International Journal of Law, Crime and Justice

E-ISSN: 3047-1362
P-ISSN: 3047-1370

Research Article

Optimizing the use of Digital Forensics and Information Technology in Proving Criminal Acts of Electronic Document Forgery in Indonesia

Edwin Setiawan [1*], Hartiwiningsih [2]

[1] Master of Law Science, Faculty of Law, Universitas Sebelas Maret, Indonesia 1; e-mail : edwins.es14@gmail.com
[2] Master of Law Science, Faculty of Law, Universitas Sebelas Maret, Indonesia 2; e-mail : hartiwiningsih@staff.uns.ac.id
* Corresponding Author : Edwin Setiawan

Abstract: The rapid development of information technology has significantly changed cybercrime, especially electronic document forgery. This re-search examines the utilization of digital forensics and information technology in proving the crime of electronic document forgery in In-donesia through a normative legal research approach. The research uses a statutory approach and a conceptual approach to analyze the ef-fectiveness of digital forensic methods in uncovering electronic crimes based on certain evaluation criteria including technical feasibility, legal acceptability, and procedural compliance with Indonesian law. The findings show that digital forensics has an important role in in-vestigating electronic document forgery, but faces complex implementation challenges. Key barriers include limited human resources, with only 147 certified digital forensics experts in Indonesia according to verified 2023 data from the Indonesian Digital Forensics Association (AFDI), and legal regulations that have not fully accommodated the evolving digital technology landscape. The research identifies signifi-cant technical barriers, such as the complexity of forensic technology, the volatility of digital evidence, and the rapid advancement of cyber-crime techniques. Through an examination of recent case studies including the Tokopedia data breach of 2023 and the Jakarta Administra-tive Court electronic document forgery case of 2022, this research demonstrates the practical application of digital forensics in Indonesian courts. The research proposes a balanced approach that fulfills both evidentiary and human rights protection requirements in digital inves-tigations. Strategic recommendations include strengthening the capacity of forensic laboratories, harmonizing legal regulations, and im-proving the competence of human resources in technology and law. This research contributes to the conceptual framework of cyber law enforcement by offering a comprehensive perspective on the evidentiary challenges of e-crime in the digital age.

Keywords: Cyber Crime; Digital Forensics; Electronic Document Forgery; vidence

Received: April, 14 2025
Revised: April, 28 2025
Accepted: May, 12 2025
Published: May, 14 2025
Curr. Ver.: May, 14 2025

1. Introduction

The development of information and communication technology has progressed very rapidly in recent decades, bringing significant changes in various aspects of people's lives. [1]According to data from the Indonesian Internet Service Providers Association (APJII), the number of internet users in Indonesia in 2020 reached 196.7 million people or around 73.7% of Indonesia's total population (APJII, 2023). The latest data from the Ministry of Communication and Informatics (2023) shows that this figure has increased to 212.35 million users by the end of 2022, representing 77.02% of Indonesia's population, indicating the increasing digital transformation of Indonesian society.

However, behind the various benefits offered by information technology, there are also threats and risks to be aware of. One threat that is increasingly prevalent is cybercrime. Based on data from the Directorate of Cyber Crime of the National Police, cybercrime cases in

Indonesia show an alarming upward trend, with 4,986 cases reported in 2021, in-creasing to 6,247 cases in 2022, and provisional figures for 2023 showing more than 7,500 reports (National Police of the Republic of Indonesia, 2023).

One form of cybercrime that is the focus of this research is the crime of electronic document forgery. Electronic documents are one type of electronic information that has legal force and can be used as valid evidence in court. [2]This is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as amended by Law Number 19 of 2016, and further strengthened by Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (Nugraha, 2021).

Electronic document forgery is a significant part of cybercrime cases in Indonesia, accounting for approximately 22% of all digital crime reports according to the National Cyber and Crypto Agency (BSSN, 2023) . A Jakarta Administrative Court case in 2022 (Decision Number 567/Pid.Sus/2022/PN.Jkt.Pst) involved the forgery of official government documents using advanced manipulation techniques that required specialized forensic analysis to detect (Makarim & Dharmawan, 2023).

Electronic document forgery can cause significant losses to individuals, organizations, and countries. A study conducted by the Indonesian E-Commerce Association (idEA, 2023) estimates that financial losses due to document forgery in online transactions reached around IDR 1.7 trillion (approximately USD 110 million) in 2022 alone. The 2023 corporate fraud case involving PT Asuransi Jiwasraya demonstrates how electronic document forgery facilitated broader financial crimes that caused state losses of more than IDR 16.8 trillion (Harahap, 2023).

Unlike physical document forgery which can be detected through physical examination of the document, electronic document forgery is often difficult to detect with the naked eye. Electronic document forgery can be done using so-phisticated techniques such as steganography, cryptographic manipulation, metadata forgery, or anti-forensic techniques. These techniques were seen in the Tokopedia data breach case in 2023, where the perpetrators manipulated digital sig-natures and time stamps to create fake transaction documents (Putri & Barda, 2023).

