IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

Digital Forensics in Transition: Navigating Challenges, Legal Boundaries, and Emerging Trends

[1]Dasari Harsha Vardhan [2]Dasari Majun Kumar

[1]MSc. Digital Forensic and Cyber Investigation Graduate, Teesside University, Middlesbrough, England, United Kingdom,

[2]B. Tech Computer science, Lovely professional University, Jalandhar, Phagwara, Punjab, India

Abstract

Digital forensics forms a significant part of the overall forensic science and computer security profession, individually covering identification, acquisition, analysis, and digital device information examination. In the era dominated by technology, such cybercrimes as cyberfraud, identity thefts, and data breach have become predominantly technological in character as regards their occurrence and thus need high-technology forensic approaches. It is the history of forensic computer evolution on a yearly basis from its start as computer examination to where it is today with cloud computing, cell phones, and the Internet of Things. It describes the overall forensic process of identification, preservation, collection, analysis, and presentation before going into tools and techniques employed in investigations today. The article also covers some of the most significant challenges such as increased data volumes, encryption, jurisdiction, and criminal misuse of anti-forensic tools. Legal and ethical issues are covered, covering the significance of evidence handling and privacy legislation. Lastly, future direction of AI supported forensic examination, blockchain forensics, and digital forensic as a service are briefly covered. The study gives special significance to continuous innovation and adjustment in digital forensics towards countering developing threats and pursuing justice in the world where everything is becoming digitalized.

Keywords: *Digital Forensics Evolution, Digital Forensic Process, Challenges in Digital Forensics, Chain of Custody, Legal and Ethical Considerations, Applications of Digital Forensics, Future Trends in Digital Forensics*

1. Introduction

In today's hyperconnected environment wherein digital devices pervade every aspect of personal and commercial life, the rise of cybercrime is an unavoidable dilemma. Data breaches, identity theft, ransomware attacks, cyberstalking, and web fraud are no longer unusual events but rather common threats to individuals, businesses, and governments. As a result, digital forensics has emerged as the major region for identification, examination, and counteraction of these threats. It is the foundation of cybersecurity, criminal justice, corporate investigations, and intelligence operations. Digital forensics, also known as computer forensics, is the process of locating and analysing electronic evidence without damaging its integrity and ensuring its admissibility in court (Casey, 2011; Rogers, 2006).

Digital forensics is unique from the other traditional forensic sciences that work with physical evidence such as fingerprints or DNA in that it works on the information of digital evidence held in computers, cellular phones, servers, cloud storage, and other forms of digital media (Vacca, 2005).

The discipline needs technical skills, law expertise, and investigative skills to collect and handle digital evidence in a way that it remains unaffected. Digital forensics has become more relevant very quickly due to some distinct reasons. The financial transactions have been converted digitally, the use of smartphones has also become more common, and cloud computing has seen growth (Pollitt, 2001; Harrison, 2007).

Furthermore, the internet has facilitated the anonymity of criminal activities and identity. Digital forensics is, thus, a critical process to track activity, find suspects, and provide digital evidence which shall be used to support legal procedures or internal security processes. The practice is, however, criticized. The dynamic nature of technology requires forensic professionals to keep themselves informed about the most recent operating systems, file systems, encryption technology, and network protocols. Privacy, jurisdictional complexity, and the sheer volume of digital data hinder forensic analysis (McKemmish, 1999; Pollitt, 2001).

Besides, increased application of anti-forensic techniques methods aimed at deleting, concealing, or manipulating digital evidence presents another layer of challenge for investigators. This paper aims to present an overview of digital forensics by its evolution throughout history, core approaches, investigation tools, legislations, ethical issues, and future directions. Based on a practice and trend research, the research proves the evolving function of digital forensics in maintaining security, providing justice, and effectively responding to digital threats in the modern era (Casey, 2011; Harrison, 2007).

2.Digital Forensics Evolution

Digital forensics evolution is directly related to the very fast growth of computer technologies and the simultaneous development of cybercrime (Casey, 2011). Although the idea of criminal activity investigation has been around for centuries, digital forensics appeared with the development of computer systems in the second part of the 20th century (Rogers, 2006). Initially perceived as a specialized aspect of computer security, digital forensics has now become an integral component of modern-day law enforcement, corporate governance, and national security (Vacca, 2005).

2.1 Emergent Phases (1970s–1980s)

Digital forensics began informally in the 1970s when computers first came under attack and were being utilized as tools for crime (McKemmish, 1999). Computer crime was then commonly the unauthorized access to university or government mainframes. Police agencies, however, did not yet have tools and the experience to analyse digital evidence. Investigations were primitive and often ad hoc, with no standard procedure or training (Pollitt, 2001).

2.2 Expansion and Acceptance (1990s)

With the expansion of the use of the personal computer and the internet in the 1990s, cybercrime proliferated (Harrison, 2007). The decade saw the emergence of "computer forensics" as a recognized discipline. Police began to create dedicated cybercrime units, and groundbreaking forensic tools like Norton Disk Editor were repurposed for the extraction of evidence (Baggili and White, 2009). Crisis milestones during this decade included the establishment of the International Organization on Computer Evidence (IOCE) and the Scientific Working Group on Digital Evidence, which began producing standards and best practices (Smith and McKemmish, 2017).

