

Digital Forensics and the Investigation of Contemporary Cybercrime

Jiankun Hu

Professor, University of New South Wales (UNSW Canberra), Australia

Abstract

The rapid expansion of digital technologies has transformed cybercrime into a complex and continuously evolving global challenge. Modern cybercriminal activities increasingly involve advanced techniques such as ransomware attacks, identity theft, digital fraud, data breaches, cloud-based crimes, and attacks on interconnected systems. In this environment, digital forensics has emerged as a critical discipline for identifying, preserving, analysing, and presenting digital evidence to support cybercrime investigations.

This research examines the role of digital forensics in contemporary cybercrime investigation by exploring forensic processes, emerging technological approaches, analytical challenges, and future directions. The study adopts a conceptual research approach based on an extensive review of scholarly literature, cybersecurity frameworks, and established forensic practices. The analysis highlights the importance of evidence acquisition, forensic integrity, advanced data analysis, artificial intelligence-assisted investigation, and cross-platform examination techniques in improving investigative effectiveness.

The study also identifies major challenges, including encryption barriers, increasing data volumes, privacy concerns, anti-forensic techniques, and rapidly changing attack methodologies. The findings suggest that successful cybercrime investigation requires a combination of advanced forensic technologies, skilled professionals, ethical governance, and internationally coordinated investigative frameworks. Digital forensics will continue to play a fundamental role in strengthening cybersecurity resilience and ensuring accountability within the digital ecosystem.

Keywords: Digital Forensics, Cybercrime Investigation, Digital Evidence, Cybersecurity, Malware Analysis, Artificial Intelligence, Incident Response, Data Recovery.

1. Introduction

The increasing dependence on digital infrastructure has significantly changed the nature of criminal activities in modern society. Organisations, governments, businesses, and individuals generate enormous volumes of digital information through computers, smartphones, cloud platforms, Internet of Things (IoT) devices, and online communication systems. While these technologies have improved connectivity and efficiency, they have also created new opportunities for cybercriminal activities. Contemporary cybercrime has evolved beyond traditional hacking practices and now includes sophisticated attacks such as ransomware campaigns, financial fraud, cyber espionage, data theft, and attacks against critical digital infrastructure.

Digital forensics has become an essential component of cybersecurity and law enforcement because cybercriminal activities frequently leave behind complex digital traces. Digital forensic investigation involves the systematic identification, collection, preservation, examination, and interpretation of electronic evidence while maintaining evidentiary integrity. Unlike traditional investigations, digital investigations require specialised techniques because digital evidence can be easily modified, encrypted, distributed across multiple locations, or hidden through advanced anti-forensic methods. Therefore, maintaining authenticity and reliability of digital evidence remains one of the most important requirements in cybercrime investigations.

The growth of contemporary cyber threats has expanded the scope of digital forensic practices. Earlier forensic investigations primarily focused on analysing computer storage devices; however, modern investigations involve cloud environments, mobile devices, network infrastructures, cryptocurrency transactions, social media platforms, and artificial intelligence-generated content. Investigators must now analyse diverse digital sources while dealing with large-scale datasets and rapidly changing technological environments. These developments have encouraged the adoption of advanced approaches such as machine learning-based evidence analysis, automated malware detection, and intelligent forensic investigation frameworks.

Despite significant technological advancements, digital forensic investigations continue to face several operational and technical challenges. Increasing encryption usage, sophisticated malware, anonymous communication networks, jurisdictional limitations, and privacy-related concerns create difficulties in obtaining and analysing digital evidence. Furthermore, cybercriminals increasingly employ anti-forensic strategies to conceal their activities, delete traces, or manipulate evidence. These challenges require continuous improvement in forensic methodologies, professional expertise, and international cooperation.

This research examines the importance of digital forensics in investigating contemporary cybercrime. The study explores major forensic techniques, emerging technological applications, investigative limitations, and future opportunities for strengthening cybercrime response mechanisms. By analysing current practices and challenges, the research highlights how digital forensics contributes to reliable evidence discovery, criminal attribution, and improved cybersecurity preparedness in an increasingly digital society.

