World Journal of Information Technology
ISSN: 2959-9911
DOI: https://doi.org/10.61784/wjit3018

ADVANCING DIGITAL FORENSIC INVESTIGATIONS: ADDRESSING CHALLENGES AND ENHANCING CYBERCRIME SOLUTIONS

Firzah Hafiz Deandra, Sherly, Iskandar Muda*
Universitas Sumatera Utara, Medan, Indonesia.
Corresponding author: Iskandar Muda, Email: ismuda.jurnal.internasional@gmail.com

Abstract: Digital forensics is a critical discipline focused on the identification, preservation, analysis, and presentation of digital evidence in a legally admissible manner. This paper examines the implementation of Digital Forensic Investigations (DFIs) in combating cybercrime, emphasizing the technical, organizational, and legal challenges hindering their effectiveness. The study highlights strategies to enhance forensic processes and improve cybercrime investigations. Structured forensic methodologies, guided by international standards like ISO 27037:2012, ensure the integrity and credibility of evidence while addressing challenges such as encrypted communications, cloud environments, and decentralized data storage. Specialized tools for data recovery, mobile forensics, and cloud forensics are increasingly pivotal in modern investigations. The paper underscores the role of digital forensics in strengthening cybersecurity, reconstructing cybercrime events, and supporting legal proceedings through reliable evidence. Advancements in artificial intelligence and machine learning are also explored as innovative approaches to tackling sophisticated cyber threats, underscoring the evolving nature of digital forensics in ensuring justice and securing digital ecosystems.
Keywords: Digital forensics; Cybercrime; Digital evidence; Digital Forensic Investigations (DFIs); Cybersecurity

1 INTRODUCTION

The rapid advancement of technology and the increasing accessibility of critical and sensitive information have elevated the risks associated with cybercrime. Digital Forensic Investigations (DFIs) play a crucial role in identifying, analyzing, and addressing these crimes, linking digital evidence to establish factual information for judicial processes [1]. The implementation of DFIs in cybercrime scenarios requires a thorough understanding of both the challenges and principles governing forensic investigations.

Information security should be a shared priority among IT personnel, users, and management within organizations. However, historical trends indicate that it has not consistently ranked as a top concern. Organizations often prioritize budgets and operational challenges, such as staff shortages, over investing in information security measures. Surveys and reports highlight barriers such as insufficient resources, limited funding, and inadequate tools, which leave organizations vulnerable to sophisticated cyberattacks. Consequently, forensic investigators often operate in environments with weak security protocols, complicating efforts to track and mitigate cyber threats.

Access control is a cornerstone of information security, but its inconsistent implementation increases vulnerabilities. Systems should enforce strict levels of authorization, limiting programmers to “read-only” access after production and restricting user access based on job responsibilities. Failure to enforce these controls creates risks of unauthorized access and insider threats, which are significant in cybercrime cases.

Digital forensics has grown in importance in situations where digital devices are used in crimes. Initially focused on computers, the field now includes various digital devices capable of storing and processing information. DFIs link digital evidence to establish factual information for judicial review, requiring adherence to principles such as auditability, repeatability, reproducibility, and justifiability to ensure credibility.

The implementation of DFIs emphasizes methodical processes for identifying, isolating, and analyzing evidence. By addressing systemic gaps in information security and applying robust forensic principles, organizations can strengthen their ability to combat cybercrime effectively, aligning investigative processes with evolving technological and legal landscapes. [2]

The prevalence of cybercrime has surged in recent years, posing significant challenges to individuals, organizations, and governments. Cybercriminals exploit vulnerabilities in information systems, leveraging advanced technologies to steal sensitive data, disrupt operations, or perpetrate fraud [3]. As digital devices increasingly become central to both personal and professional activities, they also serve as instruments and repositories of evidence in cybercrimes. Addressing these threats necessitates robust digital forensic investigations (DFIs) [4].

Digital forensics is a specialized field focused on identifying, preserving, analyzing, and presenting digital evidence in a manner that is admissible in court [5]. It plays a pivotal role in uncovering the "how," "why," and "who" behind cybercrimes [6]. While DFIs are critical for combating cybercrime, their effective implementation is often hindered by organizational, legal, and technical challenges [7]. Weak information security practices, unauthorized access to critical systems, and the rapid evolution of cyber threats further exacerbate the situation [8].

This paper explores the implementation of DFIs in addressing cybercrime, highlighting key challenges and strategies to enhance their effectiveness. By examining existing practices and emerging methodologies, the paper aims to provide actionable insights for strengthening forensic processes and improving cybercrime investigations.

