Exploring the Role of Digital Forensics in Identifying Cyber Crime in Indonesia’s Criminal Procedure Law

Cindy Monique
Faculty of Law, Universitas Brawijaya, Indonesia
email: cindymonique21@student.ub.ac.id

Yuliati
Faculty of Law, Universitas Brawijaya, Indonesia
email: yuliaticholil@ub.ac.id

Faizin Sulistio
Faculty of Law, Universitas Brawijaya, Indonesia
email: faizin@ub.ac.id

Abstract
Digital forensics is an indispensable component in the process of detecting and examining cybercrimes in accordance with the Criminal Procedure Law of Indonesia. This study investigates where digital forensics fits into Indonesia’s Criminal Procedure Law for cybercrime detection. As cybercrime rises, it’s important to understand how digital forensics can investigate and prosecute cybercrimes. This study examines Indonesian digital forensics law and practice using normative legal research. The author employs normative legal research procedures in this specific legal study. This study found that due to laws, Indonesia needs digital forensics to protect electronic evidence. Treat electronic evidence differently than physical. Indonesian courts’ use of digital forensics is valued since cybercriminals can tamper with electronic evidence. The processes manage cybercrime electronic evidence legally. Validation of criminal procedure. Criminal procedural laws must be enforced by police, prosecutors, legal experts, and judges. Police should standardize electronic evidence management with digital forensics. In wealthier nations like the US, digital forensics protects electronic evidence.

INTRODUCTION
In the rapidly advancing digital age, cybercrime poses a significant threat to societies worldwide, including Indonesia. Digital crimes such as hacking attacks, identity theft, online fraud, and other similar activities result in financial losses and erode public
confidence in online security. Cybercrime is a criminal act that occurs in the virtual world, without limitations of distance or time, and can be perpetrated by anyone, anywhere (Brown, 2015; Malik & Choudhury, 2019). The author argues that cybercrime is an extension of conventional criminal acts. This is due to the fact that the actions carried out by the perpetrators are considered criminal acts, which are typically covered by existing criminal laws. In Indonesia, crimes are regulated in Book II of Law Number 1 of 1946 concerning Criminal Law Regulations, commonly known as the Criminal Code (Rauzi et al., 2023). As an illustration, when fraud is committed in the virtual realm, it falls under the purview of Article 378. Consequently, conventional acts of fraud can be classified as cyber crimes. As per experts in cyber law, the various types of cyber crimes hold distinct interpretations (Chawki et al., 2015; Tsakalidis & Vergidis, 2017)

Proof is a crucial aspect of procedural law, particularly in cases involving cyber crime. In this context, the focus is on gathering and presenting evidence within the framework of criminal procedural law. Proof establishes the occurrence of a criminal act and the identification of the defendant, ultimately holding them accountable for their actions. In the realm of criminal procedural law, evidence refers to the methods and endeavors employed to gather information through legally admissible evidence, with the aim of establishing the veracity of the defendant's alleged criminal act (Rusli, 2007). The Criminal Procedure Code, specifically Article 184 Paragraph 1 of Law Number 8 of 1981, provides clear and valid evidence in criminal procedural law (Chen, 2016; Damanik et al., 2021).

a) Testimonies from witnesses;
b) Insights from experts;
c) Written correspondence;
d) Directions; and
e) Defendant’s declaration.

In this scenario, the question arises as to the precise location of electronic evidence inside the criminal evidence system, as outlined in the Criminal Procedure Code. Subsequently, the introduction of Law Number 11 of 2008, also known as the ITE Law, addressed this issue. This law was later modified by Law Number 19 of 2016, known as the ITE Amendment Law (El Asam & Samara, 2016; Iswari & Rudy, 2023). Article 5 of the ITE Amendment Law states:

a) Electronic information, electronic documents, and printouts are legally admissible as valid proof.
b) Electronic Information, Electronic Documents, and printouts, as defined in paragraph (1), are considered legitimate evidence under the current Procedural Law in Indonesia.
c) Electronic Information and/or Electronic Documents are deemed legally binding if the Electronic System is utilized in compliance with the regulations stipulated in this Law.
d) The regulations concerning Electronic Information and/or Electronic Documents, as mentioned in paragraph (1), are not applicable if they are already governed by the Law.