2. Review of Literature

2.1 Evolution of Digital Forensics and Cybercrime Investigation Practices

Digital forensics has developed from a specialised computer recovery practice into a comprehensive investigative discipline that supports modern cybersecurity operations and legal proceedings. Early research in digital investigation primarily focused on recovering deleted files, analysing computer storage devices, and identifying unauthorised access activities. As cybercrime became more sophisticated, researchers highlighted the need for structured forensic frameworks that could ensure evidence reliability, repeatability, and legal acceptance. Carrier and Spafford introduced foundational concepts of digital investigation by emphasising systematic evidence identification, preservation, and analysis processes that maintain the integrity of digital artefacts.

Subsequent developments expanded digital forensics beyond traditional computer investigations. The emergence of network-based attacks, mobile computing, cloud services, and connected devices

required investigators to adopt broader approaches capable of examining multiple digital environments simultaneously. According to Casey, digital evidence management became increasingly complex because cyber incidents often involve distributed data sources, encrypted communication channels, and rapidly changing technological platforms. This transformation established digital forensics as a multidisciplinary field combining cybersecurity, information systems, legal procedures, and investigative science.

Modern forensic practices now incorporate automated tools, artificial intelligence techniques, and advanced data analytics to improve investigation efficiency. Researchers have explored the use of machine learning algorithms for malware classification, anomaly detection, and identification of suspicious digital behaviour. These developments demonstrate that digital forensics has shifted from reactive evidence recovery toward proactive cyber threat investigation and intelligence-driven security management.

2.2 Digital Evidence Analysis and Emerging Forensic Technologies

Digital evidence represents the foundation of cybercrime investigation because it provides critical information regarding criminal activities, attack methods, and potential offenders. Research in digital evidence analysis has highlighted the importance of maintaining evidence authenticity, establishing chain of custody, and applying scientifically valid examination procedures. Digital forensic investigators must ensure that collected information remains unchanged from acquisition to presentation, particularly when evidence is used in judicial contexts.

The rapid adoption of cloud computing, mobile applications, and Internet of Things technologies has introduced new complexities in evidence collection. Cloud environments create challenges because data may be distributed across multiple geographical locations and controlled by external service providers. Similarly, mobile devices generate diverse forms of evidence, including communication records, location information, application data, and biometric information. Researchers have suggested that traditional forensic approaches require continuous adaptation to address the dynamic nature of these technologies.

Artificial intelligence and big-data analytics are increasingly being investigated as supportive technologies for digital forensic examination. Automated systems can assist investigators in identifying patterns within large datasets, detecting malware behaviour, prioritising evidence, and reducing manual analysis time. However, researchers also emphasise that automated forensic systems require careful validation because inaccurate interpretation of digital evidence may negatively affect investigative outcomes.

2.3 Contemporary Cybercrime Trends and Investigative Challenges

Contemporary cybercrime has become increasingly organised, financially motivated, and technologically advanced. Studies indicate that cybercriminal groups now utilise ransomware-as-a-service models, advanced persistent threats, cryptocurrency-based financial transactions, and social engineering techniques to conduct large-scale attacks. These developments have increased the complexity of investigations because attackers often operate across international boundaries and employ sophisticated methods to conceal their identities.

A significant area of research focuses on anti-forensic techniques used by criminals to obstruct investigations. These techniques include data wiping, encryption, metadata manipulation, anonymous communication methods, and malware designed to avoid detection. Researchers have highlighted that investigators require advanced analytical capabilities and continuous training to successfully overcome these obstacles.

Another important research area involves balancing investigative effectiveness with privacy protection. Digital forensic investigations frequently involve personal information, raising ethical and legal concerns regarding data access, storage, and usage. Scholars have suggested that future forensic frameworks should integrate privacy-preserving approaches while maintaining the ability to identify and prosecute cybercriminal activities. This balance between security requirements and individual privacy remains a central issue in the advancement of digital forensic practices.