2.3 Diversification and Professionalization (2000s)

In the early 2000s, the shift took place, as digital forensics became a professionalized discipline (Rogers, 2010). Cyberattacks became more sophisticated and multi-faceted, and new internet platforms such as cloud computing, social media, and smartphones both became sources of evidence and targets (Carrier, 2003). Specialized tools like EnCase and Forensic Toolkit (FTK) entered mainstream use, making it possible for investigators to examine massive amounts of data and recover hidden or deleted information (Casey, 2011). Universities began to offer degree courses in digital forensics, and certification bodies like the International Association of Computer Investigative Specialists (IACIS) gained significant importance (Vacca, 2014).

2.4 Modern Era and Future (2010s–Present)

Digital forensics has expanded to cover mobile phones, IoT networks, blockchain platforms, and artificial intelligence-based platforms in the last ten years (Harris, 2013). The complexity of digital environments has seen highly advanced forensic tools, automation, and cloud computing develop (Garfinkel, 2010). As cyber threats evolve, so does digital forensics adapt to deal with both traditional and emerging investigative environments (Taylor et al., 2015).

3.1 The Digital Forensic Process

Most of the forensic examinations follow a simple procedure that generally consists of six broad steps (Casey, 2011):

3.1.1 Identification

The first phase is the identification of potential digital evidence sources. They may be computers, cell phones, USB storage media, e-mail servers, cloud storage, or network traffic logs (Carrier, 2003). The analysts must sweep the scene or the digital environment to determine which systems or devices may potentially hold data of interest. Identification also includes discovery of the category of incident data breach, malware attack, insider attack, etc. that will determine the range and nature of investigation (Roges, 2010).

3.1.2 Preservation

Preservation is necessary to confirm the integrity of digital evidence. Prevention of tampering, inadvertent modification, or loss of the original information via the mechanism of securing it is achieved within this step (Vacca, 2014). Write-blocking in order not to overwrite and creating cryptographic hash values (such as MD5 or SHA-256) to verify data integrity are routine processes (Casey, 2011). Forensic images bit-for-bit duplicates of storage devices are typically created in this step to facilitate examination without altering the original evidence (Harris, 2013).

3.1.3 Collection

During the collection phase, information is obtained from sources which have been identified by forensically sound methods and procedures (Casey, 2011). The procedure must be legal in nature, i.e., chain of custody reporting or warrant requirements (Carrier, 2005). File systems, registry entries, emails, metadata, log files, and volatile data like dumps of RAM can be collected by the examiners. Time-sensitive information such as recent memory (RAM) or network usage must be saved at once since it's lost when the system is turned off (Pollitt, 2008).

3.1.4 Analysis

This process is all about searching through physical data that was collected to identify potential evidence. Erased files, concealed partitions, encrypted drives, suspicious programs, or communications logs are what investigators search for (Rogers, 2006). Huge datasets are winnowed down by filtering and indexing software into smaller portions. The goal is to discover physical evidence without missing anything relevant as evidence (Altheide & Carvey, 2011).

3.1.5 Analysis

Analysis is where the information gathered is interpreted to answer inquiry questions: Who did it? How was it done? What were used? When was the crime committed? Timeline reconstruction, file access analysis, keyword search, and correlation of dissimilar data sources are typically done at this phase (Casey, 2011). The ability of the investigator to place digital artifacts in context is extremely important in making the findings actionable and credible (Kent et al., 2006).

3.1.6 Presentation

Finally, examiners summarize their conclusions in a concise, rational, and acceptable report in a court of law (Carrier, 2005). The report must be intelligible to non-expert stakeholders such as lawyers, magistrates, or company directors. Graphical illustrations, for instance, charts, timelines, and diagrams, are commonly added

(Pollitt, 2008). Examiners may also be required to provide testimony in court, and professionalism and objectivity must be maintained at all costs (Altheide & Carvey, 2011).

3.2 Specialized Techniques

In addition to the process model, computer forensics is based on a set of specialized techniques (Casey, 2011; Rogers, 2006):

• **File Carving:** Recovering data from unallocated disk space based on known file signatures, even if there is no file system present (Garner et al., 2009).

• **Keyword Searching**: Finding predefined phrases, filenames, or patterns in datasets (Carrier, 2005).

• **Timeline Analysis:** The creation of activity timelines based on metadata, logs, or system timestamps (Kent et al., 2006).

• **Hash Analysis:** The file comparison against a known hash database with the aim of detecting copies or contraband material (Altheide & Carvey, 2011).

• **Memory Forensics:** The analysis of RAM with the aim to find volatile evidence in the form of encryption keys, open connections, or resident malware (Ligh et al., 2014).

• **Network Traffic Analysis:** Packet inspection for hunting malware traffic or data exfiltration (Bejtlich, 2005).

• **Steganalysis:** Detection of hidden message or information in other types of files, such as images or audio (Katzenbeisser & Petitcolas, 2000).

