An Introduction to Digital Forensics

Michael Hegarty

Abstract: Computer forensics, also known as digital forensics, is the practice of extracting, preserving, and analysing digital evidence from electronic devices, such as computers, smartphones, and tablets, to support criminal investigations, legal disputes, and regulatory compliance. This field, initially spearheaded by law enforcement, has since expanded into the commercial sector, where it aids in cases like intellectual property theft, employment disputes, and fraud investigations.

The forensic process follows a structured approach, starting from readiness and evaluation, through data preservation, acquisition, analysis, and presentation of findings, and concluding with a review to improve future investigations. Despite its growing importance, computer forensics faces technical, legal, and administrative challenges. Adhering to principles such as those outlined in the ACPO guidelines ensures the reliability and admissibility of evidence in legal proceedings.

Keywords: Computer Forensics, Digital Evidence, Data Acquisition, Write Blockers, Guiding Principles

Introduction

Computer forensics, often referred to as digital forensics, involves the collection, preservation, analysis, and presentation of digital evidence in a legally admissible manner. It should be conducted by trained forensic examiners who extract valuable data such as search histories, emails, purchase records, and time logs from various devices, including computers, smartphones, tablets, and more. This evidence can be crucial in criminal investigations, civil disputes and employment disputes (Nelson et al., 2018).

Examiners analyse the recovered data and present it in a way that is accessible and understandable to legal professionals, investigators, and non-technical stakeholders, such as judges and juries, mediators, HR Professionals, CEO’s and others. The goal is to provide insights into digital activities relevant to the case, while ensuring the integrity and reliability of the evidence (Casey, 2011).

When and How is Computer Forensics Used?

Computer forensics can be applied across a wide range of scenarios, including criminal investigations, civil litigation, corporate disputes, and regulatory compliance. Law enforcement agencies are among the most prominent users, often relying on forensic techniques to solve crimes ranging from cyberattacks, fraud, and intellectual property theft to violent crimes such as murder and kidnapping (Solomon et al., 2011). Private sector companies also use computer forensics for internal investigations involving employee misconduct, data breaches, and disputes over intellectual property (Harries, 2015).

Computers and other digital devices are often considered crime scenes in cases of hacking, denial-of-service (DoS) attacks, and data theft. However, they also frequently hold evidence of crimes that occurred elsewhere, such as incriminating emails, internet histories, and digital documents relevant to crimes like fraud or drug trafficking (Bunting and Philip, 2012).

Computer forensic examinations can reveal more than just the content of files and emails. Examiners also focus on metadata, which provides details about a file's history—such as when it was created, last edited, accessed, printed, or copied. Additionally, system logs and application data (like browser histories) can provide a detailed record of user actions (Casey, 2011).

Uses of Computer Forensics in Commercial Settings

In the commercial world, businesses use computer forensics for a variety of cases, such as:

- Intellectual property theft: Detecting unauthorized access or theft of proprietary information.
- Employment disputes: Investigating allegations of misconduct or contract breaches.
- Invoice fraud: Uncovering fraud schemes facilitated by phishing or other malicious techniques.
- Forgeries: Verifying the authenticity of documents or communications.
- Inappropriate use of IT systems: Identifying employees engaging in unauthorized email or internet use.
- Regulatory compliance: Ensuring adherence to industry-specific regulations (Solomon et al., 2011).

Recommendations for Effective Digital Forensics

For forensic evidence to be admissible in court, it must adhere to strict standards of integrity and reliability. The evidence must be untampered, accurately preserved, and presented in a way that is transparent and impartial (Nelson et al., 2018). The ACPO (Association of Chief Police Officers) Good Practice Guide for Digital Evidence provides a widely respected framework for handling digital evidence. Although originally designed for UK law enforcement, the core principles are globally relevant and applicable to both law enforcement and commercial forensics (ACPO, 2012).

Here are the four main principles from the ACPO guide:

1. Do not alter data: No actions should change data on a computer or storage media that may later be relied on in court.
2. Competence in handling: If original data must be accessed, only qualified personnel should do so, and they must explain their actions and any consequences.
3. Audit trails: A full record of all processes applied to the evidence should be maintained so that an independent third party could replicate the results.
4. Responsibility: The lead investigator is responsible for ensuring that all applicable laws and guidelines are followed (ACPO, 2012).

Live Acquisition: Handling Powered-On Systems

In certain situations, forensic examiners must conduct a live acquisition—retrieving data from a device while it is still powered on. This is necessary when shutting down a system could result in the loss of valuable evidence (such as data stored in volatile memory) or cause operational disruptions. Although live acquisition violates the ACPO guideline of avoiding data changes, it is permissible if the examiner **carefully documents their actions and explains their necessity** (Casey, 2011).