3. Objectives of the Study

3.1 Examination of Digital Forensic Frameworks in Cybercrime Investigation

The primary objective of this study is to analyse the role and significance of digital forensic methodologies in investigating contemporary cybercrime. The study examines how forensic processes support evidence identification, acquisition, preservation, examination, and interpretation during cybercrime investigations.

The objective further focuses on understanding how traditional forensic approaches are adapting to modern digital environments involving cloud computing, mobile technologies, artificial intelligence systems, and interconnected devices.

The study aims to evaluate the contribution of digital forensics in improving investigative accuracy, evidence reliability, and cybercrime response capabilities.

3.2 Evaluation of Emerging Technologies and Future Investigative Approaches

This study also aims to explore the influence of emerging technologies on the future development of digital forensic investigation. Particular attention is given to artificial intelligence, machine learning, automation, and advanced analytical techniques that enhance the ability to process large-scale digital evidence.

The objective is to identify opportunities where technological innovation can improve forensic efficiency while addressing limitations associated with complex cybercrime scenarios.

The study further examines future requirements for developing ethical, scalable, and reliable forensic frameworks capable of responding to evolving cyber threats.

4. Research Methodology

4.1 Research Design and Conceptual Approach

This study adopts a conceptual research design to examine the relationship between digital forensics and contemporary cybercrime investigation practices. The research approach is based on the systematic analysis of existing scholarly literature, cybersecurity frameworks, forensic investigation models, and documented technological developments. A conceptual methodology is appropriate because the study focuses on understanding investigative processes, emerging forensic techniques, operational challenges, and future directions rather than testing a specific experimental hypothesis.

The research framework considers digital forensics as an integrated investigative discipline that combines technical examination, evidence management, cybersecurity practices, and legal considerations. The study analyses major components of digital forensic investigation, including evidence acquisition, preservation procedures, forensic analysis methods, technological applications, and challenges affecting investigative effectiveness.

The conceptual approach enables a broader understanding of how digital forensic practices are evolving in response to increasingly sophisticated cybercrime patterns. It also supports the identification of research gaps related to automation, scalability, privacy protection, and international cooperation.

4.2 Data Sources and Literature Selection Approach

The study is based on secondary data collected from peer-reviewed research publications, academic books, cybersecurity standards, digital investigation frameworks, and professional security reports. The reviewed sources focus on major areas including digital evidence analysis, cybercrime investigation methodologies, malware investigation, cloud forensics, mobile forensics, and artificial intelligence-assisted forensic techniques.

The literature selection process considered sources that directly contributed to understanding contemporary cybercrime investigation challenges and technological advancements in digital forensics. Priority was given to academically reliable publications that discuss established forensic models, investigative procedures, and emerging security concerns.

The collected information was analysed through thematic evaluation, where major concepts were categorised into forensic processes, technological innovations, investigative limitations, and future development opportunities.

4.3 Analytical Framework

The analytical framework of the study examines digital forensics through four interconnected dimensions: evidence management, technological capability, investigative challenges, and future advancement. These dimensions provide a structured method for evaluating how forensic practices support cybercrime investigations.

The framework considers that effective cybercrime investigation requires not only advanced forensic tools but also reliable procedures, skilled investigators, ethical guidelines, and collaboration among cybersecurity stakeholders. The analysis therefore integrates technical and organisational perspectives to provide a comprehensive understanding of digital forensic effectiveness.

The study uses qualitative interpretation to evaluate relationships between emerging cyber threats and corresponding forensic responses. The findings are presented through comparative analysis and conceptual assessment of major forensic components.

4.4 Research Methodology Framework

Table 1: Research Methodology Framework for Digital Forensic Investigation Study

Research Component	Description
Research Design	Conceptual research approach based on digital forensic and cybersecurity literature
Data Sources	Peer-reviewed articles, cybersecurity frameworks, forensic standards, and academic publications
Analysis Method	Thematic analysis of forensic practices, technologies, and investigative challenges
Research Focus	Digital evidence management, cybercrime investigation methods, emerging forensic technologies

Interpretation: The methodology framework demonstrates that the study follows a structured conceptual process combining theoretical knowledge and contemporary cybersecurity practices. The approach supports a comprehensive evaluation of digital forensics as an investigative mechanism for addressing modern cybercrime.

