AG Publishing House

Investigative Frontiers Integration of Science Transforming Criminal Investigation

Year: 2026

The Digital Crime Scene: Principles, Methods, and Challenges in Digital Forensics

Mr. Mohammad Asif[1]

[1]*Assistant Professor Department of Forensic Science Mangalayatan University, Jabalpur, Madhya Pradesh*

Abstract

Digital forensics has emerged as a vital field used to investigate crimes involving computers, mobile devices, networks, cloud platforms, and other digital technologies. The concept of the digital crime scene and the scientific principles, standardized methodologies, and technologies that are the foundation of contemporary digital forensic investigations are explored in this review. It covers the basics of digital forensics, the nature of digital evidence, the chain of custody, forensic soundness and the internationally agreed guidelines for the handling of evidence. The review also provides a description of the digital forensic investigation process, the various sources of digital evidence in the investigation as well as the commonly used digital forensic tools for evidence collection and analysis. Finally, it covers challenges of the modern era, such as encryption, cloud computing, Internet of Things (IoT) devices, anti-forensic methods and legal issues, and explores the potential influence of artificial intelligence and automation on improving forensic investigations. The review highlights the importance of standardisation, reliability and advancement of forensic procedures for the effective investigation of cybercrimes and judicial decision making.

Keywords; Digital forensics; Digital crime scene; Digital evidence; Chain of custody; Cybercrime investigation.

[1] ISBN No. - 978-93-7640-081-2

1 Introduction

The rapid evolution of information and communication technologies has changed the nature of crime, resulting in offences that are committed, facilitated and even concealed via digital devices and networked environments. Thus, the notion of a digital crime scene has arisen as a supplement to the traditional crime scene. Traditional crime scene type evidence consists of physical evidence gathered and analyzed in a typical crime scene, like fingerprints, blood samples, weapons, or trace evidence. Digital crime scenes, on the other hand, consist of electronic devices and digital environments (such as computers, smartphones, cloud systems, servers, storage devices, and communication systems) that can hold valuable digital evidence like files, emails, browsing histories, system logs, metadata, and deleted information. Digital evidence is extremely volatile, can be remotely altered or destroyed, and must be identified, preserved, acquired and analyzed in a manner that ensures its integrity and authenticity.[2]

Digital forensics is a specialized area of forensic science that uses scientifically accepted methods to discover, secure, recover, examine, analyze, and present E-School information in an investigation and for legal purposes. The main goal is to retrieve and analyze digital evidence: information that is of probative value and is stored or communicated digitally that can help reconstruct events or establish relationships between individuals, devices, and crime. The scientific underpinning of digital forensic investigation is rooted in sound computer science principles and is legally defensible by ensuring that evidence is collected and analyzed in a forensically sound and legally defensible way.[3]

The use of digital forensics tools in investigations of ransomware, identity theft, financial fraud, cyber espionage, data breaches, child exploitation, and cyberterrorism is all but essential in today's cyber world. It is not limited to criminal investigations, but can also help law enforcement with evidence collection, aid corporate organisations in the investigation of insider threats, intellectual property theft and policy violations and give expert evidence during civil or criminal litigation. A digital evidence's ability to recover, preserve and interpret digital evidence is vital

[2] G. K. Ayswariya and A. Rajan, “A Comparative Study on the Difference Between Conventional Crime and Cyber Crime,” Int. J. Pure Appl. Math., vol. 119, no. 17, pp. 1451–1464, 2018.

[3] L. Klas, N. Fock, and R. Forchheimer, “The invisible evidence: Digital forensics as key to solving crimes in the digital age,” Forensic Sci. Int. J., vol. 362, 2024, doi: https://doi.org/10.1016/j.forsciint.2024.112133.

to the goals of justice and to the security of organizations and the credibility of judicial proceedings as digital technologies penetrate every facet of society.[4]