Stages of a Computer Forensics Examination

A typical digital forensic examination follows key stages:

Readiness: Ensuring that forensic tools and personnel are prepared. This includes proper training, equipment testing, and maintaining awareness of legal and technical challenges (Harries, 2015).

Evaluation: Clarifying the scope of the investigation and conducting risk assessments, such as evaluating potential threats, conflicts of interest, or health and safety concerns (Nelson et al., 2018).

Preservation**:** in computer forensics is crucial for ensuring the **integrity** of digital evidence. This involves securing the data in its original state to prevent any alteration or contamination during the forensic process. A key tool used during this stage is a **write blocker**, which allows forensic examiners to access and copy data from a storage device without making any changes to the original data. Write blockers act as a safeguard by blocking any signals from the examiner's system that could alter the contents of the storage media, ensuring that no new data is written to the device. This is essential for maintaining the evidential integrity required for legal admissibility, as even the slightest modification could invalidate the evidence in court (Nelson et al., 2018).

By using write blockers, examiners can create an exact forensic image of the device, preserving the original evidence while working with a copy for analysis. *This step is a foundational principle in forensic investigations*, ensuring that the evidence remains unaltered and that a clear audit trail is maintained throughout the process (Casey, 2011).

Acquisition: The forensic collection of evidence, often through creating a forensic image (duplicate), (a bit-by-bit copy) of the data, which is then used for analysis. Proper documentation and **chain-of-custody** procedures are crucial to preserve the integrity of the evidence (Bunting and Philip, 2012).

Analysis: Examining the acquired data to uncover relevant information. Depending on the case, this could involve reconstructing file histories, recovering deleted data, or identifying network activity. The analysis must be thorough, unbiased, and capable of withstanding scrutiny (Solomon et al., 2011).

Presentation: Summarizing findings in a clear, structured report. This stage often involves translating technical information into non-technical terms for legal professionals, clients, or courts (Harries, 2015).

Review: After the investigation, examiners should conduct a review of the process to identify areas for improvement. This helps ensure that future investigations are more efficient and effective (Nelson et al., 2018).

Challenges Faced by Computer Forensic Examiners

Computer forensic investigators face a variety of technical, legal, and administrative challenges:

Technical Issues:

Encryption: Encrypted files or systems can be difficult or impossible to access without the correct key or password.

Increasing storage capacity: Modern devices store vast amounts of data, requiring more powerful tools and systems for analysis.

Emerging technologies: The rapid evolution of hardware, software, and operating systems requires constant learning and adaptation.

Anti-forensics: Criminals may employ techniques to obscure or destroy evidence, such as encryption, data wiping, or metadata manipulation (Casey, 2011).

Legal Issues:

Jurisdictional complexities: Data stored on cloud servers in other countries may be subject to different legal frameworks, complicating evidence collection (Bunting and Philip, 2012).

Trojan defence: A common defence strategy is to claim that malicious activity on a computer was carried out by malware, not the user (Nelson et al., 2018).

Administrative Issues:

Lack of universal standards: There is no universally accepted set of guidelines governing computer forensics, leading to variability in practices across different jurisdictions and industries.

Qualification of practitioners: In some regions, there are no formal certification requirements for computer forensic examiners, which can lead to inconsistent quality in investigations (Solomon et al., 2011).

Conclusion

Computer forensics plays a critical role in modern investigations, providing the ability to uncover, preserve, and present digital evidence in a legally sound manner. From law enforcement to corporate disputes, the field continues to evolve alongside technological advancements, and forensic examiners must stay informed about emerging challenges and tools to maintain the integrity of their investigations.

References

ACPO (2012) Good Practice Guide for Digital Evidence. 5th ed. London: Association of Chief Police Officers.

Bunting, S. and Philip, W. (2012) The Official EnCase Certified Examiner Study Guide. Indianapolis: Wiley.

Casey, E. (2011) Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Amsterdam: Elsevier.

Harries, S. (2015) Computer Forensics: Investigating Network Intrusions and Cyber Crime. London: Course Technology.

Nelson, B., Phillips, A. and Steuart, C. (2018) Guide to Computer Forensics and Investigations. 6th ed. Boston: Cengage Learning.

Solomon, M.G., Barrett, D. and Broom, N. (2011) Computer Forensics JumpStart. 2nd ed. San Francisco: Wiley.