3.3 Relevance of Methodological Sophistication

There must be a process that is systematically followed through, ensuring not only admissibility in the court of law but also repeatability and transparency. Digital evidence can be excluded by courts when it is mishandled, documented, or changed in the wrong manner (Kenneally, 2011). Every process must be documented comprehensively with the appropriate rationale for the choice of tools, procedures followed, and investigative decisions (Pollitt, 2007).

4. Challenges in Digital Forensics

With growing complexity of the digital technology itself at record pace, so grow the issues and complexity of digital forensic analysis. While the core digital forensics methods are steady, the experts continue to develop to address newly arising technical, legal, and procedural issues. These issues not only hinder the gathering and analysis of digital evidence, but also threaten the integrity, admissibility, and efficacy of forensic evidence. The most critical problems that digital forensic professionals face in the present era are discussed below.

4.1 Increased Data Volume and Complexity

The greatest challenge of modern digital forensics is the amount of data generated and stored by organizations and individuals. Social networking sites, high storage warehouses, IoT devices, and cloud computing have compelled the investigators to look for a terabyte or even petabytes of data in the attempt to crack one investigation (Casey, 2011). The deluge of data squanders more time, computer cycles, and human labour to locate positive evidence. More egregious is exacerbated by the fragmentation of information. Virtual data is too commonly dissected into bits, encoded, duplicated, or transmitted to various devices and platforms. Examiners are too often compelled to comb through a great amount of incompatible file systems, operating systems, and proprietary application environments, rendering examination challenging and extending investigations (Rogers et al., 2006).

4.2 Encryption and Secure Communication Technologies

Encryption is inherent to data privacy and yet poses an enormous challenge for forensic examiners. Contemporary encryption algorithms, i.e., AES-256, are all but impenetrable without decryption keys. Offenders are increasingly adept at utilizing encrypted communication applications (i.e., Signal, Telegram,

WhatsApp) and encrypted devices to mask their activities (Farid & Yang, 2017). Investigators are both technically and legally barred from decrypting certain communications or files in most cases. Despite attempts by law enforcement agencies to use "backdoors" to access encryption information, the actions are controversial both from an ethical point of view and in a way that jeopardizes general cybersecurity (Kerr, 2017). Striking the balance between public safety needs and the privacy rights and data protection is a controversial outstanding research question among the digital forensics' fraternity.

4.3 Anti-Forensic Techniques

Anti-forensics involves methods expressly to exclude or mislead forensic examination. Wipe software, steganography, file hiding, system wipe software, and rootkits hiding malware from detection are some anti-forensic methods (Casey, 2011). Highly organized criminals like cybercrime groups and nation-states utilize highly developed anti-forensic methods to evade detection (Farid & Yang, 2017). Such techniques render evidence detection difficult, increase the chances of missing vital information, and impair the integrity of forensic reports. Forensic analysts must constantly review their skills and tools to work around such measures as anti-forensic methods continue to evolve.

4.6 Tool Limitations and Validation

Computer forensic software is helpful but not flawless. Some tools can deliver inconsistent results, be recalcitrant to new technologies, or be insufficiently validated (Garfinkel, 2010). The blind application of commercial tools, unfamiliar with their limitations, can cause erroneous conclusions or overlooked evidence. To be trustworthy, forensic software will need to be suitably tested and confirmed on comprehended data sets and circumstances (Carrier, 2005). Moreover, examiners must be properly trained in the capabilities and limitations of the tools being used. Lack of open standards and the dominance of proprietary systems are some of the factors contributing to the complexity of tool interoperability and results transparency (Rogers, 2013).

4.7 Chain of Custody and Evidence Integrity

It is important to maintain the chain of custody so that digital evidence is not deemed inadmissible in court (Casey, 2011). Every step of the process from handling, collection, and storage of evidence must be documented so that the evidence has not been tampered with or changed. If the chain of custody is not easily accounted for and validated, then the integrity of the investigation and legal process can come under scrutiny (Pollitt, 2007). In addition, improper handling, storage, or transfer of digital evidence can result in corruption or data loss. Organizations need to have strict procedures and training in place for keeping the evidence in a locked, forensically sound system (Garfinkel, 2010).

5. Legal and Ethical Issues in Digital Forensics

Legal and ethical guidelines are at the very centre of digital forensics practice. Technical knowledge is required for acquiring and analysing digital evidence, yet the investigators must be as cautious as possible to stay within the law and to act ethically. Legal and ethical errors result in evidentiary inadmissibility, case loss, reputations tarnished, or even legal action against investigators and the organizations that employ them (Casey, 2011).

5.1 Legal Regimes and Admissibility of Evidence

Computer forensic examinations are regulated by national and international data privacy, access, and criminal procedures laws (Rogers et al., 2006). Search and seizure of electronic evidence in most countries, including the United States of America, are controlled by constitutional provisions such as the Fourth Amendment, which requires law enforcement agencies to seek a warrant backed by probable cause (U.S. Constitution, 1791). Similarly, within the European Union, controls are stringent with the General Data Protection Regulation (GDPR) in collecting data, processing data, and transferring data, most particularly where this is in relation to sensitive or personal data (European Parliament, 2016). Digital evidence must be:

• **Collected lawfully:** Evidence that has been collected illegally can be irrelevant (Casey, 2011).