As to the author's statement, the inclusion of electronic evidence, such as information, electronic documents, and printed results, is an extension of the evidence outlined in the Criminal Procedure Code, serving as a reference for criminal procedural law in Indonesia. Electronic evidence, unlike conventional evidence, is intangible and stored in a data drive. It is susceptible to alteration or deletion, allowing cybercriminals to erase any traces of their actions. Consequently, electronic evidence necessitates exceptional handling, specifically through the application of digital forensic techniques.

In the field of criminal justice, judges frequently disregard electronic evidence because of doubts about its authenticity and integrity. Consequently, the role of digital forensics is to reconstruct electronic evidence and provide insight into cyber crimes. Consequently, the utilization of digital forensic technologies has emerged as a crucial approach for investigating and revealing instances of cyber crime in Indonesia. This text will examine the impact of digital forensic techniques on the verification of criminal procedural law in order to expose cybercrime in Indonesia.

The purpose of the study is to examine and analyse the significance of digital forensics within the framework of Indonesia’s legal system, particularly in the context of identifying and investigating cybercrimes.

METHOD
Normative legal research methodologies are utilized by the author in this particular piece of legal study. The investigation of applicable legal norms is the primary emphasis of normative legal research methods, which are a methodological approach in the field of legal researching. For the purpose of comprehending, interpreting, and assessing the laws that are available inside a specific legal system, this method is utilized. In the field of research, the normative legal research method is a research strategy that centres on the examination of legal standards that are applicable (Johnny Ibrahim, 2005; Syahrum, 2022). Through the use of this approach, researchers will investigate a wide range of legal regulations, judicial decisions, legal doctrine, and other legal sources in order to comprehend and interpret the rules that are now in place. As part of this investigation, the researcher adopted a research methodology by conducting an analysis of legal materials, law, and literature. These sources contain notions derived from legal professionals and serve as an analytical tool for addressing a legal matter.

FINDING AND DISCUSSION
The Significance of Digital Forensics as a Technique for Managing Electronic Evidence in Indonesia
The field of digital forensics is crucial in the management of electronic evidence in Indonesia. This technique enables investigators to locate, safeguard, and examine
digital evidence from diverse electronic devices, such as computers, cell phones, servers, or networks. The usage of information technology and electronic transactions in Indonesia is regulated by Law Number 11 of 2008, often known as the Information and Electronic Transactions Law (UU ITE). Digital forensics is a crucial instrument for upholding the ITE Law and addressing illicit activities associated with the utilization of technology (Atlam et al., 2020; Harbawi & Varol, 2016; Prayudi et al., 2015).

The field of digital forensics enables law enforcement agencies to address the rising prevalence of illicit acts in the digital age. Digital forensic activities encompass the procedures of gathering, obtaining, retrieving, preserving, and scrutinizing electronic data. These activities are crucial in the realm of cyber investigation and law enforcement in the present digital age. Digital forensics possesses the capacity to unveil evidence that may elude direct observation by the human eye, yet can furnish crucial indications in resolving criminal instances utilizing technology. Digital forensics professionals can examine digital evidence left by criminals in cyberspace by employing specialized techniques and instruments. This not only facilitates the implementation of the legislation, but also guarantees that the legal procedure is conducted with equity and transparency. In addition, digital forensics plays a crucial role in verifying the genuineness and reliability of electronic evidence utilized in criminal investigations and legal proceedings.

The significance of digital forensics is acknowledged not just by professionals in the area, but also in diverse literature and government policy. Digital forensics has become an essential component of the criminal justice system’s management of electronic evidence in several nations, including Indonesia. The Indonesian government is becoming more cognizant of the pressing need for digital forensics in addressing the escalating and intricate cyber crime risks. Digital forensics plays a crucial role not only in detecting and resolving technology-related crimes, but also in safeguarding individual rights, upholding justice, and enhancing national cyber security. Law enforcement agencies investigating cybercrime, data theft, online fraud, and other technology-based criminal activities are increasingly dependent on digital analysis. Digital forensics aids in the identification of the culprit, digital evidence, as well as the motives and techniques employed in the criminal act (Al Mutawa et al., 2019; Hewling, 2013). This enables investigators to implement suitable measures and preserve the principles of justice.