2 LITERATURE REVIEW

2.1 Overview of Cybercrime and the Need for Digital Forensics

The prevalence of cybercrime has surged over the last decade, driven by increased digitalization across personal, organizational, and governmental domains [8]. Cybercriminals exploit weaknesses in information systems to steal sensitive data, disrupt operations, and commit fraud, often using sophisticated methods like phishing, ransomware, and hacking [9]. According to the 2023 Global Threat Report, cybercrime incidents have become increasingly complex, involving large-scale data breaches, advanced persistent threats (APTs), and malicious software targeting critical infrastructure [10]. As digital devices such as smartphones, computers, and cloud systems increasingly serve as instruments of both crime and evidence repositories, the need for robust Digital Forensic Investigations (DFI) has never been greater.

DFI is crucial in addressing the challenges posed by cybercrime. It is the process of identifying, collecting, preserving, analyzing, and presenting digital evidence that can be used in legal contexts [11]. DFIs aim to uncover the "how," "why," and "who" behind cybercriminal activities. However, as cybercrime evolves, digital forensics faces unique challenges that hinder effective implementation.

2.2 The Role of Digital Forensics in Combating Cybercrime

Digital forensics plays an integral role in uncovering the perpetrators and mechanisms behind cybercrimes. Unlike traditional criminal investigations, which primarily rely on physical evidence, DFI focuses on the examination of electronic data to reconstruct events, identify sources of attacks, and attribute blame [9]. This can include activities such as recovering deleted files, analyzing metadata, and tracing digital footprints across networks.

A significant aspect of DFI is its importance in maintaining the integrity and admissibility of digital evidence in court. The legal process requires evidence that is not only relevant but also collected, preserved, and analyzed in a manner that adheres to established forensic procedures [10,11]. Given the widespread use of encrypted and anonymized communication tools, DFI techniques have had to evolve to handle new forms of evidence, such as encrypted files, anonymized network traffic, and data stored in cloud environments. As cybercriminals increasingly rely on technologies like Tor, VPNs, and end-to-end encryption, forensic investigators face difficulties in tracing the origin of cybercrimes or accessing critical evidence. To address this, digital forensics has incorporated advanced decryption techniques, network traffic analysis, and the use of specialized software to identify hidden data [12].

3 METHODOLOGY

The implementation of Digital Forensic Investigations (DFIs) follows a structured process to ensure the integrity and admissibility of digital evidence. The investigation begins with the identification of potential evidence sources, such as compromised systems or devices. Once identified, preservation techniques are applied, including creating forensic images of storage devices to avoid data alteration. Collection of digital evidence follows, with particular attention to legal constraints around data privacy and jurisdiction. Investigators then move to examination, where tools like FTK Imager and X1 Search are used to recover deleted or hidden files, followed by analysis to reconstruct events and identify perpetrators. Finally, the findings are presented in a clear report for legal proceedings, maintaining compliance with legal standards to ensure the evidence's admissibility in court. Techniques such as network traffic analysis, mobile forensics, and cloud forensics are employed to handle modern challenges like encrypted communications and decentralized data storage [8,9,14].

The tools used in DFIs include forensic imaging software like EnCase, data recovery tools such as R-Studio, and network forensic tools like Wireshark for analyzing suspicious activity. Specialized tools for mobile and cloud forensics, like Cellebrite UFED and Elcomsoft Cloud Explorer, are crucial as mobile devices and cloud-based storage become common targets in cybercrime. Moreover, encryption-breaking tools such as Passware assist in accessing protected data, while legal documentation tools ensure chain of custody and evidence integrity [12,16]. A hypothetical case study illustrates this methodology: in a corporate data breach, investigators identify and preserve compromised systems, recover data using forensic tools, analyze logs and evidence to pinpoint a cybercriminal group, and present their findings to support legal actions. This approach ensures a comprehensive, legally compliant, and technically proficient investigation into cybercrime [13,15].

4 RESULT & DISCUSSION

4.1 Result

Digital forensic investigation is the process of identifying, collecting, analyzing, and preserving digital evidence from electronic devices to address criminal activities, security breaches, or other incidents involving digital data. This process

integrates technical expertise with legal standards to ensure that evidence is both reliable and admissible in court. The main objectives include safeguarding evidence, analyzing data from devices like computers, mobile phones, cloud systems, and networks, and reconstructing events to establish timelines that support legal cases.

