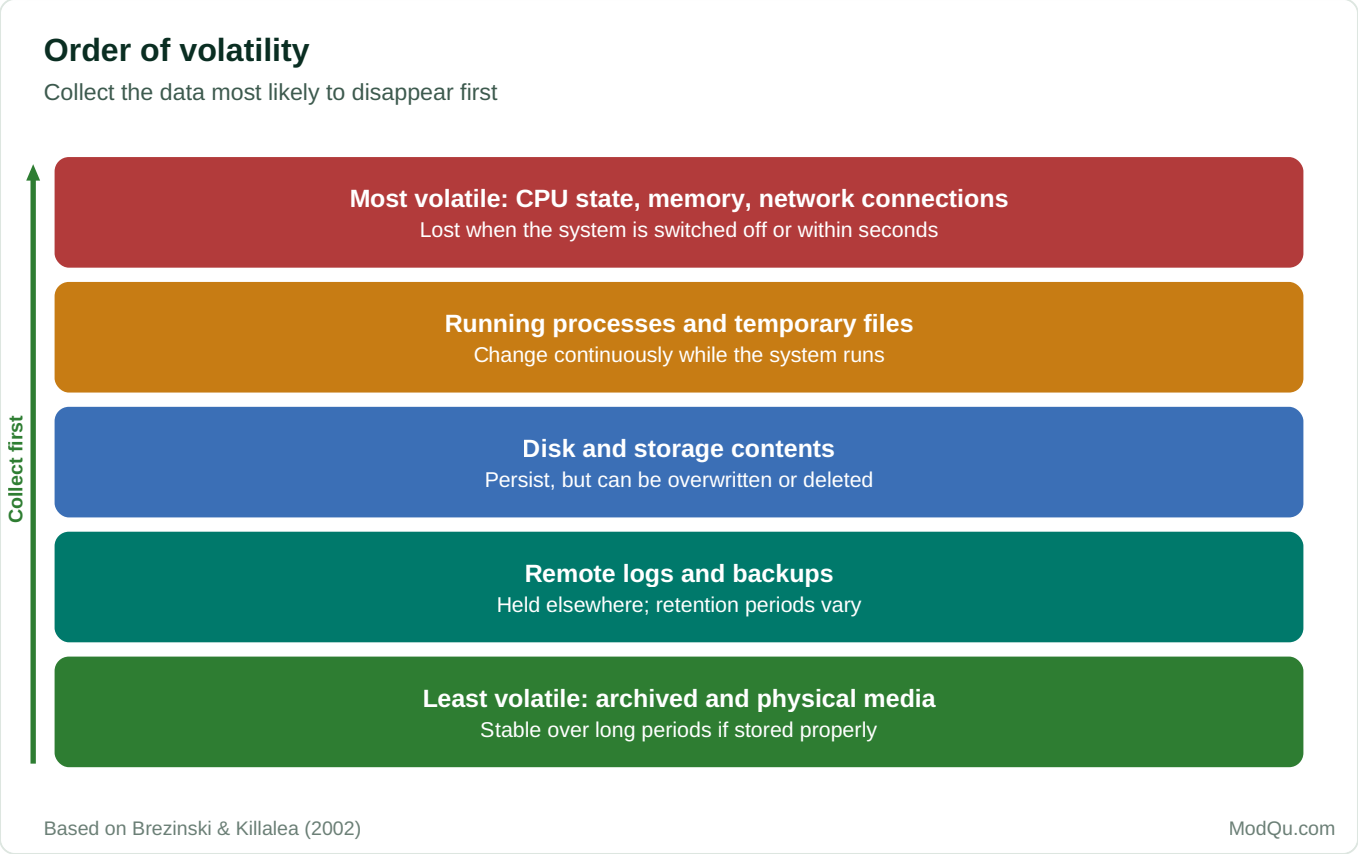


Figure 2. The order in which digital evidence should generally be collected. Capturing memory from a running system can preserve evidence, such as encryption keys and active connections, that would be lost if the system were simply switched off. Diagram by ModQu.

Acquisition

Acquisition creates a forensic copy of the data. For a hard drive, this is usually a bit-for-bit image of the whole device, including deleted and unallocated space, made through a write-blocker and verified by hash values. For phones, acquisition is more varied: depending on the device, its security and the tools available, investigators may obtain a full physical copy, a file system copy or only a logical extraction of accessible data. Memory acquisition captures the contents of a running system's memory, which can reveal running programs, network connections, encryption keys and malicious code that never touched the disk (Ligh et al., 2014). Cloud data are usually obtained from the service provider or through the user's account, which raises legal as well as technical questions.