In the legal proceedings, the presence of dependable evidence holds utmost significance in rendering equitable and evidence-based judgments. Amidst the prevalence of electronic gadgets in the modern age, electronic evidence is gaining significance and relevance in legal proceedings. The significance of digital forensics is paramount in this context. Through meticulous examination of digital evidence, the court can render findings grounded in the factual information unveiled by the digital traces discovered. The process of digital forensics encompasses the collection of electronic evidence, as well as a comprehensive comprehension of technological functioning and investigative methodologies that adhere to legal norms.
Digital forensics serves as a crucial investigation technique and provides a strong basis for law enforcement in the modern digital age. Digital forensics plays a crucial role in ensuring both the actual and perceived delivery of justice by presenting trustworthy evidence. This contributes to enhancing public confidence in the justice system. The significance of digital forensics is growing in parallel with the advancements in technology and the emergence of novel digital dangers. The complexity of cyber security threats is growing, necessitating the use of digital forensics for their specialized treatment. Within this particular framework, digital forensics aids businesses and individuals in the surveillance, examination, and mitigation of information security occurrences that have the potential to inflict harm upon them.

The significance of digital forensics is intricately linked to safeguarding personal data and ensuring information security. Amidst the prevalent occurrence of data breaches and the improper handling of personal information, the field of digital forensics has emerged as an essential tool for detecting and addressing these security breaches. Digital forensics plays a crucial role in implementing legislation like the ITE Law, which prioritize the safeguarding of personal data and sensitive information. It ensures that these regulations are not just theoretical, but are effectively put into action. Through the ongoing advancement of techniques and strategies, digital forensics will progressively assume a more significant role in managing electronic evidence and safeguarding the security and authenticity of information in the future (Subektiningsih & Hariyadi, 2022; Syaufi et al., 2023; Zulkifli et al., 2021). In addition, digital forensics is crucial in assuring adherence to relevant legal requirements and standards pertaining to the utilization of information technology. In Indonesia, in addition to the ITE Law, there are various regulations and standards that govern the use of information technology. These include regulations concerning the protection of personal data and privacy rights. Digital forensics is a crucial component in the examination of security incidents. Organizations might employ digital forensics to examine data breaches, virus assaults, or unlawful intrusion into their systems. Through the analysis of digital traces, one can ascertain the origin of the issue, implement remedial measures, and proactively avert future attacks of a similar nature (Santhi & Nuarta, 2023).

In Indonesia, digital forensics plays a vital role in managing electronic evidence. Digital forensics serves as more than just an investigative tool; it is the fundamental pillar for upholding justice, security, and order in the contemporary digital society. Digital forensics, aided by regulations like the ITE Law and relevant standards, safeguards the security and integrity of information, upholds the law, and ensures adherence to applicable rules and regulations in the utilization of information technology.
The Role of Law Enforcement Officials in Organizing Electronic Evidence in Indonesia

The involvement of law enforcement personnel in managing electronic evidence in Indonesia is crucial not only for upholding security, enforcing the law, and ensuring fairness in the utilization of information technology, but also for guaranteeing that the legal proceedings adhere to the relevant legal norms (Hidayatullah & Wahyudi, 2023).

Here is a more detailed explanation of the primary responsibilities of law enforcement officials and their connection to relevant laws:

a) Aggregation of Digital Evidence: The Law Number 11 of 2008, also known as the Electronic Information and Transactions (UU ITE), serves as a crucial legal framework for the management of electronic evidence in Indonesia. Law enforcement officers have the duty to ensure that every stage of gathering electronic evidence adheres to the ITE Law. It is imperative for them to adhere to established protocols, uphold the values of human rights, privacy, and information security, and preserve the integrity of evidence. When presenting electronic evidence in a court of law, it is imperative to ensure that the evidence is acquired legally and adheres to the specifications outlined in the ITE Law. Law enforcement agents must possess a comprehensive comprehension of and adhere to protocols for utilizing electronic evidence in court, elucidating its genuineness and pertinence to judges and juries.

b) Electronic Evidence Analysis: The examination of electronic evidence by law enforcement personnel in Indonesia is a crucial step in managing evidence. The study must be conducted meticulously and comprehensively in accordance with the norms of digital forensics. The systematic process commences with the acquisition of evidence from many sources, followed by its examination by digital forensic specialists. It is imperative for authorities to guarantee adherence to digital forensics standards, encompassing the values of integrity, authenticity, and privacy. The court must consider the analysis results, while adhering to the norms of human rights and information security. Hence, the examination of digital evidence plays a crucial role in maintaining justice through law enforcement in Indonesia (Abraha, 2021; Siregar et al., 2022).