The strategic role of digital forensics lies in its ability to ensure the integrity and admissibility of evidence in court by following international standards like ISO 27037:2012. These standards guide the processes of identifying, collecting, preserving, and analyzing digital evidence, strengthening legal cases against cybercriminals while maintaining the credibility of investigations. Digital forensics also helps reconstruct cybercrime events by analyzing digital traces such as log files, metadata, and encrypted data, allowing investigators to understand attack methods and identify those responsible.

Digital forensics contributes to improving security by identifying vulnerabilities exploited by attackers. For example, forensic techniques like log analysis and triage forensics can pinpoint weaknesses in cloud-based systems, helping organizations enhance their defenses. It also plays a vital role in tackling cybercrime across borders by adopting standardized frameworks like the Integrated Digital Forensic Process Model (IDFPM), ensuring consistent evidence handling and effective collaboration between law enforcement agencies worldwide.

With the rapid evolution of technology, digital forensics is key to addressing new threats like encrypted communications, IoT devices, and distributed networks. Advancements in tools and methodologies, such as artificial intelligence and machine learning, allow digital forensics to counter sophisticated tactics used by cybercriminals. This ability to adapt makes digital forensics essential for not only solving cybercrimes but also securing digital systems and preventing future attacks.

One of the key branches of digital forensics is cloud forensics, which focuses on collecting and analyzing evidence from cloud environments. This area addresses unique challenges such as the distributed nature of cloud data storage, shared resources in multi-tenant infrastructures, and jurisdictional complexities due to data being stored in different regions. Additionally, it ensures that evidence complies with legal standards and privacy regulations, making it admissible in court. Other branches include computer forensics, mobile forensics, network forensics, IoT forensics, and database forensics, each specialized for different digital environments[18].

Digital forensics plays a crucial role in addressing cybercrime by ensuring digital evidence is identified and processed in a way that maintains its integrity. For example, the ISO 27037:2012 framework offers guidelines for the stages of identification, collection, acquisition, and preservation of digital evidence, which are essential for its legal use. By analyzing digital traces and data left by perpetrators, investigators can reconstruct cybercrime events, identify attack methods, and trace the actors behind them. In cloud forensics, challenges like distributed data are addressed through techniques such as log analysis and forensic triage, which help investigators understand attacks and prevent future incidents[18].

Another important function of digital forensics is supporting legal proceedings. The results of digital forensic investigations are often compiled into technical and evaluative reports that adhere to legal standards, ensuring the validity of evidence presented in court. Frameworks like the Integrated Digital Forensic Process Model (IDFPM) help structure investigations to guarantee that evidence is relevant, reliable, and admissible. Through systematic procedures, digital forensic investigations ensure that cybercriminals can be identified and prosecuted, and that justice is served in increasingly complex digital environments[19].

4.2 Discussion

Digital Forensic Investigation detects cybercrime through systematic processes that adhere to established frameworks and standards, such as ISO 27037:2012 [18]. The process begins with the identification of potential sources of digital evidence, such as computers, mobile devices, cloud systems, or IoT devices, with a focus on prioritizing relevant and volatile data that may be lost if not promptly collected. Securing the crime scene is the next critical step[19], involving isolation, access control, and maintaining a chain of custody to ensure the evidence remains uncontaminated. Once secured, evidence is collected and acquired using appropriate techniques, such as live acquisition for volatile data or static acquisition for non-volatile data, while adhering to forensic standards to preserve authenticity [18,19]. The collected evidence is then analyzed to detect patterns, identify malicious activities, and reconstruct cybercrime events by examining logs, metadata, network traffic, and file structures. In cloud forensics, specific challenges such as distributed data and multi-tenant environments are addressed through methods like log analysis and forensic triage, enabling investigators to identify attack methods and actors involved. The analysis results are used to reconstruct the sequence of events leading to the cybercrime, linking evidence to specific actions or individuals. Finally, the findings are compiled into detailed reports adhering to legal and technical standards, providing reliable evidence for legal proceedings and the prosecution of cybercriminals. This structured approach ensures the integrity, reliability, and legal admissibility of evidence, making digital forensic investigation a crucial tool in combating cybercrime.

The digital forensic process involves four critical stages: identification, preservation, analysis, and presentation. In the identification phase, investigators pinpoint relevant digital artifacts like system logs, communication records, or malware traces. The preservation stage ensures that digital evidence remains unaltered during the investigation. This involves creating forensic copies of storage devices or systems, often using write-blocking tools. During the analysis phase, the evidence is meticulously examined using specialized software to uncover activities like unauthorized access or data breaches. Finally, the presentation stage organizes findings into a clear and admissible format for use in legal proceedings [21,24].