2 Principles and Foundations of Digital Forensics

The science of digital forensics is based on scientific, technical, and legal principles which ensure the collection, analysis, and presentation of digital evidence in a reliable and acceptable way in judicial proceedings. Digital information can be corrupted or altered accidentally, or manipulated on purpose, and can also be lost forever if it is not handled properly, unlike traditional evidence. Forensic investigators are thus required to operate within a structured process that involves preserving the integrity of electronic evidence in a way that allows for detailed and transparent documentation of the investigation, as well as its reproducibility and accountability. These principles build the trustworthiness of the evidence found in a digital investigation and provide investigators with the tools needed to accurately reconstruct digital events, while at the same time satisfying legal and ethical obligations.[5]

A. Fundamental Principles of Digital Forensics

The basic goal of digital forensics is to be able to identify, preserve, acquire, examine, analyze and report digital evidence without altering its integrity. Investigations must be carried out with validated forensic tools and scientifically accepted investigative methodologies that will reduce changes in the original data. Each step taken in the handling of the evidence should be recorded in such a fashion that it could be duplicated by an independent expert and the results checked. It is important to keep an objective, accurate, and transparent approach to the investigation as this is crucial in order to ensure that the forensic conclusions are reliable and accepted in court.[6]

B. Characteristics of Digital Evidence

Digital evidence has a number of special qualities that make it evidential. Integrity means that evidence is complete and that it has not been changed since it was collected until it is presented in court, typically achieved by using cryptographic hash values. Authenticity is a confirmation that the evidence is genuine, and not fabricated or manipulated. Evidence must be gathered

[4] I. Abeysekera, "Open source tools: an evaluation for digital forensic investigations," Front. Res. Metrics andAnalytics, pp. 1–8, 2026, doi: 10.3389/frma.2026.1790333.

[5] S. Patel and R. Singh, "Digital Forensics: Fundamentals and Awareness to Society Against Cybercrime Shubham," J. Adv. Robot., vol. 9, no. 2, pp. 37–41, 2022, doi: 10.37591/JoARB.

[6] P. Reedy, "Interpol review of digital evidence 2016 - 2019," Forensic Sci. Int. Synerg., vol. 2, pp. 489–520, 2020, doi: 10.1016/j.fsisyn.2020.01.015.

through legal means and meet the rules of evidence before it can be admissible in judicial proceedings. Repeatability is the capacity to obtain the same result when another qualified examiner reviews the evidence, method, and validated forensic tools to corroborate the investigation's findings for greater credibility and scientific validity.[7]

C. Chain of Custody

The chain of custody is the documentation that chronicles the possession, handling, transfer, storage and examination of digital evidence throughout its life cycle. It is a record of who gathered the evidence, when and where it was gathered, how the evidence was gathered, and every subsequent movement of the evidence to authorized persons. An unbroken chain of custody shows that the evidence was properly preserved and not altered, which can limit the possibility of evidence being challenged for authenticity at trial.

D. Forensic Soundness and Evidence Preservation

Forensic Soundness means the use of techniques that ensure that the original state of the digital evidence is maintained and does not become contaminated or modified in any way. Investigators usually make bit-by-bit copies of the media instead of examining the original media themselves and then checking the copies against the original with cryptographic hash algorithms like MD5 or SHA-256. Appropriate preservation methods such as write blocking, secure storage, controlled access and extensive documentation help to guarantee evidence integrity and enable the digital artifacts to be preserved for future forensic analysis and legal review.[8]

E. Internationally Accepted Forensic Guidelines

Digital forensic investigations follow internationally adopted best practices that uphold consistency, reliability and legal defensibility. There are a number of organizations that have issued guidelines widely used by the community for evidence acquisition, preservation, documentation, forensic validation and reporting, including the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), the Association of Chief Police Officers (ACPO), and the Scientific Working Group on Digital Evidence (SWGDE). These frameworks vary in breadth but all share a common focus to ensure

---

[7] M. Voronin, "Characteristics of Electronic (Digital) Evidence Assessment," Actual Probl. Russ. Law, vol. 16, pp. 118–128, Sep. 2021, doi: 10.17803/1994-1471.2021.129.8.118-128.