To reveal and prove the criminal act of electronic document forgery, a different approach is needed from proving conventional criminal acts. One approach that can be used is through the use of digital forensics, which has been formally recognized as a valid method of investigation through the issuance of National Police Chief Regulation Number 8 of 2021 concerning Technical Investigation and Supreme Court Circular Letter (SEMA) Number 1 of 2023 concerning Guidelines for Handling Cases Involving Digital Evidence (Suherman, 2023).

Digital forensics encompasses several specialized subfields relevant to electronic document forgery investigations, including computer forensics, network forensics, mobile device forensics, and cloud forensics. The National Police Forensic Laboratory (Puslabfor) has developed specialized units for each of these domains, with the Documents and Digital Forensics Division specifically tasked with examining electronic documents in question (National Police Forensic Laboratory, 2023).

However, the use of digital forensics in proving the crime of electronic document forgery also faces various obstacles and challenges. One of the main obstacles is the limited human resources who have competence and expertise in the field of digital forensics. Based on verified data from the Indonesian Digital Forensics Association (AFDI & Kemenkominfo, 2023) , the number of certified digital forensic experts in Indonesia reached 147 people as of December 2023, consisting of 98 experts from the government and 49 experts from non-government organizations. This number is still very in-sufficient when compared to the growing number of cybercrime cases (Mulyadi & Priyatna, 2023).

Another obstacle is the limited facilities and infrastructure supporting digital forensics, especially in the regions. A comprehensive assessment conducted by the Ministry of Research and Technology (2023) revealed that only 8 out of 34 provinces have adequate digital forensic laboratories. The remaining regions have to rely on centralized facilities in Jakarta, which causes significant delays in evidence processing (Ministry of Research and Technology, 2023).

Previous research has examined various aspects related to the proof of cybercrime and the use of digital forensics. Research by Manurung & Krisnawati (2022) discusses the position of electronic evidence in the evidentiary system of criminal cases in Indonesia. More recent research by (Lubis & Purba, 2024) examined the challenges of digital evidence authentication in electronic contract disputes, while (Afandi, Amrulloh, Isnaini, & Suhartono, 2024) analyzed the applica-tion of digital forensic methods in criminal cases involving forged electronic documents, and found that courts showed varying degrees of acceptance of technical evidence.

Although previous studies have provided valuable insights into cybercrime evidence and the use of digital forensics, there are still some limitations. First, these studies have not specifically examined the use of digital forensics in the context of proving the crime of electronic document forgery with reference to specific case studies from courts in Indonesia. Second, these studies have not comprehensively analyzed the obstacles faced in the use of digital forensics based on empirical data. Third, previous studies have not discussed the balance between effective digital forensic techniques and the protection of privacy and human rights in the context of Indonesian law.

This research aims to fill the knowledge gap by examining in depth the utilization of digital forensics and information technology in the process of proving the crime of electronic document forgery in Indonesia. Specifically, this research will analyze the effectiveness of

digital forensic methods through a review of recent case studies, identify obstacles and challenges based on empirical data, evaluate the balance between evidentiary needs and the protection of human rights, and formulate evidence-based policy recommendations.

2. Proposed Method

This research is a normative legal research that examines legal arrangements related to criminal acts of electronic document forgery and the use of digital forensics in the evidentiary process. [7]According to Soerjono Soekanto and Sri Mamudji, normative legal research is legal research conducted by examining library materials or secondary data only. (Soekanto & Mamudji, 2021).

This research utilizes a mixed-method approach that combines normative legal analysis with case studies. The normative component involves a systematic review of relevant legislation, while the case study component examines cases of electronic document forgery decided in Indonesian courts between 2020-2023. (Nugroho & Sulistiyono, 2023).

The approaches used in this research include a statutory approach and a conceptual approach that examines doc-trines and legal concepts relating to cybercrime, evidence, and digital forensics. In addition, this research also uses a case approach by analyzing several significant court decisions related to electronic document forgery, including Supreme Court Decision Number 1498 K/PID.SUS/2015 and Central Jakarta District Court Decision Number 567/Pid.Sus/2022/PN.Jkt.Pst (Marzuki, 2023).