The effectiveness of digital forensic investigations hinges on the adoption of robust frameworks and tools. Widely recognized methodologies include the Systematic Digital Forensic Investigation Model (SDFIM), which emphasizes a step-by-step approach to preserving evidence integrity. Another effective framework is the Wycliffe Comprehensive Digital Forensic Investigation Framework (WCDFIF), which adheres to international standards like ISO/IEC 27043:2015 for consistent handling of digital evidence. Emerging models like the Cyber Forensics Model in Digital Ecosystems (CFMDE) address modern challenges posed by interconnected systems and anti-forensic tactics. These frameworks guide investigators in adapting to sophisticated and rapidly evolving cyber threats [21,24].

Digital forensic investigations bring several advantages. First, they enhance the ability to detect and address cybercrimes by uncovering hidden digital traces, even from encrypted or deleted files. Second, the process ensures legal compliance, making evidence admissible in court by following stringent protocols for data integrity. Third, they improve organizational resilience by identifying vulnerabilities exploited in attacks, thus guiding the development of stronger security measures. Finally, they facilitate international collaboration in tackling cybercrime, which is often a transnational issue, by providing standardized frameworks and methodologies [22,24]. Despite its effectiveness, digital forensic investigations face several challenges. The complexity of modern technology, such as the rise of IoT devices, cloud systems, and encrypted communications, makes evidence extraction more difficult. Cybercriminals also employ anti-forensic techniques to erase or manipulate digital traces, complicating investigations. Resource constraints, including the high cost of forensic tools and the need for skilled professionals, further limit the capability of law enforcement and organizations. Moreover, cross-border investigations face legal and ethical challenges, such as conflicts with sovereignty laws and potential breaches of privacy [22,24].

The constantly evolving landscape of cybercrime necessitates that digital forensic methods stay ahead of criminal tactics. For instance, investigators must now deal with advanced encryption, distributed networks, and anonymizing tools like Tor or VPNs, which criminals use to hide their identities. Regular updates to forensic tools and methodologies are essential to keep pace with these developments. The integration of artificial intelligence (AI) and machine learning in digital forensics has proven promising, allowing for faster detection and analysis of anomalies in massive datasets [24].

To enhance the effectiveness of digital forensic investigations, international collaboration is vital. Organizations such as Interpol and Europol, alongside global cyber task forces, work to share intelligence and best practices. Adopting international standards like ISO/IEC 27037, which guides evidence handling and preservation, ensures uniformity in procedures across borders. Collaborative efforts also help in developing universal frameworks to address jurisdictional challenges and streamline evidence collection in transnational cases [22,24].

Digital forensic investigation is indispensable in combating cybercrime, ensuring justice, and safeguarding digital ecosystems. Frameworks like SDFIM and CFMDE offer structured methodologies to detect and prosecute cybercriminals effectively. However, the process is not without challenges, including technological complexity, resource constraints, and legal ambiguities. Addressing these requires ongoing investment in tools, training, and international collaboration. As the cyber threat landscape continues to evolve, the field of digital forensics must advance in tandem, leveraging innovations in AI, big data analytics, and blockchain to secure the digital future [20,25].

5 CONCLUSION

Digital Forensic Investigations (DFIs) play a central and irreplaceable role in combating cybercrime by providing systematic and methodological processes for identifying, collecting, preserving, analyzing, and presenting digital evidence. As cybercrimes continue to increase in complexity and frequency, particularly with the rise of sophisticated threats such as hacking, ransomware, identity theft, and data breaches, the need for effective digital forensic investigations has become more crucial than ever. Digital forensic investigations are not only essential for identifying the perpetrators of cybercrimes but also for reconstructing events and understanding the methods used by cybercriminals, providing critical insight for both prevention and prosecution. The integration of technical expertise with legal standards is fundamental in ensuring the credibility, reliability, and admissibility of digital evidence in court, a key element in securing justice for victims and holding perpetrators accountable.

DFIs have evolved significantly from their early focus on computer forensics to encompass a wide array of digital environments, including mobile forensics, cloud forensics, network forensics, and IoT forensics. This expansion has come as a response to the rapid advancement in digital technologies, with devices like smartphones, cloud systems, and IoT devices becoming integral to both personal and professional activities, as well as crucial sources of evidence in cybercrime investigations. Cloud forensics, in particular, has gained prominence due to the unique challenges presented by the distributed nature of cloud data storage, multi-tenant infrastructures, and complex jurisdictional issues arising from the global nature of cloud services. As more data is stored and processed in the cloud, forensic investigators must navigate these challenges to ensure the preservation and integrity of evidence while maintaining compliance with privacy and legal regulations.