5. Analysis

5.1 Role of Digital Forensics in Contemporary Cybercrime Investigation

Digital forensics has become a fundamental mechanism for identifying cybercriminal activities and establishing reliable connections between digital evidence and criminal events. Modern cyber incidents generate multiple forms of evidence, including system logs, network traffic records, application data, metadata, digital communications, and financial transaction records. The ability to collect and analyse these sources determines the effectiveness of cybercrime investigations.

The analysis indicates that forensic investigation follows a structured process beginning with evidence identification and preservation, followed by examination, interpretation, and reporting. Maintaining evidence integrity throughout this process is essential because manipulated or improperly collected evidence can reduce investigative credibility. Digital forensic procedures therefore provide a scientific foundation for converting complex digital traces into meaningful investigative information.

The increasing complexity of cyber threats has expanded the role of forensic investigators from evidence recovery specialists to cybersecurity intelligence professionals. Investigators now analyse attack patterns, identify vulnerabilities, reconstruct digital events, and support preventive security strategies.

5.2 Analysis of Emerging Technologies Supporting Digital Forensics

Advanced technologies are significantly influencing the development of modern digital forensic practices. Artificial intelligence, machine learning, automation, and big-data analytics provide new

capabilities for analysing extensive volumes of digital information. These technologies help investigators identify suspicious activities, classify malware behaviour, and prioritise relevant evidence.

Artificial intelligence-based forensic systems can reduce investigation time by automating repetitive analytical tasks. For example, machine learning models can assist in detecting abnormal network behaviour, recognising malicious patterns, and correlating information from multiple evidence sources. However, human expertise remains essential because automated outputs require professional interpretation and validation.

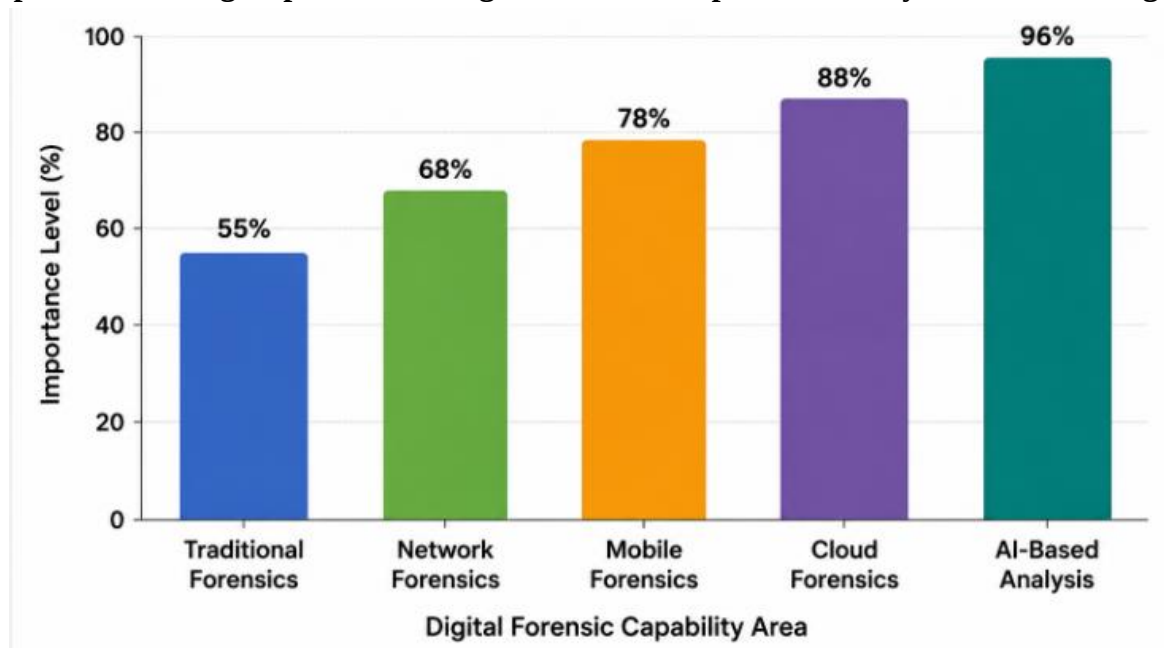
Cloud computing and Internet of Things environments have also transformed forensic requirements. Investigators must now examine distributed systems, remote storage platforms, and interconnected devices, requiring adaptive forensic methodologies capable of handling diverse digital ecosystems.