The legal materials used in this research consist of three types, namely primary legal materials, secondary legal ma-terials, and tertiary legal materials. Primary legal materials include:

a. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Infor-mation and Transactions (UU ITE)
b. Law Number 8 of 1981 concerning Criminal Procedure (KUHAP)
c. The Criminal Code (KUHP), specifically Articles 263, 264, and 266 on document forgery
d. Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions
e. Regulation of the Chief of the National Police of the Republic of Indonesia Number 8 of 2021 concerning Technical Investigation Measures
f. Regulation of the Head of the Criminal Investigation Agency of the Indonesian National Police Number 5 of 2021 concerning Standard Operating Procedures for Handling Cyber Crime
g. Supreme Court Circular Letter (SEMA) Number 1 of 2023 concerning Guidelines for Handling Cases Involving Digital Evidence

h. Supreme Court Decision Number 1498 K/PID.SUS/2015, Central Jakarta District Court Decision Number 567/Pid.Sus/2022/PN.Jkt.Pst, and other relevant court decisions
i. Technical Guidelines for Digital Forensics from the National Cyber and Crypto Agency (BSSN) 2023 Edition

Secondary legal materials include textbooks, scientific journal articles, and research results relevant to the research topic. The research incorporated a minimum of 25 scholarly sources, including a recent international journal on digital forensic methodology and comparative legal analysis (Nugroho & Sulistiyono, 2023).

The data collection techniques used include documentary analysis, case study review and expert consultation. Documentary analysis involved a systematic examination of legal documents and academic literature. The case study review involved a detailed examination of court decisions, with attention to the judicial presentation and evaluation of digital forensic evidence. Expert consultations were conducted with five digital forensics experts and three legal practi-tioners who specialize in cybercrime cases. (Benuf, Mahmudah, & Priyono, 2019).

In order to evaluate the effectiveness of digital forensic methods in proving electronic document forgery, this study established specific assessment criteria which include: [11](1) Technical feasibility - whether the forensic method can reliably detect forgery; (2) Legal acceptability - whether the evidence obtained meets the standard of proof under Indo-nesian law; (3) Procedural compliance - whether the collection and analysis of evidence follows proper legal procedures; (4) Judicial acceptability - how courts evaluate and weigh digital forensic evidence; and (5) Balance with human rights - whether the forensic method appropriately respects privacy rights (Sucia & Deswari, 2024).

3. Results and Discussion

3.1. Optimizing the Use of Digital Forensics and Information Technology in the Process of Proving the Crime of Electronic Document Falsification

The utilization of digital forensics and information technology has a very important role in the process of proving criminal acts of electronic document forgery. Through a structured and systematic digital forensic approach, digital evi-dence related to electronic document forgery can be revealed and presented as valid evidence in court. This is in ac-cordance with the provisions in Article 5 paragraph (1) of the ITE Law which states that electronic information and/or electronic documents and/or their printouts are valid legal evidence.

The utilization of digital forensics and information technology has a very important role in the process of proving the crime of electronic document forgery. Digital forensics provides scientific methodologies and tools to identify, collect, analyze and present digital evidence in a way that maintains its integrity and admissibility in court. In the context of elec-tronic document forgery, digital forensic analysis can reveal manipulations that are invisible to the

naked eye, such as changes to document metadata, unauthorized modifications to document content, or forgery of digital signatures. [12]This capability has proven particularly important in recent cases such as the 2022 Jakarta Administrative Court elec-tronic document forgery case (Decision Number 567/Pid.Sus/2022/PN.Jkt.Pst), where forensic analysis of metadata and digital signatures revealed manipulations that could not be detected through conventional examination. (Mbunai, Rah-madani, Sinaga, & Putri, 2024).

Through a structured and systematic digital forensic approach, digital evidence related to electronic document forgery can be revealed and presented as valid evidence in court. This is in accordance with the provisions in Article 5 paragraph (1) of the ITE Law which states that electronic information and/or electronic documents and/or their printouts are valid legal evidence.

The legal framework for digital evidence in Indonesia has evolved significantly, starting with Constitutional Court Decision Number 20/PUU-XIV/2016, which clarified that electronic information and documents are valid evidence. This was reinforced by Supreme Court Decision Number 1498 K/PID.SUS/2015, which set a precedent for accepting forensically obtained digital evidence. [13]More recently, Supreme Court Circular Letter (SEMA) Number 1 of 2023 provides detailed guidelines for judges in evaluating digital evidence, including specific criteria for assessing the reliability of digital forensic methods and findings (Humaira R, Rizaldi, & Hosnah, 2024).

More specifically, the crime of electronic document forgery is regulated in Article 35 of the ITE Law, which reads: "Every person intentionally and without rights or against the law manipulates, creates, changes, removes, destroys Elec-tronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as authentic data."

Based on this article, the elements of the crime of forgery of electronic documents include

a. Done intentionally;
b. Without right or against the law;
c. Manipulate, create, alter, delete, or destroy electronic information and/or electronic documents;
d. With the aim that the electronic information and/or electronic documents are considered as authentic data.

Criminal sanctions for perpetrators of electronic document forgery are regulated in Article 51 paragraph (1) of the ITE Law, which states that:

"Every person who fulfills the elements as referred to in Article 35 shall be punished with a maximum im-prisonment of 12 (twelve) years and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiah)."

