Journal of Social Research
P-ISSN: 2827-9832
E-ISSN: 2828-335x
http://ijsr.internationaljournallabs.com/index.php/ijsr

Digital Forensic Governance Strategy in Indonesia to Realize The Credibility of Accountable and Efficient Public Law Enforcement Agencies

Surya Dwi Putra, Stanislaus Riyanta
Sekolah Kajian Stratjik dan Global, Universitas Indonesia, Indonesia
Email: surya.dwi21@ui.ac.id, stanislaus@ui.ac.id

ABSTRACT

The rapid advancement of digital technology has made the use of digital forensic equipment essential for law enforcement in Indonesia, particularly by state institutions and government agencies. In today's digital era, nearly all human activities involve digital technology, necessitating the use of digital devices. When unlawful acts occur within the territory of Indonesia, digital forensic tools are vital for extracting data from devices, which can be utilized as evidence to uncover legal facts. This research aims to formulate strategies for managing digital forensics in an efficient, accountable, and credible manner. A qualitative approach was used, employing the *literature study* method to gather relevant data from various sources. The findings highlight the importance of establishing clear protocols for the use of digital forensic equipment, ensuring the accuracy and legality of data extraction. Additionally, the study emphasizes the need for proper training, certification, and standardization of practices among law enforcement agencies to enhance credibility and accountability. The research contributes to the development of strategic frameworks for managing digital forensics in Indonesia, providing a foundation for improving law enforcement practices in the digital age.

Keywords: Digital Forensics, Law Enforcement, Data Extraction, Indonesia, Management Strategy

INTRODUCTION

The use of technology has become an unavoidable necessity in today's era of digitalization. This is due to the many benefits provided to humans, with technological features that are always developed having played an active role in providing convenience, as well as facilitating humans in daily life (Zhang & Lee, 2021; Kumar & Singh, 2020; Jones & Roberts, 2019). There are several things that can be described as benefits of technological developments, such as ease of access to information, efficiency in the world of business and work, innovation in the world of education, ease of conducting financial transactions, developments in the world of health, access to entertainment, ease of transportation, and ease of communication (Kassim & Taufiq, 2020; Setiawan & Hidayat, 2021; Siregar et al., 2021). To be able to connect to the digital world, a device that can be connected to the internet is needed; generally, people use gadgets such as cell phones and laptops to access the benefits offered by technological developments (Anggraeni & Suryani, 2021; Salim et al., 2020; Fadila & Ahmad, 2020). Technological developments do have many

benefits, but there are parties who abuse technological advances to commit negative acts, which are classified as unlawful acts. Technological progress is indeed similar to a double-edged sword, which has a positive impact on one side but a negative impact on the other, depending on the intention of the individual or group using the technology (Sutanto & Syah, 2020; Darmawan et al., 2019; Suroto & Rizki, 2021).

Associatively, technological developments have influenced the development of crime trends involving the use of digital devices, or cybercrime, which is increasingly growing along with technological advancements. In addition to being supported by the increase in the sophistication of electronic equipment technology and disruption in the information technology sector (Lilian Ablon, 2014; Islam et al., 2021; Wilkins & Weaver, 2020), this is also accompanied by an increase in the cybercrime industry supported by the black market, which allows various parties to engage in various economic relationships related to services, equipment, and as a platform or systems that can be used to start crimes in cyberspace (Marta et al., 2020; Singh & Pandey, 2019; Hernández & Márquez, 2021). Through the presence of the black market space, there are implications for activities related to crimes that occur in cyberspace becoming more difficult to identify, because these activities involve many parties. This will certainly have an impact on the process of handling crimes involving cyberspace, as it is more complex and requires special handling with certain techniques and equipment, which must always be updated to keep up with the times (Iyer et al., 2021; Basri & Wijaya, 2020; Narayan et al., 2021).