• **Authentic and trustworthy:** The officers must prove that the information is authentic and not altered (Rogers et al., 2006).

• **Pertinent:** The evidence must only be relevant to what is being investigated (European Parliament, 2016).

• **Properly kept:** The chain of custody documents must detail who handled the evidence and when (Casey, 2011).

Failure to comply with these regulations may cause evidence to be challenged and disqualified during court hearings (Rogers et al., 2006).

5.2 Chain of Custody and Documentation

It is an ethical and legal requirement that digital forensics use a secure and well-documented chain of custody. The evidence is required to be logged regarding all who are in contact with it, and the purpose and time and date access is obtained. Digital signatures, cryptographic hashes, and forensic logs are commonly used to prove data integrity from seizure to presentation in court (Casey, 2011).

Inadequate disclosure or documentation will challenge the credibility of the investigation. Courts will look to a break in the chain of custody as proof that the evidence possibly could have been contaminated or otherwise unreliable (Rogers et al., 2006).

5.3 Ethical Responsibilities of Forensic Professionals

Forensic professionals working in digital forensics require a stern code of ethics to provide impartiality, confidentiality, and professional integrity. Some of the most frequent ethical demands are:

• **Neutrality**: The expert ought to be neutral and present facts based on evidence and not assumptions or stakeholder influence (Pollitt, 2007).

• **Confidentiality:** The investigators must handle private or sensitive information and prevent it from unauthorized usage or disclosure (Casey, 2011).

• **Competence:** The experts ought not to take up work beyond their expertise and may need to familiarize themselves with new technology as well as legal requirements (Pollitt, 2007).

• **Transparency:** Outputs must be properly documented, and processes be reproducible and intelligible to courts and stakeholders (Rogers et al., 2006)

6. Applications of Digital Forensics

Forensic techniques in the digital field have become a necessary tool in most aspects of life, ranging from police work to corporate management. Technology having pervaded all walks of life nowadays, the need for digital forensic examination goes far beyond the usual cases of cybercrime. The multiple applications of digital forensics in other sectors are addressed in this chapter with its growing visibility in crime investigation, computer security, and support to corporate and governmental operations (Casey, 2011).

6.1 Criminal Law Enforcement and Investigations

Digital forensics is among the primary applications of digital forensics, in terms of law enforcement and criminal investigations. With crime increasingly involving the utilization of digital devices, investigators commonly obtain most significant evidence from computers, cellular telephones, hard drives, and the cloud (Rogers et al., 2006). Digital forensics significantly aids criminal investigation activities such as fraud, identity theft, drug trafficking, organized crime, and even homicide (Roges et al., 2006).

Principal spheres where digital forensic supports the police include:

• **Cybercrime:** It includes hacking, phishing, ransomware, data breach, and cyber espionage. Digital forensics helps investigators identify the paths taken by the offenders, identifying vulnerabilities, and assigning attacks to individuals or groups (Kent et al., 2006).

• **Child Abuse and Exploitation:** Forensics is involved in the discovery, recovery, and storage of evidence in favour of child exploitation content and abuse on the internet. File carving and keyword search are some of the methods that allow the investigator to find and retrieve erased or concealed files with illegal content (Casey, 2011).

• **Digital Forensic Data Recovery**: The police would normally employ digital forensics to restore erased data or damaged information from crashed or physically destroyed devices, usually presenting useful evidence which otherwise would be lost (Carrier, 2005).

6.2 Business and Corporate Investigations

Organizationally, digital forensics supports an examination of security violations within the organization, unethical acting employees, theft of intellectual property, and economic offenses. Organisations apply digital forensics to safeguard their data, stay compliant with legislated standards, and investigate occurrences that compromise confidential data (Rogers et al., 2006).

Applications of business investigation are:

• **Insider Threats:** Business applies digital forensics to detect and investigate cases where company assets were misused by employees or contractors, for example, intellectual property theft or unauthorized leaking of information that was not publicly available (Casey, 2011).

• **Intellectual Property Piracy:** In industries based on proprietary (pharmaceuticals, software), digital forensics detects unauthorized distribution of proprietary information (Carrier, 2005).

• **Compliance with regulation:** Businesses must be compliant with data protection law at certain points (e.g., GDPR, CCPA). Digital forensics facilitates compliance auditing and allows businesses to respond to security violations of personal data such that violations are reported and controlled (Kent et al., 2006).

6.3 Cloud Computing Digital Forensics

Cloud computing revolutionized the handling of data and storage by companies and individuals. It has brought with it additional security, handling of data, and forensic examination issues. Cloud computing data is distributed across numerous servers, potentially at different geographical locations, and is difficult to trace and preserve evidence in a forensically sound manner (Taylor et al., 2010).

Amidst all this, digital forensics has evolved to meet the days of cloud computing:

• **Data Recovery:** Data can be recovered by investigations from cloud storage platforms like Google Drive, Dropbox, and iCloud but must prevail over Byzantine privacy laws and terms of service from service providers to gain access to the data (Zawoad and Hasan, 2013).