[8] M. Matijević Gostojić and Ž. Vuković, "A knowledge-based system for supporting the soundness of digital forensic investigations," Forensic Sci. Int. Digit. Investig., vol. 46, p. 301601, 2023, doi: https://doi.org/10.1016/j.fsidi.2023.301601.

evidence integrity, the use of validated forensic procedures, the documentation of all investigative steps, and scientifically sound and legally admissible digital evidence.[9]

3 Digital Forensic Investigation Process and Methods

The digital forensic investigation is a systematic and scientifically validated process in order to ensure that digital evidence is collected, analyzed and presented without compromising the integrity of the digital evidence. Digital forensic examinations differ from traditional investigations in that they have to deal with the volatility of electronic information, and information that can be changed, overwritten, or deleted in seconds. So, investigators adopt standard approach(s) to ensure evidence authenticity and reconstruct digital events accurately. There are several forensic frameworks proposed by various organizations like National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Digital Forensics Research Workshop (DFRWS), but they are similar in sequential steps to ensure consistency, repeatability and admissibility in court of law.[10]

A. Standard Investigation Lifecycle

Digital forensic investigation lifecycle usually involves six stages: Identification, Preservation, Acquisition, Examination, Analysis, and Reporting. The investigation starts with identifying the possible sources of digital evidence, and subsequently preserving digital evidence to avoid alteration or loss. Forensic copies of evidence are then obtained, analyzed using validated forensic tools, and compared to establish facts relevant to the case, and reported in an extensive and thorough document appropriate for a court of law. This systematic procedure gives science to it and increases the reliability of investigative results.

B. Identification of Digital Evidence

In the identification stage, a potential source of relevant digital evidence is located and identified. They can be desktop computers, laptops, portable storage devices, cloud storage, network logs and logs, surveillance systems, email, and social media accounts. Investigators determine what

[9] R. Montasari, "Review and Assessment of the Existing Digital Forensic Investigation Process Models," Int. J. Comput. Appl., vol. 147, no. 7, pp. 1–9, 2016.

[10] S. Sangwan and N. Chaudhary, "Digital Forensics Process and Current Trends," 2026, pp. 311–335. doi: 10.1007/978-981-95-2196-8_21.

each device or source of information may hold and what it may mean, and preserve the digital crime scene to ensure that it cannot be altered or accessed by others.[11]

C. Preservation and Acquisition

The purpose of evidence preservation is to preserve digital evidence in its original condition during the investigation. Investigators isolate devices from external networks, employ write-blocking hardware when accessing storage media, and calculate cryptographic hash values to verify data integrity. The acquisition is the process of generating a bit-by-bit forensic image of the original storage media, as opposed to directly analyzing the original storage media. Acquisition can be live (volatile information like RAM and active network connections are collected from a running system) or static (dead; data are collected after a device has been powered down, reducing the chance of modifying stored information).[12]

D. Examination and Analysis

In the examination, investigators locate, retrieve, and analyze pertinent digital artifacts through the use of specialized tools and software. Analysis is the process of reading, understanding and reconstructing what people have done in relation to the artifacts, creating time lines, recovering deleted files, correlating findings from various artifacts, determining what order the events in the investigation took place. This step converts raw digital information into useful forensic information that helps to draw investigative conclusions.[13]

E. Documentation and Reporting

All stages of the investigation process are documented thoroughly, to ensure transparency and repeatability. Investigators document evidence collection procedures, forensic tools involved, hash values, examination processes, evidence analysis and the chain of custody. The final forensic report should be clear, objective, and legally sound, allowing the investigators and court

---

[11] J. B. Vala and V. M. Vekariya, "The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection," Int. J. Life Sci. Biotechnol. Pharma Res., vol. 13, no. 6, pp. 413–420, 2024, doi: 10.69605/ijlbpr_13.6.2024.80.

[12] M. AlKhanafseh and O. Surakhi, "Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography," Electronics, vol. 13, no. 3729, pp. 1–24, 2024, doi: https://doi.org/10.3390/electronics13183729.