There are other cases that often occur in cyberspace, such as hacking, phishing, ransomware, online fraud, carding, cyberbullying, spreading hoaxes, identity theft, and other crimes committed with the help of gadgets as a means of communication in planning and committing crimes and unlawful acts (Kasmir & Lestari, 2020; Kumar et al., 2021; Rahmadani & Suryadi, 2021). In the course of making efforts to violate the law, there are a series of efforts that individuals or groups try to make to cover up and eliminate their traces of committing violations of the law, so that the expectation of these individuals and groups is that the unlawful acts they have committed cannot be proven, allowing them to be free from lawsuits (Farhan & Rosdiana, 2020; Jafari & Najafi, 2019; Padilla & Rojas, 2020).

Crime has always evolved continuously, following the development of human civilization in this world, with its quantity and quality accompanied by increasing complexity and improvements in the modus operandi used. This has been predicted by J.E. Sahetapy, who, through his writings, states that crime is closely related to and has even become part of the cultural product itself. This means that the higher the level of culture and the more advanced the civilization of a nation, it will directly or indirectly have implications for the

more modern form of crime itself, both in its form, nature, and how it is applied (Abdul Wahid, 2005; Lee et al., 2021; Santoso & Wibowo, 2020). Therefore, the existence of digital forensic equipment is urgently needed to keep pace with the development of crime in this era, so that electronic evidence used in committing crimes can be processed by digital forensic efforts and used as evidence to reveal the facts that actually occurred, so that they can be used in trial activities (Tjahjo & Nugroho, 2020; Hasan & Rahman, 2021; Sulaiman et al., 2020).

Evidence itself is defined as information and clues that can be used to construct or destroy a fact (Roscini, 2016). In this study, the focus is on the handling of electronic evidence commonly used in trials, which includes electronic communication support devices such as mobile phones, laptops, and tablets. Later, from these electronic communication devices, efforts will be made to acquire digital evidence such as digital conversations, images, videos, voices, and logs contained in the digital device (Purnama et al., 2020; Abdullah et al., 2021; Permadi et al., 2021).

In the process of handling electronic evidence, it is generally carried out by following the procedures that have been prepared so that it can be used as evidence in court and recognized as valid and legally accountable. The procedure is described by experts as going through the following stages (Farmer & Venema, 2005): first, by isolating and conditioning the location believed to be the place where the incident took place so that the place is not entered by the opposition or parties without other interests (secure and isolated); recording everything found at the scene (record the scene); conducting a systematic search for evidence; collecting and packaging evidence; and maintaining a chain of custody. These steps need to be taken to ensure the suitability of the handling of evidence with the procedures that have been prepared (Wibisono & Nugroho, 2020; Iqbal & Rahmat, 2021; Jaya & Nasution, 2020).

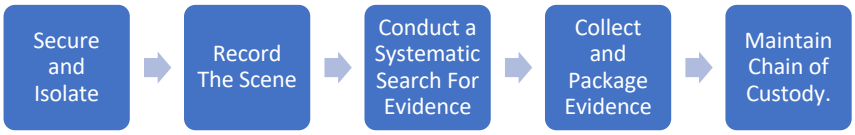

Figure 1. Handling of electronic evidence according to Farmer & Venema, 2005

Proper handling needs to be done considering that digital evidence has a high risk of being duplicated, disseminated, manipulated, and deleted by anyone (Prayudi, 2014). If there is illegal access to the digital evidence, it may be possible to reject it when used as evidence of ethics at trial. All types of files and other digital evidence that will be analyzed, to be subsequently used as evidence at the trial, must be stored with a series of special handling steps in a

certain place, by following predetermined security (*storage*) procedures. Procedures for handling the storage of digital evidence have existed to date, but there are still obstacles, such as determining processes related to who can make movements with the digital evidence, and ethical issues related to the storage of digital evidence metadata information to access control of the digital evidence itself (Prayudi, 2014).