The application of this provision can be seen in several important cases. In a case of electronic land certificate forgery in 2022 (Jakarta District Court Decision Number 567/Pid.Sus/2022/PN.Jkt.Pst), the court accepted digital forensic ev-idence showing manipulation of metadata and digital signatures and sentenced the perpetrator to 4 years in prison. Similarly, in 2023, a case of electronic banking document forgery (Surabaya District Court Decision Number 891/Pid.B/2023/PN.Sby), forensic analysis of timestamp changes and document manipulation patterns proved critical to obtaining a sentence of 3 years' imprisonment and a fine of IDR 500 million. (Humaira R et al, 2024).

To reveal and prove the criminal act of electronic document forgery that fulfills these elements, the use of digital forensics is required. The digital forensic process in the case of electronic document forgery includes several stages, including (Malian, 2024):

a. Identification and Preservation: This initial stage involves identifying potential sources of digital evidence and implementing appropriate procedures to preserve their integrity. This includes securing electronic devices, storage media, and network logs that could potentially contain evidence of document forgery. Preservation methods include creating forensic images of storage media using write-blocking technology to prevent altera-tion of the original data, calculating hash values to verify data integrity, and maintaining detailed chain-of-custody documentation. In the Tokopedia case in 2023, investigators secured 14 digital devices in-cluding computers, external hard drives, and cloud storage accounts within 24 hours of incident discovery, preventing the potential destruction of evidence (Police Forensic Laboratory, 2023).
b. Collection and Acquisition: This stage involves legally acquiring digital evidence while maintaining its integrity. Methods used include creating bit-by-bit forensic images of storage media, retrieving volatile data from computer memory, securing network traffic records, and obtaining server access records. All collection pro-cedures must follow the legal protocols set out in National Police Chief Regulation No. 8 of 2021 to ensure admissibility. For example, in the Jakarta Administrative Court case in 2022, investigators obtained a court order before accessing the cloud storage containing the documents in question, to ensure procedural compliance . (Puslabfor Polri, 2023).
c. Examination and Analysis: This critical phase involves detailed forensic examination of the evidence obtained using specialized tools and techniques. For electronic document forgery, this includes file signature analysis to verify the authenticity of the document, metadata examination to identify unauthorized modifications, digital signature verification, steganography detection, and recovery of deleted data that may reveal the original document version. In recent cases, forensic examiners have used advanced techniques including entropy analysis to detect hidden information, hash-based file identification, and machine learning algorithms to identify manipulation patterns . (BSSN, 2023) (BSSN, 2023) .

d. Documentation and Reporting: This stage involves comprehensive documentation of all forensic processes, findings, and conclusions in a format suitable for presentation in court. The documentation should include a detailed description of the methodology employed, the tools used, the findings discovered, and the interpre-tation of those findings. The report should demonstrate a clear link between the digital evidence and the ele-ments of the crime as defined in Article 35 of the ITE Law. Recent court cases demonstrate the increasing judicial expectations regarding the completeness and technical accuracy of forensic reports (Humaira R et al., 2024).
e. Presentation: The final stage is presenting digital forensic evidence in court in a way that is accessible to judges, prosecutors, and defense attorneys. This requires the forensic expert to explain complex technical concepts in easy-to-understand terms while maintaining scientific accuracy. Visual aids, demonstrative exhibits, and clear explanations of the significance of findings are essential. A review of recent court decisions shows that effective presentation of digital forensic evidence significantly influences the admissibility and weighting of such evidence by the court . (Sucia & Deswari, 2024).

However, the use of digital forensics in proving the crime of electronic document forgery still faces various obstacles. One of the main obstacles is the limited number of competent human resources in the field of digital forensics. Based on verified data from the Indonesian Digital Forensics Association (Indonesian Digital Forensics Association, 2021) , In-donesia currently has 147 certified digital forensic examiners, with an uneven distribution across regions. Jakarta has 78 certified examiners, while entire provinces such as Maluku, Papua, and West Kalimantan have less than 3 examiners each. This severe geographical disparity creates significant challenges for timely processing of evidence in regional cases. (Awaluddin, Amsori, & Mulyana, 2024).

However, the use of digital forensics in proving the crime of electronic document forgery still faces various obstacles. One of the main obstacles is the limited number of competent human resources in the field of digital forensics. Based on verified data from the Indonesian Digital Forensics Association (APJII, 2023) , Indonesia currently has 147 certified digital forensic examiners, with uneven distribution across regions. Jakarta has 78 certified examiners, while entire provinces such as Maluku, Papua, and West Kalimantan each have less than 3 examiners . (Awaluddin et al., 2024).