A key strategic function of digital forensics lies in its ability to ensure the integrity and admissibility of evidence, which is critical in the legal context. By adhering to established international standards, such as ISO 27037:2012 and ISO/IEC 27043:2015, digital forensics ensures that evidence is collected, preserved, and analyzed in a manner that adheres to legal procedures, making it admissible in court. This adherence to standards helps strengthen legal cases against cybercriminals, supports the prosecution of offenders, and provides assurance that investigations are conducted in a transparent, repeatable, and reproducible manner. The process of digital forensics goes beyond merely uncovering the

"who" and the "how" of a crime; it also reconstructs events, identifies attack methods, and helps prevent similar incidents in the future. These investigative processes are essential for understanding the full scope of a cyberattack, tracking its origin, and identifying any vulnerabilities that may have been exploited.

The successful implementation of DFIs is not without challenges,. The rapid evolution of cybercrime tactics, including the use of encryption, anonymizing tools like Tor and VPNs, and the exploitation of cloud environments, has made digital forensic investigations more complex. Cybercriminals often employ anti-forensic techniques to erase or manipulate digital traces, further complicating investigations. These include methods such as data wiping, steganography, and the use of advanced encryption techniques to conceal evidence. This has necessitated the development of new forensic tools and methodologies to address emerging challenges. The integration of artificial intelligence (AI) and machine learning (ML) into digital forensics has proven to be a promising solution, as these technologies allow investigators to analyze large datasets quickly, identify anomalies, and uncover hidden evidence. AI and ML can also aid in decrypting files, analyzing network traffic, and automating repetitive forensic tasks, making investigations more efficient and effective.

Despite the effectiveness of digital forensics, resource constraints remain a significant challenge. The high cost of forensic tools, the need for skilled professionals, and the complex nature of cybercrime investigations often limit the capacity of law enforcement and organizations to conduct thorough investigations. Moreover, cross-border investigations are complicated by legal and ethical challenges, particularly when it comes to data privacy, jurisdictional issues, and the differences in laws governing digital evidence across countries. International collaboration is crucial in overcoming these barriers. The adoption of standardized frameworks and best practices, such as those outlined in the Integrated Digital Forensic Process Model (IDFPM), helps ensure that evidence is handled consistently and securely across borders, allowing for more effective collaboration between global law enforcement agencies and organizations.

Digital forensic investigations also play an essential role in improving organizational resilience by identifying vulnerabilities in systems and guiding the development of stronger security measures. By analyzing the methods used in cybercrimes, investigators can provide organizations with insights into potential weaknesses in their digital infrastructure and recommend improvements. This proactive approach helps prevent future attacks and strengthens cybersecurity frameworks, making organizations more resilient to evolving cyber threats. Furthermore, digital forensics enables organizations to recover from cyberattacks more effectively by providing them with a clear understanding of what happened, how the attack was carried out, and what data was compromised.

As cybercrime continues to pose a significant threat to individuals, organizations, and governments, digital forensic investigations will remain an indispensable tool in ensuring the security of digital ecosystems and upholding the rule of law. The field of digital forensics must continue to evolve, leveraging new technologies and methodologies to stay ahead of cybercriminals and adapt to the ever-changing landscape of cybercrime. Continuous investment in training, tools, and international collaboration is vital to maintaining the effectiveness of digital forensics in addressing the increasingly sophisticated cyber threats of the future. By keeping pace with technological advancements and expanding its scope to address emerging challenges, digital forensics will remain a crucial component in the fight against cybercrime, ensuring justice and safeguarding digital assets for individuals and organizations alike.

Digital Forensic Investigations are not only essential for solving cybercrimes but also for preventing them in the future. The integration of artificial intelligence, machine learning, and blockchain technology into digital forensics provides investigators with the tools they need to address the growing complexity of cybercrime. By improving security measures, strengthening legal proceedings, and enabling international collaboration, digital forensics plays a pivotal role in securing the digital world. As the threat landscape continues to evolve, it is crucial that digital forensic methodologies continue to adapt, ensuring that they remain a powerful and effective tool for combating cybercrime and protecting the integrity of digital systems worldwide.