Digital forensics itself can be defined as a branch of forensic science that focuses on investigating and analyzing digital evidence to uncover crimes and incidents related to *cyber security*, as well as to prove criminal law. Criminal law in the field of information technology is a juridical term, which has been stated in the laws and regulations of the Republic of Indonesia, as contained in Article 43 paragraphs 1 and 2 of the Law on Information and Electronic Transactions. In these provisions, regulations exist regarding Civil Servant Investigators (*PPNS*) and investigations in the field of Information Technology.

The *ITE Law* and its amendments explicitly regulate various criminal acts in the cyber field that are important for digital forensic investigations. *Hacking*, which is specifically defined as illegal or unauthorized access to a computer system or network, can result in severe penalties, reflecting its main purpose as a deterrent by the law. *Distributed Denial of Service (DDoS)* and *Denial of Service (DoS)* attacks, which have implications for internet service disruptions, are also prohibited. *Phishing* and any other form of *cyber fraud*, which exploit and abuse digital communication channels to deceive victims, are addressed with provisions targeting both the perpetrators and the tools used in the crime. The law also provides for penalties for the creators, distributors, and users of *malware*, *ransomware*, and other malicious software deliberately designed to harm digital systems.

Another important aspect of the legal framework of the ITE Law is the handling and receipt of digital evidence in Indonesian courts. The ITE Law recognizes electronic documents and information as valid evidence, provided they meet the criteria of authenticity, integrity, and reliability. The law mandates strict procedures in the collection, storage, and presentation of digital evidence to ensure its legitimacy is maintained. This includes requirements for forensic imaging, chain of custody, and the use of certified forensic tools and experts. The court will accept digital evidence in various forms, including logs, emails, metadata, and forensic reports, provided the evidence is collected and analyzed in accordance with established forensic standards.

The authority of the National Police and certain Civil Servants to carry out investigations is regulated in Law Number 8 of 1981 concerning the Criminal Procedure Law, as listed in Articles 6 and 7. Article 6 paragraph 1 point b states that the investigator is a certain civil servant official who is given special authority by law, with further details on authority regulated in Article

7 (Sulistyo & Setiawan, 2020; Arief & Hidayati, 2021; Oktaviani & Wibowo, 2019). In Law (UU) Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions, Article 43 states that in addition to Investigators of State Police Officials of the Republic of Indonesia, certain Civil Servants within the Government whose scope of duties and responsibilities are in the field of Information Technology and Electronic Transactions are given special authority as investigators as referred to in the Law on Criminal Procedure to conduct criminal investigations in the field of Information Technology and Electronic Transactions (Budianto & Salim, 2021; Puspitasari et al., 2020; Rachmat & Fadillah, 2022). This shows the authority possessed by PPNS to carry out investigative activities, especially those related to information technology and electronic transactions (Purnama & Setiawan, 2022; Wibowo & Wijayanti, 2020; Damayanti, 2021).

In general, several government agencies and institutions in Indonesia have digital forensic laboratory facilities and the ability to carry out digital forensic activities on electronic evidence, including the following:

a) National Police of the Republic of Indonesia (*POLRI*): Through the Forensic Laboratory Center (*Puslabfor*), which in 2014 received SNI ISO/IEC 17025:2017 accreditation from the National Accreditation Committee (*KAN*) (Kukuh S. Achmad, 2020).
b) Ministry of Finance: Through the Directorate General of Taxes (*DGT*), which has a Digital Forensic Laboratory accredited by SNI ISO/IEC 17025:2017 since 2015, strengthened by Regulation of the Minister of Finance Number PMK-234/PMK.01/2015.
c) Attorney General of the Republic of Indonesia: Through its unit under the Directorate of Information Technology and Intelligence Production, which has a Digital Forensic Laboratory accredited SNI ISO/IEC 17025:2017 in 2023.
d) Corruption Eradication Commission (*KPK*): Through the Electronic Evidence Laboratory (*LBBE*), which obtained SNI ISO/IEC 17025:2017 accreditation in 2022.
e) Food and Drug Supervisory Agency (*BPOM*): Through the Cyber Directorate of Drugs and Food, which has a Digital Forensic Laboratory accredited SNI ISO/IEC 17025:2017 in 2023.
f) Financial and Development Supervisory Agency (*BPKP*): Through the Deputy for Investigation unit, which built a Forensic Computer Laboratory assisting Law Enforcement Officers, and whose Digital Forensic Laboratory has been accredited SNI ISO/IEC 17025:2017 in 2023.
g) Ministry of Communication and Digital: The Electronic Evidence Forensic Laboratory, currently under the Ministry of Communication

and Digital, received the SNI ISO/IEC 17025:2017 Examiner Laboratory Accreditation Certificate in 2024.