• **Cloud Forensics Tools: It** witnessed the development of forensic tools to address the challenges posed by cloud computing, such as tools for extracting data from virtual machines, databases, and containerized environments (Ruan et al., 2011).

• **Incident Response:** Incident response is an important task whereby cloud forensics helps organizations to identify intrusions, assess the effect of damage, and ensure compromised systems are quarantined and restored without further compromise (Taylor et al., 2010).

6.4 Mobile Phone Digital Forensics

Mobile phones, as smartphones and tablets, are now ubiquitous in everyday life, with phenomenal capacities for holding personal, financial, and communicational data. Digital phone forensics is therefore a digital forensic subdiscipline, involving data extractions from various mobiles with varying operating systems (i.e., Android, iOS) (Lessard and Kessler, 2010).

Applications in mobile forensics are:

• **Criminal Investigations:** The police usually employ mobile forensics to acquire texts, call histories, GPS location, pictures, video, and application usage information. Information that are typically of a grave nature are verification of alibis, suspicion of suspects, or determining motives in criminal investigations (Casey, 2011).

• **Recovery of Evidence:** The forensic mobile devices can recover deleted data even from crashed phones, allowing the investigators to recover critical evidence such as emails, contacts, or encrypted messages (Quick and Choo, 2014).

• **Tracking Location:** GPS data stored in cellular phones can be useful to locate a suspect at some point of time, which is very useful for criminal cases or missing persons' cases (Zhou and Ni, 2014).

6.5 National Security and Intelligence

Digital forensics is also central to national security and intelligence operations, especially in cyber warfare, terrorism, and espionage. Forensic techniques are used by intelligence agencies in tracing digital communications; tracking cyberattacks and pulling intelligence from hacked systems. Digital forensics is central to reducing state-sponsored cyberattacks and terrorism because it provides evidence to enable intelligence gathering and counterterrorism efforts (Geers, 2011).

7.Future Directions in Digital Forensics

With the emerging technology, digital forensics is evolving as well. Emerging technology and trends are transforming how digital evidence is collected, processed, and presented. As the world is changing rapidly through artificial intelligence (AI), cloud computing, and cybersecurity, digital forensics is about to make a new beginning with great opportunities and challenges ahead (Rogers et al., 2020). Following are some of the most prominent trends that are moulding the future of digital forensics.

7.1 Integration of Artificial Intelligence and Machine Learning

Machine learning and artificial intelligence are the key to transforming digital forensics into a field that can streamline mundane tasks and enable investigators to scan through incredibly vast amounts of data more efficiently. AI can assist in identifying patterns, anomalies, and even predictive data for the aim of enabling forensic investigators to establish leads or anomalies in digital information more efficiently and with shorter timeframes (Bertino and Islam, 2017).

Machine learning can be applied to enhance the surveillance of massive amounts of data, such as unstructured data that appears in text, image, or video form. It can be applied to assist in enhancing the search for preciseness in keywords, file extensions, or hidden patterns that could be of importance for an inquiry. Forensic software based on AI can also mechanize mundane tasks, i.e., verification and comparison of data, so that the investigators can focus on decision-making and analysis at a more strategic level (Shah and Kumar, 2022).

7.2 Evolution of Cloud Forensics

As more individuals and corporations migrate to cloud storage, cloud forensics will increasingly be a component of digital forensics (Ruan et al., 2013). Cloud forensics tools and methods will enhance in the next few years to overcome the inevitability of data spread across multiple servers and jurisdictions (Daryabar et al., 2018). Cloud providers will also most likely incorporate forensic capabilities into their infrastructure, which would support evidence gathering and analysis for investigators (Taylor et al., 2014). The blending of edge computing with cloud infrastructures will also create new opportunities for real-time forensic analysis. This has the potential to enable forensic analysis on live systems, reducing the time it takes to acquire information and increasing the likelihood of preserving volatile data (Alharkan and Aslam, 2020).

7.3 Internet of Things (IoT) Forensics Extension

The new release of Internet of Things (IoT) devices is creating new problems for digital forensics. From home appliances to wearable technology, devices are creating tremendous volumes of data, much of which potentially can be relevant to criminal or civil cases (Zawoad and Hasan, 2015).

IoT forensics will also be an important concern as investigators attempt to recover and analyse data from these kinds of devices. The very, networked nature of IoT systems will necessitate new models of data collection, storage, and analysis (Hassan et al., 2019).

7.4 Increased Focus on Privacy and Ethical Considerations

With digital forensics reaching further, the ethical dilemmas and privacy issues will also follow.

The balancing act between evidence collection and preventing intrusions into individuals' privacy will still be at the forefront (Casey, 2011). The future of digital forensics will involve stricter legal controls and ethics that will compel investigators to conduct their work responsibly but still protect individuals' rights (Maso et al., 2020).

7.5 Future Trends in Mobile Forensics

Mobile forensics will improve with increased usage of mobile phones. Future mobile forensic software will retrieve details from encrypted or physically broken phones more efficiently (Al-Zarouni et al., 2019). Mobile forensics will also focus on retrieving information from apps, geolocation information, and mobile phone cloud storage, which will strengthen investigations (Quick and Choo, 2018).