Examination

Examination uses specialised tools to recover and present data: files, deleted material, emails, messages, internet history, location records, system logs and metadata. Knowledge of how file systems store and delete data is central to this stage; Carrier (2005) describes how deleted files can often be recovered and how file system records reveal when files were created, accessed and modified. The volume of data is often enormous, so examination involves filtering, searching and prioritising, guided by the investigation's questions.

Analysis

Analysis interprets the recovered data to answer those questions. It might reconstruct a timeline of a user's activity, establish who used a device at a particular time, trace how a file was transferred, or determine whether a document was altered. This is the stage at which the examiner's reasoning matters most. Data do not interpret themselves: a file in a user's folder may have been saved deliberately, downloaded automatically, placed there by malware or synchronised from another device. Good analysis considers alternative explanations and tests them against the evidence.

Reporting

The report explains what was examined, how, what was found and what it means, including limitations and the level of confidence in each conclusion. It should be written so that a non-specialist can understand it and another specialist can check it. Good reports distinguish clearly between what the data show directly, such as the fact that a file existed in a particular folder with particular timestamps, and the examiner's interpretation, such as the inference that a particular person created it. Where the interpretation depends on assumptions, such as the accuracy of a device's clock or the identity of the person using an account, those assumptions should be stated.

Challenges

Volume and variety

The amount of data in a typical case has grown enormously, while forensic resources have not kept pace. Quick and Choo (2014) reviewed the problem of increasing data volumes and the resulting backlogs in digital forensic laboratories. Garfinkel (2010) warned that the "golden age" of digital forensics, in which a small number of operating systems and file formats made examination relatively straightforward, was ending, as devices diversified, storage grew and encryption spread.

Encryption and security

Modern phones and computers encrypt data by default, and many messaging services use end-to-end encryption. Access may depend on obtaining passcodes, exploiting vulnerabilities or obtaining data from other sources such as backups or the other party's device. Each route raises technical and legal issues.

Cloud and jurisdiction

Data stored in the cloud may be held by a provider in another country, replicated across several jurisdictions and subject to different laws. Ruan et al. (2011) describe the distinctive challenges of cloud forensics, including the lack of physical access and dependence on the provider's cooperation. Legal mechanisms have developed in response: the United States Clarifying Lawful Overseas Use of Data Act (2018), known as the CLOUD Act, for example, clarifies when United States providers must disclose data held abroad and allows agreements with other countries for access to data.

Mobile devices

Phones are now the most important source of digital evidence in many investigations, and the most difficult. They hold messages, call records, photographs with location data, application data, health and movement records and links to cloud accounts. But they are designed to be secure. Data are encrypted, access depends on a passcode or biometric lock, and operating systems are updated frequently, so that a method that works on one version may fail on the next. Commercial extraction tools try to keep pace, but the level of access they achieve varies by device and version. Examiners must therefore record exactly how a phone was extracted and what kind of extraction was obtained, since this determines what data could have been recovered and what may be missing. Applications also store data in their own formats, which change with updates, and examiners must understand those formats to interpret what is recovered.

Anti-forensics

Some people take deliberate steps to defeat forensic examination. Methods include wiping tools that overwrite deleted data, encryption of individual files or whole devices, changing file dates to mislead timelines, using applications that delete messages automatically, and running software from removable media so that little trace is left on the computer. Such steps rarely leave no trace at all. The presence of wiping software, gaps in otherwise continuous logs, or timestamps that are inconsistent with each other can themselves be evidence, both of what happened and of an attempt to hide it. Examiners should report signs of anti-forensic activity carefully, since some of these tools also have legitimate uses, such as protecting privacy or securely disposing of old devices.

Tool reliability

Forensic examiners depend on software tools to extract and present data, and errors in those tools can produce misleading results. Horsman (2019) reviewed concerns about tool testing and reliability and called for more systematic validation. Standards for forensic laboratories, such as ISO/IEC 17025 and the code of practice issued by the Forensic Science Regulator in England and Wales, require methods to be validated before use (ISO, 2017; Forensic Science Regulator, 2023).

Cognitive bias

Digital forensics is vulnerable to the same biases as other forensic disciplines. Sunde and Dror (2019) describe how contextual information, expectations and the way evidence is presented can influence what examiners look for and how they interpret it. Because digital examinations involve many choices about what to search for and what to report, the risk that examiners will find what they expect is considerable. Measures such as recording the hypotheses being tested, seeking evidence for alternative explanations and peer review of findings help to reduce it.