c) Utilization of Forensic Technology: The involvement of law enforcement officers is vital in the acquisition and examination of digital evidence. In order to effectively perform these responsibilities, it is necessary for them to consistently enhance their abilities and expertise in the field of forensic technology. Technological advancements give rise to new obstacles in addressing technology-related offenses, such as cybercrimes and the progressively intricate utilization of electronic evidence. Enhancing proficiency in forensic technology enables law enforcement officials to more effectively and precisely identify, gather, and examine electronic evidence. Proficiency in diverse forensic analysis techniques is essential, encompassing data retrieval,
digital trail detection, and metadata analysis. Furthermore, it is crucial for law enforcement officers to adhere to the principles and standards established by pertinent institutions, such as digital forensics bodies or certification bodies. These guidelines and standards ensure that the process of gathering and analyzing electronic evidence is conducted with utmost integrity and accuracy. Enhanced proficiency and strict compliance with forensic technology standards enable law enforcement officials to surmount the obstacles associated with technology-based crimes. Forensic experts possess the capacity to enhance their effectiveness in probing criminal cases that involve electronic evidence, while also guaranteeing the fairness and transparency of legal procedures. Hence, acquiring expertise and understanding in forensic technology is crucial for enhancing the efficacy and triumph of law enforcement officials in maintaining law and justice in society.

d) Presentation of Evidence in Court: Law enforcement officers must present electronic evidence acquired and evaluated in line with relevant legal rules. The process of presenting involves meticulousness and adherence to specified legal protocols. Law enforcement personnel are obligated to provide a clear and transparent account of the source of evidence, the procedures used for its collection, and the methodology employed for its examination. Additionally, they must guarantee that the evidence is comprehensible to both judges and juries, and fulfills all relevant legal prerequisites. Hence, the procedure of presenting digital evidence is crucial for upholding equity, openness, and confidence in the judicial system. For example. Engaging in cooperation with forensic specialists and affiliated organizations: The cooperation of law enforcement personnel, digital forensic experts, and relevant institutions is crucial in managing cases that involve electronic evidence. Digital forensics specialists offer technological proficiency, whilst legal officers contribute legal and procedural competence. Relevant agencies furnish the requisite resources and technology. This teamwork guarantees the dependability of evidence, the honesty of investigations, and triumph in law enforcement.

e) Legal and ethical considerations are significant in the practice of digital forensics. Adhering to right processes is crucial not only for ensuring the authenticity of evidence in court, but also for upholding public faith in the justice system and law enforcement. A comprehensive comprehension of both technical and legal aspects is required for effective participation in digital investigations.

f) Ultimately, the emergence of anti-forensic techniques employed by cybercriminals poses a significant difficulty. The investigation procedure is becoming more complex due to the use of more advanced encryption technologies and information hiding strategies. The advancement of digital forensics techniques must align with the technological progress employed by cybercriminals.
To address these issues, it is crucial for law enforcement and security specialists to enhance their technological abilities, foster collaboration across different sectors and countries, and reinforce the legislative framework that governs digital forensics activities. Effective combat against the continuously expanding cybercrime can only be achieved via the implementation of a comprehensive and sustainable strategy in digital forensics.

CONCLUSION

The significance of digital forensics in Indonesia lies in its role as a crucial method for managing electronic evidence, particularly in response to the pressing legal requirements associated with processing such evidence. The handling of electronic evidence should not be considered equivalent to traditional physical evidence. Given the susceptibility of electronic evidence to tampering by criminals seeking to conceal or eliminate traces of cyber crimes, the utilization of digital forensic methods in Indonesia’s legal system is a welcome development. These methods ensure that electronic evidence in cyber crimes is handled in a manner that aligns with legal requirements. Establishing the validity of criminal procedure legislation. Moreover, Law enforcement officers also play a crucial role in criminal procedural law, which necessitates collaboration and consistent coordination among police officers, prosecutors, legal advisors, and judges. The paradigm of law enforcement officers should be uniform in their approach to the use and management of electronic evidence using digital forensic techniques. In several developed countries, including the United States, digital forensic techniques have been employed and demonstrated to effectively preserve the integrity of electronic evidence.

References


Hewling, M. O. (2013). Digital forensics: an integrated approach for the investigation of cyber/computer related crimes.