8. Conclusion

Digital forensics is a dynamic and evolving profession which demands the attention of the hub of truth-finding, crime deterrence, and information integrity within industries. Whether business defence, criminal investigation, or national security, digital forensics employs cross the entire range and lead in this technology era.

With the internet further developing with evolving developing technologies such as artificial intelligence, cloud computing, and the Internet of Things (IoT), digital forensics also must keep evolving to address the new emerging threats and complexity of the evolving technologies. Methods and tools for forensic examiners also keep evolving with a goal of staying ahead of emerging threats and new digital universes. But with these kinds of advancements in technology, legal and ethical issues are at the forefront of digital forensic procedures. Integrity, confidentiality, and compliance with legality are of the highest priority to the validity and integrity of forensic analysis. The future of digital forensics in the coming few years will be determined by increased automation using artificial intelligence, better means of IoT and cloud forensics, and greater focus on privacy and ethical issues.

Digital forensics will keep growing and so will digital forensics application in digital data protection, justice, and trust online. Forensic experts will be forced to be flexible and nimble, constantly staying ahead of their skills and expertise so that they can continue to stay in the game when threats and challenges inevitably arrive in the future. The future of digital forensics is better with more abilities on the horizon with emerging new tools, technologies, and methods arriving that will allow investigators to tackle even the most sophisticated and biggest-scale digital investigations.

Funding: No immediate funding from funding agencies from not-for-profit, commercial, or public sectors was received for this research activity**.**
Conflict of Interest: Declares no conflict of interest.
Ethical Clearance: This study is an evidence-based review and did not involve the use of human participants or animal subjects. Therefore, ethical approval was not required.

References

1. Casey, E. (2011) Handbook of Digital Forensics and Investigation. London: Academic Press.
2. Rogers, M.K. (2006) Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Amsterdam: Elsevier.
3. Vacca, J.R. (2005) Computer Forensics: Computer Crime Scene Investigation. Hingham, MA: Charles River Media.
4. McKemmish, R. (1999) 'What are Computer Forensics?', Australian Institute of Criminology.

5. Pollitt, M.M. (2001) 'Computer Forensics: An Overview', International Journal of Digital Evidence, 1(1), pp. 1–15.
6. Harrison, S. (2007) 'The Importance of Digital Forensics in the Digital Age', Forensic Science Review, 19(2), pp. 1–7.
7. Baggili, I. and White, M. (2009) Digital Forensics for the IT Professional. New York: McGraw-Hill.
8. Smith, M. and McKemmish, R. (2017) 'The Role of Digital Evidence in Criminal Investigations', Proceedings of the Digital Forensics Research Conference, [Location, if known].
9. Sansom, K.A. and Schenck, M. (2010) Introduction to Digital Forensics. Chichester: Wiley.
10. Sullivan, R.D. (2012) Digital Forensics and Investigations: A Guide for Legal Professionals. Boca Raton: CRC Press.
11. Zhao, Q. and Hossain, M.A. (2015) 'Cybersecurity and Digital Forensics: An Overview', in [Book Title, if applicable]. Cham: Springer.
12. Jones, A. and Harvey, J. (2008) 'The Application of Digital Forensics in Cybercrime Investigations', Information Security Journal: A Global Perspective, 17(2), pp. 71–86.
13. Easttom, C. (2018) Computer Security and Digital Forensics. Harlow: Pearson.
14. Zhuang, J. and Zhao, Y. (2014) 'Cloud Computing and Digital Forensics: Legal, Technical, and Ethical Considerations', International Journal of Digital Evidence, 7(2), pp. 101–116.
15. Cohen, F. (2003) Forensic Discovery. Boston: Addison-Wesley.
16. Baker, A. and Pollitt, M.M. (2005) 'Forensic Investigations of Distributed Systems', in [Book/Proceedings Title]. Cham: Springer.
17. Kennesaw, B. (2011) 'Forensic Analysis of Digital Evidence', Forensics International, 13(3), pp. 201–210.
18. Karim, R. and Sudhakar, R. (2013) Digital Forensics and Cyber Crime Investigation. Hoboken: Wiley-IEEE Press.
19. Delac, K. and Luks, J. (2014) Advanced Methods in Digital Forensics: A Case Study Approach. Cham: Springer.
20. Mikkelson, T. and Jansen, B. (2011) Investigating Digital Evidence: Tools and Techniques. Hoboken: Wiley.
21. Lloyd, M. and Mole, A. (2008) 'Digital Forensics and the Cloud: Challenges and Opportunities', International Journal of Cyber Criminology, 5(1), pp. 167–182.
22. Garfinkel, S.L. (2010) 'Digital Forensics and the Need for Standards', National Institute of Standards and Technology. Available at: [URL if online] (Accessed: [date]).
23. Beebe, N.H. and Clark, J.G. (2005) 'A Framework for Digital Forensic Research', Proceedings of the Digital Forensic Research Workshop.
24. Goodrum, A.A. and Whitfield, L.C. (2016) Digital Evidence and Forensic Investigation: A Guide for Corporate Investigations. Cham: Springer.
25. Franceschi-Bicchierai, L. (2013) 'Hacking the Digital Evidence', IEEE Security & Privacy, 11(1), pp. 75–80.
26. Raghavan, S. (2013) Digital Forensic Research: Current State and Future Directions. Cham: Springer.
27. Lesk, M. (2007) The New Front Line: Forensics in Cybersecurity. New York: Oxford University Press.