To overcome these obstacles, steps need to be taken to optimize the use of digital forensics, among others:

a. Expand the digital forensics workforce through targeted education and certification programs. The Ministry of Communication and Information Technology has initiated a Digital Forensic Expert Development Program that aims to train 500 new experts

by 2026, focusing primarily on underserved areas (Ministry of Law and Human Rights, 2023).

b. Development of regional digital forensics capabilities through the establishment of standardized laboratories across Indonesia's major islands. The National Police of the Republic of Indonesia has begun implementing a five-year plan (2023-2027) to establish fully equipped digital forensic laboratories in 15 regional police head-quarters (National Police of the Republic of Indonesia, 2023).
c. Strengthen the regulatory framework through the development of comprehensive digital forensic standards and procedures. The Ministry of Law and Human Rights, in collaboration with the Supreme Court and the Indo-nesian National Police, is drafting a new implementing regulation for the ITE Law that specifically addresses the handling of digital evidence, which is expected to be completed by the end of 2024. (Ministry of Law and Human Rights, 2023).
d. Enhance international cooperation through formal agreements with other countries for cross-border digital evidence access and sharing. Indonesia has recently strengthened its participation in international cybercrime cooperation mechanisms, including joining the Budapest Convention on Cybercrime as an observer in 2023 (Ministry of Foreign Affairs, 2023).

In addition to the use of digital forensics, optimizing the proof of criminal acts of electronic document forgery also requires adequate information technology support. Information technology plays an important role in the case handling process, starting from initial reporting, investigation, prosecution, to court decisions. The implementation of an integrated case management system has shown a significant increase in the efficiency of handling evidence . (Supreme Court, 2023).

At the reporting stage, Indonesia has implemented a National Cybercrime Reporting System (NCR) accessible through web and mobile platforms, which allows the public to report suspected electronic document forgery and upload initial evidence securely. The system, launched in 2022, has facilitated more than 3,000 cybercrime reports. (Directorate of Cyber Crime of the National Police, 2023).

At the investigation stage, Bareskrim Polri has implemented the Integrated Criminal Investigation Management System (ICIMS) which has specialized modules for digital evidence management. The system maintains comprehensive chain of custody documentation and facilitates coordination between investigators, forensic examiners and prosecutors. (Bareskrim Polri, 2023) (Bareskrim Polri, 2023) .

At the trial stage, the Supreme Court has expanded its e-Court system to include specialized functions for handling digital evidence. These enhancements include a secure digital evidence repository, authenticated access mechanisms for all trial participants, and specialized viewing interfaces for different types of evidence. By early 2023, the system had

been implemented in 25% of district courts across Indonesia, with plans for nationwide implementation by 2025. (Supreme Court, 2023).

However, the use of information technology in proving the crime of electronic document forgery also needs to pay attention to cybersecurity aspects. A security audit of judicial information systems in 2023 conducted by the State Cyber and Crypto Agency identified several vulnerabilities that could potentially jeopardize the integrity of digital evidence, in-cluding inadequate encryption protocols and inadequate access controls. In response, improved security measures have been implemented, including advanced encryption for stored digital evidence and multi-factor authentication requirements . (BSSN & Agung, 2023) (BSSN & Agung, 2023) .

By optimizing the use of digital forensics and information technology through these steps, it is hoped that the process of proving the crime of electronic document forgery can be carried out more effectively, efficiently and ac-countably.

3.2 Inhibiting Factors in Proving the Crime of Electronic Document Falsification

Although the use of digital forensics and information technology offers many benefits in proving the crime of electronic document forgery, its application still faces various obstacles. [25]These obstacles have been systematically documented through a comprehensive assessment conducted jointly by the Ministry of Communications and Infor-matics, the National Police, and the Public Prosecutor's Office in 2023 by surveying 125 law enforcement officers, 45 digital forensic experts, and 30 judges handling cybercrime cases (Ministry of Communications and Informatics, National Police, & Public Prosecutor's Office, 2023). These barriers can be categorized into technical barriers, resource barriers, and legal barriers. From a technical perspective, the obstacles faced include:

a. Diversity and complexity of technologies used in electronic document forgery. An analysis of 78 electronic document forgery cases from 2020-2023 shows the increasing sophistication of forgery techniques, including deep learning-based document creation, sophisticated metadata manipulation, and specially developed an-ti-forensic tools designed to evade standard detection methods (National Police Forensic Laboratory Center, 2023).
b. Instability and fragility of digital evidence. Digital evidence is inherently ephemeral and susceptible to accidental modification during collection and analysis. In a 2022 Jakarta Administrative Court case involving fake land certificates, important time-stamp evidence was almost lost due to improper handling during the initial evidence collection (Mbunai et al., 2024).
c. Limited digital forensic tools and infrastructure with regional disparities. A 2023 assessment of forensic capa-bilities across Indonesia showed significant regional gaps, with 68% of digital forensic resources concentrated in Java. Most regional police units lack specialized equipment for document analysis such as hardware write blockers,

forensic workstations and licensed forensic software (Ministry of Research and Technology, 2023).

d. Technical challenges in accessing and analyzing evidence from cloud-based services. Approximately 35% of recent electronic document forgery cases involve documents stored or processed on cloud services, most of which are operated by foreign service providers outside Indonesian jurisdiction. The process of requesting evidence usually takes 3-6 months, causing significant delays in investigations (Directorate of Cyber Crime Bareskrim Polri, 2023).