The reliability of computer evidence

Courts often treat computer records as reliable unless there is evidence to the contrary. In England and Wales, there is a common law presumption that mechanical instruments, including computers, were working properly at the material time. The Post Office Horizon scandal, in which hundreds of sub-postmasters were prosecuted on the basis of shortfalls shown by an accounting system that was later found to contain bugs, errors and defects, has led to strong criticism of this presumption. In *Bates v Post Office Ltd (No 6: Horizon Issues)* (2019), the High Court found that the system had not been remotely robust and that its defects could cause apparent shortfalls in branch accounts. Mason and Seng (2021) review the law on electronic evidence and the problems that arise when the reliability of computer systems is assumed rather than established.

The lesson for investigators is that digital records are evidence produced by systems that can fail. Their reliability should be tested, especially when they are the main or only evidence against someone.

Law and privacy

Digital devices hold vast amounts of personal information, which makes searching them highly intrusive. Courts have recognised this. In *Riley v. California* (2014), the United States Supreme Court held that police generally need a warrant to search the digital contents of a phone seized during an arrest, noting that phones contain the "privacies of life". In *R v Fearon* (2014), the Supreme Court of Canada allowed searches of a phone incident to arrest only under strict conditions, including that the search be tailored to its purpose and carefully recorded.

In corporate investigations, access to employees' devices and accounts is governed by employment contracts, policies and data protection law. Investigators should limit searches to what is relevant and proportionate, document the legal basis, and protect the data they obtain.

A short example

The following hypothetical case illustrates the process. A company suspects that an employee copied confidential designs before leaving for a competitor. Its investigator identifies the employee's laptop, email account and cloud storage as relevant. The laptop is collected, photographed and imaged through a write-blocker, and the hash values of the original and the image are recorded and match. The company's cloud provider is asked to preserve the account.

Examination of the image shows that a USB storage device was connected two days before the resignation and that the design folder was accessed shortly afterwards. File system records show that several files were opened in that period. Analysis considers alternative explanations: the employee had legitimate reasons to work on the designs, and opening a file does not prove copying. However, system logs show that the files were copied to the USB device, and the cloud storage records show that the same files were uploaded to a personal account the next evening. The report sets out these findings, explains what each record shows and what it does not, and notes that the contents of the USB device itself could not be examined because it was not recovered.

Conclusion

Digital forensics provides some of the most detailed evidence available to investigators, but that evidence is fragile, voluminous and dependent on the systems that produced it. Its reliability rests on sound principles: preserving original data, working on verified copies, documenting every step, using validated tools, considering alternative explanations and reporting limitations honestly. As devices, services and encryption continue to evolve, those principles remain the foundation for evidence that courts and decision-makers can trust.

References

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

Bates v Post Office Ltd (No 6: Horizon Issues) [2019] EWHC 3408 (QB).

Brezinski, D., & Killalea, T. (2002). *Guidelines for evidence collection and archiving* (RFC 3227). Internet Engineering Task Force. https://doi.org/10.17487/RFC3227

Carrier, B. (2005). *File system forensic analysis*. Addison-Wesley.

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

Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 1213 (2018).

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

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation, 7*(Suppl.), S64–S73. https://doi.org/10.1016/j.diin.2010.05.009

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

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).

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

Ligh, M. H., Case, A., Levy, J., & Walters, A. (2014). *The art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory*. Wiley.

Mason, S., & Seng, D. (Eds.). (2021). *Electronic evidence and electronic signatures* (5th ed.). University of London Press.

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

Palmer, G. (2001). *A road map for digital forensic research* (DFRWS Technical Report DTR-T001-01). Digital Forensic Research Workshop.

Pollitt, M. (2010). A history of digital forensics. In K.-P. Chow & S. Shenoi (Eds.), *Advances in digital forensics VI* (pp. 3–15). Springer. https://doi.org/10.1007/978-3-642-15506-2_1

Quick, D., & Choo, K.-K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation, 11*(4), 273–294. https://doi.org/10.1016/j.diin.2014.09.002

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence, 1*(3), 1–12.

Riley v. California, 573 U.S. 373 (2014).

Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011). Cloud forensics. In G. Peterson & S. Shenoi (Eds.), *Advances in digital forensics VII* (pp. 35–46). Springer. https://doi.org/10.1007/978-3-642-24212-0_3

R v Fearon, 2014 SCC 77, [2014] 3 S.C.R. 621.

Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. *Digital Investigation, 29*, 101–108. https://doi.org/10.1016/j.diin.2019.03.011