5.3 Comparative Analysis of Major Digital Forensic Areas

Table 2: Major Digital Forensic Domains and Their Investigative Contributions

Forensic Domain	Primary Evidence Source	Investigative Contribution
Computer Forensics	Hard drives, operating systems, system files	Recovery and analysis of digital activities
Network Forensics	Network traffic and communication records	Detection of attacks and intrusion patterns
Mobile Forensics	Smartphones and application data	Analysis of communication and user activities
Cloud Forensics	Cloud storage and virtual environments	Investigation of distributed digital evidence

Interpretation: The table demonstrates that different forensic domains contribute unique capabilities to cybercrime investigation. Effective investigations increasingly require integration among multiple forensic approaches because contemporary cyberattacks commonly involve several digital platforms simultaneously.

Graph 1: Increasing Importance of Digital Forensic Capabilities in Cybercrime Investigation

Interpretation: The graph indicates a progressive increase in the importance of advanced forensic capabilities. While traditional computer forensics remains essential, contemporary cybercrime investigations increasingly depend on network analysis, mobile evidence examination, cloud investigation, and artificial intelligence-assisted approaches.

6. Challenges

6.1 Increasing Complexity of Cybercrime Techniques

The continuous evolution of cybercrime represents one of the most significant challenges for digital forensic investigators. Cybercriminals increasingly employ sophisticated methods such as advanced malware, ransomware, encrypted communication channels, artificial intelligence-assisted attacks, and identity concealment techniques. These approaches make it difficult for investigators to identify attack sources, reconstruct criminal activities, and collect reliable digital evidence.

The complexity of modern cyber environments also creates difficulties because cyber incidents rarely occur within a single technological platform. A single cyberattack may involve compromised computers, cloud services, mobile devices, social media platforms, and international networks. Investigators must therefore integrate evidence from multiple sources while maintaining accuracy and consistency throughout the forensic process.

Another major concern is the rapid development of anti-forensic techniques. Cybercriminals may intentionally modify, delete, encrypt, or hide digital traces to prevent successful investigation. Addressing these challenges requires continuous improvement in forensic methodologies, advanced analytical tools, and specialised investigator training.

6.2 Data Volume, Encryption, and Privacy Concerns

The enormous growth of digital data has created significant challenges for forensic examination. Modern devices and online platforms generate massive quantities of information, making manual investigation

approaches inefficient. Investigators require advanced technologies capable of filtering relevant evidence, analysing large datasets, and identifying meaningful patterns without compromising accuracy.

Encryption has further increased investigative difficulty by protecting information from unauthorised access. Although encryption provides essential security and privacy benefits, it can also restrict investigators' ability to access critical evidence during cybercrime investigations. Developing lawful and technically effective approaches for dealing with encrypted data remains a continuing challenge.

Privacy protection is another important consideration in digital forensic activities. Investigations often involve sensitive personal and organisational information, requiring careful management of evidence collection, storage, and analysis. Maintaining a balance between effective cybercrime investigation and protection of individual privacy rights is essential for ethical forensic practices.

6.3 Skill Requirements and Legal Challenges

Digital forensic investigation requires highly specialised knowledge because cybercrime techniques and technologies change rapidly. Investigators must understand operating systems, networks, malware behaviour, cloud infrastructures, artificial intelligence applications, and legal procedures. The shortage of skilled professionals creates limitations in responding effectively to increasingly complex cyber incidents.