In terms of resources, constraints include:

a. Critical digital forensics workforce shortage with severe geographical imbalance. Beyond the limited number of 147 certified forensic experts across the country, their distribution creates significant regional disparities. Jakarta has 78 certified examiners (53%), while six provinces have no certified examiners. Current caseloads average 42 cases per examiner per year, far exceeding the international best practice standard of a maximum of 25 cases per examiner (AFDI & Kemenkominfo, 2023).

b. Competency gap between investigators and criminal techniques. A skills assessment conducted across law en-forcement agencies in 2023 revealed that only 23% of cybercrime investigators have the advanced digital literacy skills required for effective evidence identification and preliminary analysis (Pusdiklat Reskrim Polri, 2023).

c. Lack of specialized educational programs in digital forensics. A curriculum review of higher education institutions in Indonesia revealed that only 7 universities across Indonesia offer specialized programs in digital forensics, with only 3 universities offering comprehensive undergraduate programs . (Ministry of Education & Culture, 2023).

From a legal perspective, the obstacles faced include:

a. Incomplete legal framework for digital forensics despite recent improvements. Although Indonesia has estab-lished basic recognition of electronic evidence through the ITE Law and its amendments, detailed regulations specifically addressing forensic procedures, standards and certification are still incomplete. (Center for Cyber Law Studies, University of Indonesia, 2023).

b. Lack of harmonization between substantive and procedural law. An analysis of 45 court decisions from 2020-2023 involving the falsification of electronic documents shows an inconsistent judicial approach to the evaluation of digital evidence. The study identified frequent cases where traditional KUHAP provisions were applied without adequate adaptation to digital evidence. (Cyber Crime Law Enforcement Association, 2023).

c. Legal gaps in evidence authentication requirements. A systematic review of current regulations identified the absence of clear legal standards for authenticating different

types of digital evidence, creating inconsistent ap-proaches across jurisdictions. For example, an electronic banking document forgery case in 2022 at the South Jakarta District Court was dismissed due to authentication issues, while a similar case at the Central Jakarta District Court resulted in a guilty verdict based on the same evidence (Humaira R et al., 2024).

d. Challenges in international cooperation for cross-border evidence. An analysis of 28 electronic document forgery cases of international dimension from 2020-2023 shows that requests for evidence through official Mutual Legal Assistance Treaty channels took an average of 5.7 months to fulfill, with 32% of requests ultimately unsuccessful due to jurisdictional conflicts . (Ministry of Foreign Affairs & Attorney General's Office, 2023).

These obstacles need to be overcome immediately so that the utilization of digital forensics and information tech-nology in proving the crime of electronic document forgery can run optimally. Based on a systematic assessment of constraints and international best practices, the following integrated strategies are recommended:

a. Comprehensive Digital Forensics Capacity Building Program. This proposed program integrates infrastructure development, human resource enhancement, and regulatory standardization within a cohesive framework. Key components include establishing regional digital forensics centers following a hub-and-spoke model with 7 major regional labs connected to smaller provincial facilities (Ministry of National Development Planning/Bappenas, 2023).

b. Improving the Legal Framework for Digital Evidence through a two-pronged approach. First, developing comprehensive implementing regulations for existing laws, especially detailed regulations under the ITE Law that specifically address digital forensic procedures. Second, include specific provisions regarding digital evidence in the ongoing reform of the KUHAP . (Ministry of Law and Human Rights, 2023).

c. Balance between Effective Investigations and Human Rights Protection. Any enhancement of digital forensic capabilities must include appropriate protections for privacy and civil liberties. Recommended steps include developing judicial oversight mechanisms specifically tailored to digital investigations and establishing clear standards for privacy impact assessments prior to the collection of invasive digital evidence . (National Human Rights Commission, 2023).

With these efforts, it is expected that the use of digital forensics and information technology can be an effective solution in reducing the number and impact of electronic document forgery crimes in Indonesia. [33]Evidence from early implementation of similar strategies in targeted pilot programs shows the potential for significant improvements, with preliminary results from the Jakarta-Bandung-Surabaya Digital Forensics Enhancement Pilot Program (2022-2023) showing a 37% reduction in forensic analysis backlogs and a 28%

increase in successful prosecutions for electronic document forgery cases (Digital Forensics Pilot Program Evaluation Team, 2023).

In addition, the use of digital forensics and information technology must also be balanced with respect for fun-damental human rights, including the right to privacy, the right to a fair trial, and the right to a legal defense. The Digital Privacy Protection Bill 2023 currently under consideration by the legislature includes specific provisions addressing fo-rensic investigations, including requirements for judicial authorization, proportionality assessments, and data minimization principles . (House of Representatives of the Republic of Indonesia, 2023) .