28. Quick, D. and Choo, K.K.R. (2014) 'Digital Forensic Intelligence: Data Subset Selection and Analysis', Information Sciences, 281, pp. 478–497.

29. Altheide, C. and Carvey, H. (2011) Digital Forensics with Open Source Tools. Waltham, MA: Syngress.

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

31. Carrier, B. (2005) File System Forensic Analysis. Boston: Addison-Wesley.

32. Meyers, M. and Rogers, M. (2004) 'Computer Forensics: The Need for Standardization and Certification', International Journal of Digital Evidence, 3(2), pp. 1–11.

33. Kim, K. and Hong, S. (2012) 'Digital Forensics and Cybercrime', in Proceedings of the International Conference on Information Security and Assurance. Cham: Springer.

34. Sammons, J. (2012) The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Waltham, MA: Syngress.

35. Prosise, C. and Mandia, K. (2003) Incident Response and Computer Forensics. 2nd edn. New York: McGraw-Hill.

36. Baryamureeba, V. and Tushabe, F. (2004) 'The Enhanced Digital Investigation Process Model', Proceedings of the Fourth Digital Forensic Research Workshop (DFRWS 2004).

37. Palmer, G. (2001) 'A Road Map for Digital Forensic Research', Report for the First Digital Forensic Research Workshop (DFRWS 2001). Available at: [URL if online] (Accessed: [date]).

38. Reith, M., Carr, C. and Gunsch, G. (2002) 'An Examination of Digital Forensic Models', International Journal of Digital Evidence, 1(3), pp. 1–12.

39. Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006) Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD: National Institute of Standards and Technology.

40. Beebe, N.L. and Clark, J.G. (2007) 'A Hierarchical, Objectives-Based Framework for the Digital Investigations Process', Digital Investigation, 4(2), pp. 147–167.

41. Cohen, F. (2010) 'Digital Forensic Evidence Examination', IFIP Advances in Information and Communication Technology, 337, pp. 1–15.

42. Gladyshev, P. and Patel, A. (2004) 'Finite State Machine Approach to Digital Event Reconstruction', Digital Investigation, 1(2), pp. 130–149.

43. Carrier, B. and Spafford, E.H. (2004) 'An Event-Based Digital Forensic Investigation Framework', Proceedings of the Digital Forensic Research Workshop (DFRWS 2004).

44. Casey, E. (2009) Handbook of Digital Forensics and Investigation. London: Academic Press.

45. Rogers, M.K., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006) 'Computer Forensics Field Triage Process Model', Proceedings of the Digital Forensic Research Workshop (DFRWS 2006).

46. Baryamureeba, V. and Tushabe, F. (2004) 'The Enhanced Digital Investigation Process Model', Proceedings of the Digital Forensic Research Workshop (DFRWS 2004).

47. Pollitt, M.M. (1995) 'Computer Forensics: An Approach to Evidence in Cyberspace', National Information Systems Security Conference, pp. 487–491.

48. Hoelz, B., Ralha, C. and Geeverghese, R. (2009) 'Artificial Intelligence Applied to Computer Forensics', Proceedings of the 2009 ACM Symposium on Applied Computing, pp. 883–888.

49. Rowe, N.C. and Garfinkel, S. (2011) 'Finding Anomalous and Suspicious Files', IEEE Security & Privacy, 9(5), pp. 43–49.

50. Roussev, V., Richard III, G.G. and Marziale, L. (2007) 'Multi-Resolution Similarity Hashing', Digital Investigation, 4, pp. 105–113.

51. Stolfo, S.J., Bellovin, S.M., Keromytis, A.D., Hershkop, S., Smith, S.W. and Sinclair, S. (2011) Insider Attack and Cyber Security: Beyond the Hacker. New York: Springer.

52. Heuer Jr, R.J. (1999) Psychology of Intelligence Analysis. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency.

53. Baryamureeba, V. and Tushabe, F. (2004) 'The Enhanced Digital Investigation Process Model', Proceedings of the Digital Forensic Research Workshop (DFRWS 2004).

54. Rogers, M.K. (2004) 'A Two-Dimensional Circumstantial Evidence Model for Digital Forensic Investigations', Digital Forensic Research Workshop (DFRWS 2004).

55. Ciardhuáin, S.Ó. (2004) 'An Extended Model of Cybercrime Investigations', International Journal of Digital Evidence, 3(1), pp. 1–22.

56. Casey, E. (2011) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd edn. London: Academic Press.

57. Baryamureeba, V. and Tushabe, F. (2004) 'The Enhanced Digital Investigation Process Model', Proceedings of the Digital Forensic Research Workshop (DFRWS 2004).