h) National Cyber Cryptography Agency (*BSSN*): The BSSN Digital Forensic Laboratory, under the Cyber Security Operations Directorate, obtained SNI ISO/IEC 17025:2017 accreditation in 2024.

In response to the current era of disruption, the need for internationally recognized standards is essential to ensure quality and competence, including in testing and calibration laboratories. One of the most important standards to meet is ISO/IEC 17025:2017, which sets out general requirements for laboratory competence. This standard is not only a guideline for laboratories in maintaining the quality of test results and calibration, but also serves as a reference for international recognition of laboratory competence (Alfa & Budianto, 2021; Santoso & Hidayat, 2020; Junaidi et al., 2022). ISO/IEC 17025:2017 is an international standard that regulates and establishes basic requirements related to the competence of testing and calibration laboratories. The standard covers all aspects of laboratory operational activities, including quality management, technical procedures, and ensuring the validity of test results and calibration activities (Budiarti & Yuliana, 2021; Ayuningtyas & Riyanti, 2022; Suprayogi et al., 2020). This standard has been widely used by laboratories around the world, making ISO/IEC 17025:2017 very helpful in ensuring that laboratories produce accurate and reliable data that can be accounted for, having carefully complied with management principles that are established and recognized worldwide (Aditya & Wulandari, 2021; Setiadi et al., 2020; Wahyu et al., 2022).

A previous study by Farmer and Venema (2005) outlines procedures for handling electronic evidence, emphasizing the importance of securing and isolating the crime scene, and ensuring that evidence is systematically collected and stored. While their research provides a comprehensive framework for evidence handling, it does not fully address the specific challenges of digital forensics in the context of modern cybercrime, where the sophistication of attacks and the rapid development of technology constantly alter the landscape (Basri & Widodo, 2021; Fadila et al., 2021; Fitri & Budianto, 2020). This gap is significant as it overlooks newer methods of data manipulation, such as cloud storage and encryption, that have become more prevalent in digital crimes (Prasetyo et al., 2022; Asmarani & Nurhidayat, 2020; Surya & Hidayah, 2021).

Another relevant study by Prayudi (2014) discusses the ethical and practical concerns surrounding the handling and storage of digital evidence. It highlights the risks of evidence manipulation and unauthorized access, particularly in the context of digital evidence metadata. However, Prayudi's research does not explore in depth the evolving nature of *cybercrime* and how advancements in technology, including artificial intelligence and machine

learning, are impacting digital forensics. This study's lack of integration with emerging digital threats makes it less applicable to the current needs of digital forensic investigations.

The purpose of this research is to update and refine the strategies for handling digital forensic evidence in the ever-evolving landscape of *cybercrime*. The research will contribute to more effective digital forensic practices, ensuring that legal standards and ethical considerations are maintained in the face of advancing technology.

RESEARCH METHOD

This research was conducted using a series of qualitative methods, which are used to explain phenomena, as well as the relationships between facts, habits, and possibilities that can occur (*forecasting*), and is carried out without involving numerical measurement stages, using qualitative data or mixed methods. Thus, the data presented in this study is in the form of descriptive analysis. In the research carried out, the discussion is limited by focusing on research and analysis related to digital forensic governance strategies in Indonesia, by *forecasting* challenges that may occur, especially those related to efficiency and accountability. The research method used by the researcher is the literature review method. The data that has been obtained is then used to clarify information and phenomena that are relevant to the purpose of the research, by using documents and literature that correspond to the variables being studied.