Legal and jurisdictional challenges also affect cybercrime investigations. Since cybercriminals often operate across national boundaries, investigators may face difficulties related to international cooperation, evidence sharing, and differences in cybercrime legislation. Establishing consistent international frameworks is necessary to improve cross-border digital investigations.

The admissibility of digital evidence in legal proceedings requires strict compliance with forensic standards. Improper collection, insufficient documentation, or weak chain-of-custody procedures may reduce the reliability of evidence. Therefore, professional standards and regulatory frameworks remain essential components of successful digital forensic practices.

7. Discussion

7.1 Digital Forensics as a Strategic Cybersecurity Capability

The findings of this study demonstrate that digital forensics has evolved from a reactive investigative function into a strategic cybersecurity capability. Traditional security approaches primarily focused on preventing attacks; however, the increasing sophistication of cyber threats requires organisations to develop strong detection, investigation, and recovery mechanisms. Digital forensics provides valuable support by enabling organisations to understand attack methods, identify compromised systems, and develop improved security strategies.

The integration of forensic investigation with cybersecurity operations has created stronger incident response capabilities. Security teams can use forensic findings to determine the origin of attacks, assess damage, identify exploited vulnerabilities, and implement preventive measures. This relationship highlights that digital forensics is not limited to post-incident investigation but also contributes to proactive cybersecurity improvement.

Furthermore, the adoption of advanced analytical technologies has expanded forensic capabilities. Artificial intelligence and automated analysis systems provide opportunities to process large

amounts of evidence efficiently. However, technological advancement should complement rather than replace expert judgement because forensic conclusions require contextual understanding and professional interpretation.

7.2 Technological Innovation and Future Development of Digital Investigation

Emerging technologies are expected to significantly influence the future direction of digital forensics. Artificial intelligence-based investigation tools, automated evidence classification systems, blockchain-supported evidence verification, and advanced behavioural analysis methods can improve forensic accuracy and efficiency. These innovations provide opportunities to overcome limitations associated with increasing data complexity and investigation time requirements.

Cloud computing and Internet of Things environments require researchers and practitioners to redesign existing forensic approaches. Future forensic frameworks must address distributed evidence collection, real-time analysis, and cross-platform investigation. Traditional methods designed for isolated computing systems may not be sufficient for modern interconnected digital environments.

The future of digital forensics will depend on developing adaptive frameworks capable of responding to continuously changing cyber threats. Collaboration between cybersecurity researchers, law enforcement agencies, technology developers, and legal authorities will be essential for creating effective and ethically responsible forensic systems.

7.3 Ethical Governance and Responsible Forensic Practices

The expansion of digital forensic capabilities creates important ethical considerations regarding privacy, surveillance, and data protection. While forensic investigations are necessary for combating cybercrime, excessive or uncontrolled access to personal information may create risks for individual rights. Therefore, transparent procedures, legal oversight, and responsible evidence-handling practices are essential.

Future forensic frameworks should incorporate privacy-preserving approaches that allow investigators to analyse relevant evidence while reducing unnecessary exposure of personal information. Ethical governance mechanisms can strengthen public trust and ensure that digital investigation practices remain aligned with legal and social expectations.

The discussion highlights that successful digital forensics requires a balanced approach combining technological innovation, professional expertise, legal compliance, and ethical responsibility. Such integration will determine the effectiveness of cybercrime investigation in future digital ecosystems.

8. Conclusion

Digital forensics has become an indispensable discipline for investigating contemporary cybercrime because modern criminal activities increasingly depend on complex digital infrastructures. The study demonstrates that forensic methodologies provide essential capabilities for identifying digital evidence, reconstructing cyber incidents, analysing attacker behaviour, and supporting legal accountability. As cyber threats continue to evolve, digital forensic practices must continuously adapt to address new technological environments and sophisticated attack strategies.