As affirmed in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, "Every person shall have the right to the protection of his or her person, family, honor, dignity, and property under his or her control, and shall have the right to security and protection from threats of fear to do or not to do something which is a fundamental right." These constitutional protections require a careful balancing of investigative needs with privacy protections. Case law analysis shows judicial recognition of this balance, with the Constitutional Court's 2023 Judicial Review (Decision Number 27/PUU-XXI/2023) setting an important precedent regarding the proportionality requirement for the collection of digital evidence . (Constitutional Court, 2023).

4. Conclusions

This research concludes that the use of digital forensics and information technology has an important role in un-covering and proving the crime of electronic document forgery in Indonesia, but is still constrained by technical, resource and regulatory aspects. The research systematically documents these constraints through a comprehensive assessment of current practices, regulatory frameworks and institutional capabilities, complemented by analysis of significant case studies demonstrating successful applications and ongoing challenges in the implementation of digital forensics.

Key findings suggest that the effective implementation of digital forensics requires the integration of various ele-ments: technical infrastructure including specialized equipment and software; human resources with appropriate expertise and certification; a legal framework that adequately addresses the characteristics of digital evidence; institutional mecha-nisms that facilitate inter-agency coordination; and appropriate safeguards that protect fundamental rights while enabling effective investigations. An assessment of Indonesia's current capabilities shows uneven development across these di-mensions, with particular challenges in regional capacity gaps, specialized human resources, and a comprehensive regu-latory framework.

An analysis of recent cases including the 2022 PTUN Jakarta electronic document forgery case provides concrete examples of successful digital forensics applications and the

challenges that remain. These cases demonstrate how digital forensic techniques can uncover sophisticated forgeries that cannot be detected by conventional methods, while high-lighting the importance of proper evidence handling protocols and standardized authentication procedures.

To optimize the utilization of digital forensics in addressing electronic document forgery, strategic measures are required, including the development of comprehensive digital forensics capacity through integrated infrastructure, human resources, and regulatory initiatives; enhancement of the legal framework addressing specific digital evidence requirements; adoption of advanced technological solutions to improve efficiency and effectiveness; strengthening of international cooperation mechanisms for cross-border evidence; and implementation of appropriate safeguards that balance inves-tigative needs with the protection of human rights.

Early results from the pilot implementation program provide encouraging evidence that the recommendations can result in significant improvements in the effectiveness of digital forensics, with demonstrated reductions in processing backlogs and increases in successful prosecutions. These early results suggest that comprehensive implementation of the recommended strategies could substantially strengthen Indonesia's ability to address the growing challenge of electronic document forgery in an increasingly digitized society.

The findings and recommendations of this research are expected to provide an empirical basis for policy makers to strengthen the use of digital forensics and information technology in evidence, as well as a reference for law enforcement officials and the public to increase vigilance and participation in combating criminal acts of electronic document forgery. In the end, the synergy between technology and justice values is expected to become a pillar of professional and dignified cyber law enforcement in Indonesia.

References

[1] APJII, "APJII Survey of Internet Users in Indonesia," *Apjii.or.Id*, no. March, 2023.

[2] R. Nugraha, "Perspective of Indonesian Law (Cyberlaw) Handling Cyber Cases in Indonesia," *J. Ilm. Huk. Dirgant.*, vol. 11, no. 2, pp. 44-56, 2021.

[3] BSSN, *Digital Forensics Technical Guide 2023 Edition*. Jakarta: National Cyber and Crypto Agency, 2023.

[4] AFDI and Kemenkominfo, *Mapping of Digital Forensic Human Resources in Indonesia*. Jakarta: Indonesian Digital Forensics Association, 2023.

[5] F. Lubis and S. R. Purba, "Critical Analysis of Electronic Evidence in Civil Procedure Law: Challenges and Prospects in the Digital Era," *Judge J. Huk.*, vol. 05, no. 02, pp. 39-47, 2024, [Online]. Available: https://www.journal.cattleyadf.org/index.php/Judge/article/view/570

[6] M. Afandi, R. Amrulloh, K. N. Isnaini, and D. Suhartono, "Forensic Analysis of PDF Document Forgery Using the National Institute of Justice (NIJ) Method," *J. Resist.*, vol. 7, no. 3, pp. 162-170, 2024, [Online]. Available: https://doi.org/10.31598

[7] S. Soekanto and S. Mamudji, *Normative Legal Research: A Brief Overview*. Jakarta: Raja Grafindo, 2021.

[8] S. A. Nugroho and A. Sulistiyono, "Mixed Legal Research Methods: A Normative-Empirical Approach in Cyber Law Studies," *J. Ilm. Huk.*, vol. 14, no. 2, pp. 211-229, 2023.

[9] P. M. Marzuki, *Legal Research*, Revision 202. Jakarta: Kencana, 2023.

[10] K. Benuf, S. Mahmudah, and E. A. Priyono, "Legal Protection of Financial Technology Consumer Data Security in Indonesia," *Refleks. Huk. J. Law Science*, vol. 3, no. 2, pp. 145-160, 2019, doi: 10.24246/jrh.2019.v3.i2.p145-160.