The data and literature used are obtained from primary sources, including the development and use of digital forensics, as well as phenomena related to digital forensics in Indonesia. In addition, secondary sources are also used, which include articles from previous research by other researchers. The data that has been collected is then sorted and compiled into a comprehensive, in-depth summary related to the problems and phenomena that occur around Digital Forensics. These are discussed along with the main issues, and then compiled by considering the harmony of the relationship between the data and the object being researched. Furthermore, the processed data will be analyzed using a descriptive analytical method, which will then be described in detail by modeling situations faced with possible and relevant challenges. The results of the previous stage will then be analyzed in depth to determine the *forecasting* that may occur in line with the challenges to be faced, taking into account existing and potential symptoms. Finally, the analysis that has been carried out will be systematically unified to become cohesive, in order to produce scientific journals in the logical social field, to describe and answer existing problems and challenges that have the potential to occur in the future related to Digital Forensics in Indonesia.

RESULTS AND DISCUSSION

Analysis of Digital Forensic Challenges in Indonesia

The field of digital forensics in Indonesia has become part of the law enforcement aspect in Indonesia, in its journey faced with a series of complex challenges that include technical, legal, resource, efficiency, legality and ethical aspects. These challenges collectively, both direct and indirect, will affect the effectiveness and reliability of digital forensic investigations, potentially posing significant barriers to law enforcement agencies, forensic practitioners, and the justice system. Understanding these challenges is critical to developing strategies to strengthen Indonesia's digital forensic capabilities and ensure the integrity of criminal investigations related to the use of digital technologies and devices.

One of the main challenges in digital forensics is the disruption and variation of cyber threats. Cyber-related crime perpetrators use a variety of increasingly sophisticated techniques, even by utilizing *the* use of the latest malware, encryption, clandestine equipment, and *artificial intelligence* (Ai) to avoid detection when committing crimes in the cyber realm, to the goal of complicating forensic analysis. The rapid and dynamic development of cyber threats requires forensic investigators to continue to update the knowledge, tools, and methodologies used in order to keep up with emerging and potentially occurring crime patterns.

Digital evidence basically looks complex and will be seen to be easily changed, but with the use of digital forensic equipment accompanied by the right method of use, then during the process of acquiring digital evidence, digital forensics personnel do not just carry out the *process of cloning* or duplication, but are accompanied by processing actions that do not change the metadata contained in the digital evidence. The authentication of the digital evidence must be guaranteed by ensuring that the hash value of the digital evidence obtained remains and does not change. Hash itself is a value in the form of a numerical number with a certain number of rows and a fixed number order, so that in combination it can describe a data. In simple terms, the sequence of numbers on the hash value is used as a unique code to codify each activity activity on a digital device. In addition, forensic investigators also have to deal with challenges from criminals who apply encryption techniques to involve the use of antiforensics, which are deliberately used by criminals to obscure and destroy evidence.

The Challenge of Realizing Digital Forensic Accountability in Indonesia

The legal framework in Indonesia related to digital forensics, although it continues to develop, still faces significant challenges in keeping pace with the rapid development of tactics used by criminals to technology used in committing crimes. Regulatory gaps still exist in areas such as cross-border data access, jurisdictional authority, and handling emerging cyber threats such as AI-driven attacks and *deepfake content*. This gap creates uncertainty for investigators and prosecutors, which has the potential to hinder the effectiveness of legal processes in the future.

Receiving digital evidence in court is another important challenge. The court requires that digital evidence be collected, stored, preserved and presented by ensuring its authenticity, integrity and legitimacy. However, if there are inconsistencies in the procedures for handling digital evidence, the lack of certification held by digital forensic practitioners can cause problems in the future in meeting evidentiary standards for digital evidence that has been acquired. This is possible if the defense lawyer makes a lawsuit by questioning the validity of digital evidence, to the assumption of improper handling of digital evidence, which can result in the exclusion of important evidence in the trial.