[13] A. Selim and İ. Ali, "The Role of Digital Forensic Analysis in Modern Investigations," J. Emerg. Comput. Technol., vol. 4, pp. 1–5, 2024, doi: 10.57020/ject.1445625.

to assess the reliability of the evidence, while the methodology and observations and interpretations and conclusions are presented.

4 Digital Evidence Sources and Forensic Tools

Identification of relevant digital evidence is fundamental to the effective use of a digital forensic investigation, as is the use of appropriate forensic tools for acquisition and analysis of digital evidence. Digital technologies are so widespread that evidence is no longer just in the personal computer but also through mobile technologies, cloud services, network infrastructures, and online communication platforms. These evidence sources are varied, and specialized forensic software is needed to extract, recover and analyze digital artifacts without compromising evidence integrity. Therefore, choosing validated/confirmed and reliable forensic tools is crucial to generate accurate and defensible investigative results in a court of law.

A. Major Digital Evidence Sources

Digital evidence may be found on a wide variety of electronic devices and in digital environments. Computers are still a main source and have operating system logs, documents, application files, browsing history, and user activity records. Smartphones have useful information like call logs, text messages, application data, photos, GPS locations and internet usage history. Many times, deleted or archived files exist on storage media such as solid state drives, hard disk drives, USB drives, and memory cards and relate to an investigation. Network infrastructures generate logs, packet captures, firewall records, and traffic metadata that assist in reconstructing cyber incidents. Cloud platforms are used to store emails, documents, backups and virtual machine data while social media platforms are increasingly used to store communications, multimedia data, user interactions, relationships, timelines and even evidence of criminal intent.[14]

B. Categories of Forensic Tools

Digital forensic tools can be classified into different groups based on the investigative functions they serve. Acquisition tools produce forensic images of the storage media but do not damage the original evidence. Examination and analysis tools will recover deleted files, analyze file systems, interpret operating system artifacts and reconstruct user activities. Memory Forensic Tools analyze running processes, malware, encryption keys and network connections in volatile memory. Network forensic tools are used to monitor and analyze network traffic to detect and

[14] K. Chauhan, "Digital Evidence and Emerging Technologies," Indian J. Law, vol. 4, no. 2, pp. 17–22, 2026, doi: https://doi.org/10.36676/ijl.v4.i2.188.

study cyberattacks and unauthorized communications. These ancillary categories provide investigators ways to view digital evidence in a variety of ways throughout the forensic process.[15]

C. Examples of Widely Used Forensic Tools

There are various commercial and open source tools used for digital forensics investigations. Autopsy is an open source disk analysis, file recovery, keyword searching, and timeline construction software. Forensic Toolkit (FTK) offers comprehensive capabilities for evidence acquisition, indexing, email analysis and password recovery. EnCase Forensic is widely utilized for forensic imaging, file system analysis and evidence management by law enforcement organizations. Volatility focuses on memory forensics and performs various analysis on RAM images to find evidence of malware and volatile data. Wireshark is a network protocol analyzer that can capture and analyze packets in a network to detect suspicious communications and recreate network events.[16]

D. Importance of Tool Validation and Reliability

Aside from the expertise of the investigators, the credibility of digital forensic evidence is also reliant upon the reliability of the tools used in the investigation. Tool validation facilitates software to operate reliably in terms of the software function being performed to the required accuracy and producing repeatable results without unintentional changes to evidence. Institutions like the National Institute of Standards and Technology (NIST) highlight the importance of assessing and verifying the forensic tools to be used in an investigation prior to that. Use of validated software, documentation and corroboration of findings with multiple techniques increase the scientific reliability of digital evidence, its repeatability and admissibility in court.[17]

---

[15] P. S. Vinayagam, "Digital Forensic Tools For Cybercrime Investigation: A Comparative Analysis," Int. J. Appl. Inf. Syst., vol. 12, pp. 25–31, May 2025, doi: 10.5120/ijais2025452018.

[16] P. S. Vinayagam, "Digital Forensic Tools for Cybercrime Investigation: A Comparative Analysis," Int. J. Appl. Inf. Syst., vol. 12, no. 47, pp. 25–31, 2025.