CONFLICT OF INTEREST

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Sihombing, E, Erlina, Rujiman. The effect of forensic accounting, training, experience, work load and professional skeptic on auditors ability to detect of fraud. International Journal of Scientific and Technology Research, 2019, 8(8): 474-480. https://www.ijstr.org/paper-references.php?ref=IJSTR-0819-20847

[2] Montasari, R. Review and Assessment of the Existing Digital Forensic Investigation Process Models. Int. J. Comput. Appl., 2016, 147(7): 1-9.

[3] Cohen, F. Digital forensic evidence examination. Fred Cohen & Associates, 2010.

[4] Kohn, M, Eloff, J H P, Olivier, M S. Framework for a digital forensic investigation. Proceedings of Information Security South Africa (ISSA), Johannesburg, South Africa. 2006.

[5] Carrier, B. File system forensic analysis. Addison-Wesley. 2005.

[6] Casey, E. Digital evidence and computer crime: Forensic science, computers and the Internet. Academic Press. 2011.

[7] Garfinkel, S L. Digital forensics research: The next 10 years. Digital Investigation, 2010, 7(1): S64-S73. DOI: https://doi.org/10.1016/j.diin.2010.05.009.

[8] Lillis, D, Becker, B, O'Sullivan, T, et al. Current challenges and future research areas for digital forensic investigation. Annual ADFSL Conference on Digital Forensics, Security and Law, 2016.
[9] Abdullah, I, Lubis, A W, Sumitra, A. Explanation of Forensic Accounting and Its Application (Case Some Industry Sector). Journal of Pharmaceutical Negative Results, 2022, 13(9): 1585-1588. DOI: https://doi.org/10.47750/pnr.2022.13.S09.195
[10] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.
[11] Fry, J. Digital forensics: An integrated approach. Wiley. 2019.
[12] Kessler, G C. An overview of digital forensics. International Journal of Digital Crime and Forensics, 2012, 4(2): 1-19. DOI: https://doi.org/10.4018/jdcf.2012040101.
[13] Mell, P M, Grance, T. The NIST definition of cloud computing. National Institute of Standards and Technology Special Publication, 2020, 800-145. DOI: https://doi.org/10.6028/NIST.SP.800-145.
[14] Raghavan, S, Kessler, G C. Emerging challenges in digital forensics: Tools and techniques for encrypted and anonymized data analysis. Wiley. 2021.
[15] Braakman, J, de Vries, P. Digital forensics and the law: An introduction. Springer. 2013.
[16] Jansen, W, Ayers, R. Guidelines on cell phone forensics. National Institute of Standards and Technology Special Publication, 2007, 800-101. DOI: https://doi.org/10.6028/NIST.SP.800-101.
[17] Lindsay, B R. Cybercrime and international law: Strengthening the global legal framework. Oxford University Press. 2020.
[18] Soghoian, C. Cloud computing and the challenges of data privacy and cross-border data transfer. Journal of International Commercial Law and Technology, 2013, 8(3): 187-201.
[19] Alshabibi, M M, Budookhi, A K, Hafizur Rahman, M M. Forensic investigation, challenges, and issues of Cloud Data: A systematic literature review. Computers, 2024, 13(8): 213.
[20] Graeme Horsman. The different types of reports produced in Digital Forensic Investigations. Science & Justice. 2021. https://www.sciencedirect.com/science/article/abs/pii/S1355030621000927
[21] Didik, S, Yudi, P, Bambang, S. Analysis and evaluation digital forensic investigation framework using ISO 27037: 2012. International Journal of Cyber-Security and Digital Forensics, 2019, 8(1): 1-14.
[22] Chen, C, Dong, B. Digital forensics analysis based on cybercrime and the study of the rule of law in space governance. De Gruyter. 2023. https://www.degruyter.com/document/doi/10.1515/comp-2022-0266/html
[23] Mwatu, W. Digital Forensics Framework For Combating Cyber-crime. Doctoral dissertation, KCA University. 2022.
[24] Oerlemans, J J. Investigating cybercrime. Investigating cybercrime | Scholarly Publications, 2017. https://scholarlypublications.universiteitleiden.nl/handle/1887/44879
[25] Sikos, L F. AI in digital forensics: Ontology Engineering for Cybercrime Investigations. WIREs Forensic Science, 2020, 3(3). DOI: https://doi.org/10.1002/wfs2.1394.
[26] Sabillon, R, Serra-Ruiz, J, Cavaller, V, et al. Digital Forensic Analysis of Cybercrimes. International Journal of Information Security and Privacy, 2017, 11(2): 25-37. DOI: https://doi.org/10.4018/ijisp.2017040103.