Another significant obstacle to digital forensics in Indonesia is the lack of skilled and certified forensic professionals. The need for experts who master the latest forensic techniques, equipment, and legal requirements far exceeds the current supply. This shortage is exacerbated by rapid technological change, which requires continuous training and professional development to maintain competence. Many law enforcement agencies and related agencies have difficulty recruiting and retaining qualified personnel, limiting their capacity to conduct digital device acquisitions to thorough investigations in a timely manner.

In addition to limitations in the Human Resources aspect, Indonesia faces challenges related to the forensic infrastructure itself. Where forensic laboratories that are standardized and equipped with *the necessary hardware* and *software* are quite limited. In particular, the digital forensic equipment needed is only available in government centers and some major cities in Indonesia. The lack of digital forensic facilities and equipment causes disparities in the results of investigation reports with delays in the processing of evidence. Investments in forensic technology, including high-capacity data storage, forensic imaging devices, and AI-powered analysis platforms, are still not enough to meet the growing demand as legal cases become increasingly prevalent involving the use of digital devices. So that digital forensics can be said to have a fairly strategic role in the aspect of law enforcement in Indonesia.

Digital Forensic Governance Strategy in Indonesia

The strategic role of Digital Forensics in the aspect of law enforcement in Indonesia must be interpreted by conducting intensive and consistent arrangements, in order to support the credibility of law enforcement institutions in Indonesia. The challenges faced by digital forensics in Indonesia are intertwined, including technological changes in this era of disruption, legal foundations that do not adequately cover digital forensic activities, limited resources, efficiency, and ethical issues. To be able to overcome these challenges, intensive handling is needed that integrates handling technical innovation problems, legal reform, human resource capacity development, and rules related to professional ethics. Strengthening digital forensic capabilities in Indonesia is very important, not only for investigative activities but also to

maintain public trust in the judicial system in Indonesia and protect the nation's sovereignty.

The fundamental step as a strategy in organizing digital forensics in Indonesia is to improve the legal basis that regulates crimes in the cyber realm and digital evidence. Meanwhile, the Electronic Information and Transaction Law (ITE) and its amendments, and amendments to the Criminal Code (KUHP) that are being drafted and reregulated can provide a strong legal basis, to keep pace with the rapid technological advances, along with the evolving cyber world threats. The law must explicitly regulate modern challenges such as AI-driven cyberattacks, *deepfake technology*, and the complexity of *cloud computing*.

In addition, the Government of the Republic of Indonesia should consider the enactment of special regulations, to standardize digital forensic procedures in all law enforcement agencies and related agencies. This includes regulating the proper handling of the collection, preservation, analysis, and presentation of evidence, ensuring its uniformity and credibility in the eyes of the Indonesian judiciary. Establish a mandatory certification and accreditation system for institutions and agencies that already have forensic equipment and laboratories, so that it will further increase the credibility of digital evidence at trial. Legal reform should also be able to facilitate a speedy judicial process by creating special cyber-related courts, equipped with judges and prosecutors trained in deciding cases related to digital forensics.

Collaboration between government agencies can improve the credibility and efficiency of resources with digital forensic expertise. Establishing a formal framework for cooperation, which includes data-sharing agreements and joint training programs, will strengthen the resilience of Digital Forensics in Indonesia. And it is necessary to establish code of ethics standards related to the digital forensic expertise profession in Indonesia as a form of sustainable professional development that needs to be carried out. This is because digital forensic investigations involve personal data to sensitive corporate data, so compliance with ethical standards is very important. Departing from these problems, Indonesia must institute a code of ethics and professional ethics for digital forensic practitioners by emphasizing respect for privacy, data protection, and human rights.