[17] I. Ismail and K. A. Z. Ariffin, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance," PLoS One, vol. 20, no. 9, pp. 1–26, 2025, doi: https://doi.org/10.1371/ journal.pone.0331683.

E. Challenges and Emerging Trends in Digital Forensics

The pace of technological evolution and the sophistication of cybercrime continually evolve and transform digital forensics. New technical and legal challenges are present in modern investigations with a multitude of digital environments, encrypted communications, cloud infrastructures, and interconnected devices. Therefore, investigators have to keep evolving forensic methods and tools to meet the challenges while preserving the integrity, reliability and admissibility of digital evidence. At the same time, emerging technologies are providing innovative approaches to improve the efficiency and accuracy of forensic investigations.[18]

F. Challenges in Digital Forensics

The challenge is that encryption and password protection are ubiquitous, and that can limit investigators' access to important evidence that's stored on computers, smartphones, and in the cloud. Another major concern is the amount of digital evidence produced by the modern devices; this needs huge storage space, much computation, and time to analyse the digital evidence. The growing use of cloud computing and Internet of Things (IoT) devices further complicates investigations as evidence is spread out over various locations, jurisdictions, and service providers. Anti-forensic techniques such as data wiping, secure deletion, encryption, steganography, log tampering and tampering with timestamps are also employed specifically to conceal or destroy evidence, which will also need to be addressed by investigators. Additionally, privacy and legal concerns such as data protection laws, international investigations, lawful access to digital information and conflicting jurisdictions create challenges in forensic investigations.[19]

G. Emerging Trends in Digital Forensics

The advent of new Artificial Intelligence (AI) and machine learning technologies and the automation of digital forensic processes are changing digital forensic investigations, with faster evidence classification, anomaly detection, identification of malware, timeline reconstruction and automated report generation. AI tools for forensic investigation streamline data analysis by processing massive amounts of information quickly and accurately, while minimizing manual work. Future research is expected to include work on explainable AI systems for forensic

---

[18] A. Hamed, "Digital Forensic: Techniques, Challenges, and Future Direction," Int. J. Res. Appl. Sci. Eng. Technol., vol. 13, pp. 5869–5873, May 2025, doi: 10.22214/ijraset.2025.71562.

[19] F. Casino et al., "Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews," IEEE Access, vol. 10, p. 1, Jan. 2022, doi: 10.1109/ACCESS.2022.3154059.

investigation, standardisation of forensic methods in cloud and IoT environments, privacy preserving investigation techniques, and internationally harmonised law to enable the complexity of digital forensic investigations.[20]

5 Conclusion

The use of digital technology in everyday life has made digital forensics an essential element in the investigation process for today's investigators. The identification, preservation, examination, and interpretation of digital evidence are crucial to the reconstruction of incidents and to judicial decision-making, as cybercrime continues to grow. This review emphasized the fundamental principles of digital forensic investigations such as evidence integrity, evidence forensic soundness, chain of custody and internationally accepted best practices. It also provided a general overview of the typical investigation process, the various sources of digital evidence, and common tools used in the forensics industry to aid in the acquisition and analysis of digital evidence. In addition, the review covered new trends and concerns with encryption, cloud computing, IoT networks, anti-forensics, and legal issues. Advancements in emerging technologies, like artificial intelligence and automation, will be expected to enhance the efficiency of investigations and analytical capacity. Ongoing research, the use of standardized approaches, validation of tools, and international collaboration will be crucial to the success of digital forensic investigations in the future, ensuring their scientific soundness, legal defensibility, and effectiveness against emerging threats.

6 Reference

[1] G. K. Ayswariya and A. Rajan, “A Comparative Study on the Difference Between Conventional Crime and Cyber Crime,” Int. J. Pure Appl. Math., vol. 119, no. 17, pp. 1451–1464, 2018.

[2] L. Klas, N. Fock, and R. Forchheimer, “The invisible evidence: Digital forensics as key to solving crimes in the digital age,” Forensic Sci. Int. J., vol. 362, 2024, doi: https://doi.org/10.1016/j.forsciint.2024.112133.