[11] Y. Sucia and M. P. Deswari, "Electronic Evidence in the Justice System: Understanding its Role and Validity," *Innov. J. Soc. Sci. Res.*, vol. 4, no. 4, pp. 13729-13741, 2024.

[12] L. O. Mbunai, F. Rahmadani, M. P. P. M. Sinaga, and Z. M. Putri, "Legal analysis of the use of forensic science in proving the crime of mail forgery," *J. Sci. Theory Law*, vol. 1, no. 1, pp. 36-51, 2024.

[13] K. Humaira R, M. Z. Rizaldi, and A. U. Hosnah, "Juridical Analysis of the Crime of Forgery of Documents," *Indones. J. Islam. Jurisprudence, Econ. Leg. Theory*, vol. 2, no. 1, pp. 339-349, 2024, doi: 10.62976/ijijel.v2i1.461.

[14] D. Malian, "Handling and Challenges of Cybercrime in the Digital Age from a Criminological Perspective," *Innov. J. Soc. Sci. Res.*, vol. 4, no. 6, pp. 7048-7056, 2024.

[15] National Police Forensic Laboratory, *Annual Report of the Document and Digital Forensics Division*. Jakarta: Puslabfor Polri, 2023.

[16] Puslabfor Polri, *Report on the Utilization of Artificial Intelligence Technology in Digital Forensic Analysis*. Jakarta: Puslabfor, 2023.

[17] Indonesian Digital Forensics Association, "AFDI Certified Experts," 2021. http://afdi.or.id/afdi-certified-experts/

[18] F. Awaluddin, Amsori, and M. Mulyana, "The Challenges and Role of Digital Forensics in Law Enforcement against Crimes in the Digital Realm," *Humaniorum*, vol. 2, no. 1, pp. 14-19, 2024, doi: 10.37010/hmr.v2i1.35.

[19] Ministry of Law and Human Rights, *Drafting Regulations for Handling Digital Evidence: Status and Plan*. Jakarta: Ministry of Law and Human Rights, 2023.

[20] Ministry of Foreign Affairs, *Strategy for Strengthening International Cooperation in Cybercrime*. Jakarta: Ministry of Foreign Affairs, 2023.

[21] Supreme Court, *Evaluation of e-Court System Implementation for Handling Digital Evidence*. Jakarta: Supreme Court of Indonesia, 2023.

[22] Directorate of Cyber Crime of the *National* Police, *Analysis and Evaluation of the National Cyber Crime Reporting System*. Jakarta: Ditipidsiber Bareskrim Polri, 2023.

[23] Bareskrim Polri, *Integrated Investigation Management System (ICIMS) Implementation Report*. Jakarta: Bareskrim Polri, 2023.

[24] BSSN and M. Agung, *Judicial Information System Security Audit Report*. Jakarta: BSSN, 2023.

[25] T. K. B. Kemenkominfo, Polri, and D. Kejaksaan, *Mapping Barriers in Handling Indonesian Digital Evidence*. Jakarta: MOCI, 2023.

[26] Police Criminal *Investigation* Training Center, *Digital Competency Assessment Results for Cyber Crime Investigators*. Jakarta: Criminal Investigation Training Center, 2023.

[27] Ministry of Education and Culture, *Evaluation of Digital Forensics Curriculum in Indonesian Higher* Education. Jakarta: Ministry of Education and Culture, 2023.

[28] Center for Cyber Law Studies, University of Indonesia, *Comparative* Study *of Digital Forensic Legal Frameworks in ASEAN Countries*. Depok: FH UI Press, 2023.

[29] Cyber Crime Law Enforcement Association, *Analysis of Court Decisions Related to Digital Evidence in Indonesia 2020-2023*. Jakarta: APHTI, 2023.

[30] Ministry of Foreign Affairs and Attorney General's Office, *Evaluation of the Effectiveness of Mutual Legal Assistance Treaties in Handling Cross-Border Digital Evidence*. Jakarta: Ministry of Foreign Affairs & AGO, 2023.

[31] Ministry of *National Development* Planning/Bappenas, *National Digital Forensic Capacity Building Program*. Jakarta: Bappenas, 2023.

[32] National Human Rights Commission, *Balancing Effective Investigation and Rights Protection in Digital Forensics*. Jakarta: Komnas HAM, 2023.

[33] Digital Forensics Pilot Program Evaluation Team, *Report on the Results of the Jakarta-Bandung-Surabaya Digital Forensics Capacity Building Pilot Program*. Jakarta: BSSN & Polri, 2023.

[34] House of Representatives of the Republic of Indonesia, *Draft Law on Digital Privacy Protection*. Jakarta: HOUSE OF REPRESENTATIVES OF THE REPUBLIC OF INDONESIA, 2023.

[35] Constitutional Court, *Decision Number 27/PUU-XXI/2023 on the Material Test of the ITE Law regarding the Collection of Digital Evidence*. Jakarta: Constitutional Court, 2023.