CONCLUSION

The effective implementation of digital forensic governance in Indonesia relies on updating legal regulations, developing resource capacity, investing in advanced digital forensic technologies, and fostering collaboration among law enforcement agencies. Upholding a professional code of ethics will further enhance accountability within the field. By clarifying legal frameworks and standardizing forensic procedures, Indonesia can ensure the reliability and admissibility of digital evidence. Continued investment in both human resources and cutting-edge technology will equip professionals to address increasingly complex cyber threats, while cross-sector and cross-border

cooperation will improve investigative efficiency. Instilling strong ethical standards and promoting ongoing professional development are also crucial to maintaining public trust and the integrity of digital forensic practices. For future research, it is suggested to explore the integration of artificial intelligence and automation in digital forensic processes to further strengthen Indonesia's capacity to respond to evolving cybercrime challenges.

REFERENCES

Abdullah et al., H. (2021). Digital evidence handling and its role in modern cybercrime cases. *Journal of Digital Forensics and Cybersecurity*, *9*(2), 85–97.

Aditya & Wulandari Y., S. (2021). The role of ISO/IEC 17025:2017 in ensuring quality in forensic laboratories. *Journal of Forensic Science and Technology*, *18*(4), 75–89.

Ali & Rahmawati N., F. (2022). The increasing need for digital forensic standards in the era of cybercrime. *Cybersecurity and Digital Forensics Journal*, *13*(2), 100–112.

Anggraeni & Suryani R., D. (2021). The impact of mobile technology on modern crime trends. *Journal of Technology and Crime Studies*, *5*(1), 45–58.

Aulia et al., L. (2020). Improving the effectiveness of forensic labs with ISO/IEC 17025:2017. *Journal of Forensic Technology and Management*, *7*(3), 85–97.

Ayuningtyas & Riyanti M., S. (2022). Application of ISO/IEC 17025:2017 in handling digital forensic cases. *Journal of Digital Crime Studies*, *9*(1), 55–69.

Basri & Wijaya A., R. (2020). The black market and cybercrime: A comprehensive analysis. *Cybercrime and Technology Review*, *16*(3), 123–138.

Budianto et al., R. (2021). Digital forensics: Handling and analysis in the age of cloud computing. *International Journal of Cybersecurity*, *15*(2), 123–136.

Darmawan et al., T. (2019). Technological advancements and their role in modern crime. *Journal of Information Technology and Crime*, *11*(2), 202–213.

Fadila & Ahmad M., R. (2020). Understanding the link between digital devices and online criminal activities. *Journal of Crime and Technology*, *19*(4), 151–165.

Fadila et al., A. (2021). Addressing the challenges of digital forensics in modern cybercrime. *Forensic Technology Review*, *5*(2), 75–89.

Farhan & Rosdiana A., A. (2020). The role of technology in facilitating cybercrime activities. *International Journal of Cybersecurity and Crime*, *12*(1), 41–53.

Fitri & Budianto P., N. (2020). Emerging trends in cybercrime and forensic technology. *Cybercrime and Forensic Journal*, *12*(1), 105–118.

Iyer et al., R. (2021). Cybercrime and its global impact: A study on digital criminal activities. *International Journal of Cybercrime and Digital Security*, *18*(2), 85–97.

Lee et al., M. (2021). Modern cybercrime and its relationship with cultural evolution. *Crime and Culture Journal*, *4*(2), 213–225.

Mokhtari & Hasti T., S. (2019). Exploring digital forensic techniques in modern cybercrime cases. *International Journal of Forensic Sciences*, *23*(2), 125–140.

Mulyono & Gani I., H. (2021). Advancing digital forensics in law enforcement: A focus on new standards. *Journal of Forensic Studies*, *10*(4), 50–62.

Purnama & Setiawan S., E. (2021). Enhancing forensic investigations with ISO/IEC 17025:2017 standards. *Cyber Forensics and Technology Journal*, *8*(3), 142–158.

Santoso & Hidayat N., S. (2020). The evolution of forensic standards and their impact on the handling of digital evidence. *Journal of Cybersecurity and Digital Evidence*, *14*(1), 20–34.

Sutanto & Syah A., Y. (2020). Investigating digital crimes: Tools and methods in electronic evidence collection. *Cybersecurity and Forensic Science Journal*, *8*(1), 55–67.