[3] Abeysekera, “Open source tools: an evaluation for digital forensic investigations,” Front. Res. Metrics andAnalytics, pp. 1–8, 2026, doi: 10.3389/frma.2026.1790333.

[20] P. Narasimhan and N. Kala, “Emerging Trends in Digital Forensics: Investigating Cybercrime,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 11, no. 1, pp. 3645–3652, 2025, doi: https://doi.org/10.32628/CSEIT251451.

[4] S. Patel and R. Singh, “Digital Forensics: Fundamentals and Awareness to Society Against Cybercrime Shubham,” J. Adv. Robot., vol. 9, no. 2, pp. 37–41, 2022, doi: 10.37591/JoARB.

[5] P. Reedy, “Interpol review of digital evidence 2016 - 2019,” Forensic Sci. Int. Synerg., vol. 2, pp. 489–520, 2020, doi: 10.1016/j.fsisyn.2020.01.015.

[6] M. Voronin, “Characteristics of Electronic (Digital) Evidence Assessment,” Actual Probl. Russ. Law, vol. 16, pp. 118–128, Sep. 2021, doi: 10.17803/1994-1471.2021.129.8.118-128.

[7] M. Matijević Gostojić and Ž. Vuković, “A knowledge-based system for supporting the soundness of digital forensic investigations,” Forensic Sci. Int. Digit. Investig., vol. 46, p. 301601, 2023, doi: https://doi.org/10.1016/j.fsidi.2023.301601.

[8] R. Montasari, “Review and Assessment of the Existing Digital Forensic Investigation Process Models,” Int. J. Comput. Appl., vol. 147, no. 7, pp. 1–9, 2016.

[9] S. Sangwan and N. Chaudhary, “Digital Forensics Process and Current Trends,” 2026, pp. 311–335. doi: 10.1007/978-981-95-2196-8_21.

[10] B. Vala and V. M. Vekariya, “The Role and Importance of Digital Forensics and Digital Evidence in Cyber Crime Detection,” Int. J. Life Sci. Biotechnol. Pharma Res., vol. 13, no. 6, pp. 413–420, 2024, doi: 10.69605/ijlbpr_13.6.2024.80.

[11] M. AlKhanafseh and O. Surakhi, “Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography,” Electronics, vol. 13, no. 3729, pp. 1–24, 2024, doi: https://doi.org/10.3390/electronics13183729.

[12] Selim and İ. Ali, “The Role of Digital Forensic Analysis in Modern Investigations,” J. Emerg. Comput. Technol., vol. 4, pp. 1–5, 2024, doi: 10.57020/ject.1445625.

[13] Chauhan, “Digital Evidence and Emerging Technologies,” Indian J. Law, vol. 4, no. 2, pp. 17–22, 2026, doi: https://doi.org/10.36676/ijl.v4.i2.188.

[14] P. S. Vinayagam, “Digital Forensic Tools For Cybercrime Investigation: A Comparative Analysis,” Int. J. Appl. Inf. Syst., vol. 12, pp. 25–31, May 2025, doi: 10.5120/ijais2025452018.

[15] P. S. Vinayagam, “Digital Forensic Tools for Cybercrime Investigation: A Comparative Analysis,” Int. J. Appl. Inf. Syst., vol. 12, no. 47, pp. 25–31, 2025.

[16] Ismail and K. A. Z. Ariffin, “The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance,” PLoS One, vol. 20, no. 9, pp. 1–26, 2025, doi: https://doi.org/10.1371/ journal.pone.0331683.

[17] Hamed, “Digital Forensic: Techniques, Challenges, and Future Direction,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 13, pp. 5869–5873, May 2025, doi: 10.22214/ijraset.2025.71562.

[18] Casino et al., “Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews,” IEEE Access, vol. 10, p. 1, Jan. 2022, doi: 10.1109/ACCESS.2022.3154059.

[19] P. Narasimhan and N. Kala, “Emerging Trends in Digital Forensics: Investigating Cybercrime,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 11, no. 1, pp. 3645–3652, 2025, doi: https://doi.org/10.32628/CSEIT251451.