The analysis reveals that emerging technologies such as artificial intelligence, machine learning, cloud computing, and automated analytics are transforming forensic investigation processes. These technologies improve the ability to process large-scale digital evidence and detect complex cyber activities. However, technological advancement alone cannot guarantee effective investigation outcomes. Skilled professionals, validated procedures, ethical frameworks, and appropriate legal mechanisms remain equally important for maintaining forensic reliability.

Contemporary cybercrime presents challenges involving encryption, anti-forensic methods, increasing data volumes, and international jurisdictional issues. Addressing these challenges requires collaboration among cybersecurity experts, researchers, legal authorities, and technology organisations. Future digital forensic frameworks should focus on scalability, transparency, privacy protection, and international cooperation to remain effective against emerging cyber threats.

In conclusion, digital forensics represents a critical foundation for cybersecurity resilience and digital accountability. Its continued advancement will play a central role in protecting individuals, organisations, and governments from increasingly sophisticated cybercrime activities while ensuring responsible and trustworthy investigation practices.

References

1. Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press/Elsevier.
2. Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation. *International Journal of Computer Science & Information Technology*, 3(3).
3. Sindhu, K. K. (2012). Digital Forensics and Cyber Crime Datamining. *Journal of Information Security*, 3(3), 196–201.
4. Garfinkel, S. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, 7, S64–S73.
5. Rogers, M. K., & Seigfried-Spellar, K. C. (Eds.). (2013). *Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C 2012*. Springer.
6. Gladyshev, P., Marrington, A., & Baggili, I. (Eds.). (2014). *Digital Forensics and Cyber Crime: Fifth International Conference, ICDF2C 2013*. Springer.
7. Chawki, M., Darwish, A., Khan, M. A., & Tyagi, S. (2015). *Cybercrime, Digital Forensics and Jurisdiction*. Springer.
8. Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, 17(2), 183–194. <https://doi.org/10.1080/15614263.2015.1128163>.
9. Watson, D., & Jones, A. (2013). *Digital Forensics Processing and Procedures: Meeting the Requirements of ISO 17020, ISO 17025, ISO 27001 and Best Practice Requirements*. Syngress.
10. van Baar, R., van Beek, H., & van Eijk, E. (2014). Digital Forensics as a Service: A Game Changer. *Digital Investigation*, 11, S54–S62.
11. Arnes, A. (Ed.). (2017). *Digital Forensics*. John Wiley & Sons.
12. Roussev, V. (2016). *Digital Forensic Science: Issues, Methods, and Challenges*. Springer.
13. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction* (2nd ed.). Routledge.
14. Choo, K.-K. R., & Dehghantanha, A. (Eds.). (2017). *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*. Syngress/Elsevier.
15. Quick, D., Choo, K.-K. R., & Vasilios, M. (2017). Cloud forensics: A survey of challenges, methods and future directions. *Digital Investigation*.



16. Brennan, F., Udris, M., & Gladyshev, P. (2014). An Automated Link Analysis Solution Applied to Digital Forensic Investigations. In *Digital Forensics and Cyber Crime*. Springer.
17. Breitingner, F., Liu, H., Winter, C., Baier, H., Rybalchenko, A., & Steinebach, M. (2014). Towards a Process Model for Hash Functions in Digital Forensics. In *Digital Forensics and Cyber Crime*. Springer.
18. Sabillon, R., Serra-Ruiz, J., Cavaller, V., & Cano, J. J. (2018). Digital Forensic Analysis of Cybercrimes: Best Practices and Methodologies. In *Digital Multimedia: Concepts, Methodologies, Tools, and Applications*. IGI Global.
19. Breitingner, F., & Baggili, I. (Eds.). (2018). Digital Forensics and Cyber Crime: 10th International EAI Conference, ICDF2C 2018. Springer.
20. Breitingner, F., Baggili, I., & others. (2018). Digital Forensic Readiness Framework for Ransomware Investigation. In *Digital Forensics and Cyber Crime: ICDF2C 2018*, pp. 91–105. Springer.