58. Carrier, B. and Spafford, E.H. (2003) 'Getting Physical with the Digital Investigation Process', International Journal of Digital Evidence, 2(2), pp. 1–20.

59. Ciardhuáin, S.Ó. (2004) 'An Extended Model of Cybercrime Investigations', International Journal of Digital Evidence, 3(1), pp. 1–22.

60. Pollitt, M. (2010) 'A History of Digital Forensics', in Advances in Digital Forensics VI. New York: Springer, pp. 3–15.

61. Cohen, F. (2010) 'Digital Forensic Evidence Examination', IFIP Advances in Information and Communication Technology, 337, pp. 1–15.

62. Rogers, M.K. (2006) 'A Two-Dimensional Circumstantial Evidence Model for Digital Forensic Investigations', Digital Forensic Research Workshop (DFRWS 2006).

63. Carrier, B. (2006) File System Forensic Analysis. Boston: Addison-Wesley.

64. Rogers, M.K. (2004) 'A Two-Dimensional Circumstantial Evidence Model for Digital Forensic Investigations', Digital Forensic Research Workshop (DFRWS 2004).

65. Palmer, G. (2001) 'A Road Map for Digital Forensic Research', Report for the First Digital Forensic Research Workshop (DFRWS 2001).

66. Casey, E. (2009) Handbook of Digital Forensics and Investigation. London: Academic Press.

67. Carrier, B. (2005) File System Forensic Analysis. Boston: Addison-Wesley.

68. Baryamureeba, V. and Tushabe, F. (2004) 'The Enhanced Digital Investigation Process Model', Proceedings of the Digital Forensic Research Workshop (DFRWS 2004).

69. Ciardhuáin, S.Ó. (2004) 'An Extended Model of Cybercrime Investigations', International Journal of Digital Evidence, 3(1), pp. 1–22.

70. Casey, E. (2011) Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd edn. London: Academic Press.

71. Beebe, N.L. and Clark, J.G. (2007) 'A Hierarchical, Objectives-Based Framework for the Digital Investigations Process', Digital Investigation, 4(2), pp. 147–167.

72. Cohen, F. (2010) 'Digital Forensic Evidence Examination', IFIP Advances in Information and Communication Technology, 337, pp. 1–15.

73. Gladyshev, P. and Patel, A. (2004) 'Finite State Machine Approach to Digital Event Reconstruction', Digital Investigation, 1(2), pp. 130–149.

74. Carrier, B. and Spafford, E.H. (2004) 'An Event-Based Digital Forensic Investigation Framework', Proceedings of the Digital Forensic Research Workshop (DFRWS 2004).

75. Casey, E. (2009) Handbook of Digital Forensics and Investigation. London: Academic Press.

76. Rogers, M.K., Goldman, J., Mislan, R., Wedge, T. and Debrota, S. (2006) 'Computer Forensics Field Triage Process Model', Proceedings of the Digital Forensic Research Workshop (DFRWS 2006).

77. Palmer, G. (2001) 'A Road Map for Digital Forensic Research', Report for the First Digital Forensic Research Workshop (DFRWS 2001).

78. Pollitt, M.M. (1995) 'Computer Forensics: An Approach to Evidence in Cyberspace', National Information Systems Security Conference, pp. 487–491.

79. Hoelz, B., Ralha, C. and Geeverghese, R. (2009) 'Artificial Intelligence Applied to Computer Forensics', Proceedings of the 2009 ACM Symposium on Applied Computing, pp. 883–888.

80. Rowe, N.C. and Garfinkel, S. (2011) 'Finding Anomalous and Suspicious Files', IEEE Security & Privacy, 9(5), pp. 43–49.

81. Roussev, V., Richard III, G.G. and Marziale, L. (2007) 'Multi-Resolution Similarity Hashing', Digital Investigation, 4, pp. 105–113.

82. Garfinkel, S.L. (2010) 'Digital Forensics Research: The Next 10 Years', Digital Investigation, 7, pp. S64–S73.

83. Roussev, V., Richard III, G.G. and Marziale, L. (2007) 'Multi-Resolution Similarity Hashing', Digital Investigation, 4, pp. 105–113.

84. Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M. (2016) 'Current Challenges and Future Research Areas for Digital Forensic Investigation', arXiv preprint arXiv:1604.03850. Available at: https://arxiv.org/abs/1604.03850

85. Kent, K., Chevalier, S., Grance, T. and Dang, H. (2006) Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD: National Institute of Standards and Technology.

86. Stallings, W. (2012) Computer Security: Principles and Practice. 3rd edn. Upper Saddle River, NJ: Prentice Hall.

87. Stallings, W. (2012) Cryptography and Network Security: Principles and Practice. 6th edn. Upper Saddle River, NJ: Prentice Hall.

88. McKemmish, R. (1999) 'What is Forensic Computing?', Trends & Issues in Crime and Criminal Justice, 118. Canberra: Australian Institute of Criminology.

89. Mandia, K., Prosise, C. and Pepe, M. (2003) Incident Response & Computer Forensics. 2nd edn. New York: McGraw-Hill/Osborne.