Journal of Law & Social Politics
Volume 4, Issue 3, 281-291
e_ISSN: 2807-6311
https://jolastic.id/index.php/jlsp/index
DOI: doi.org/10.59261/jlsp.v4i3.131

The Urgency of Digital Forensics in Investigating the Criminal Offense of Disseminating False News at Cirebon City Police Resort

Nur Abida Yasvin*
Universitas Swadaya Gunung Jati, Indonesia

Waluyadi
Universitas Swadaya Gunung Jati, Indonesia

***Corresponding author:**
Nur Abida Yasvin, Universitas Swadaya Gunung Jati, Indonesia.
✉nurabidayasvin@gmail.com

Article Info:

Article history:
Received: May 14, 2026
Revised: June 17, 2026
Accepted: July 02, 2026

Keywords:
Digital Forensics; Investigation; False News; Hoax; ITE Law; Cirebon City Police Resort.

Abstract

Background: The rapid advancement of information technology has transformed communication and information dissemination, particularly through digital platforms and social media. However, this progress has also increased the risk of cybercrime, including the spread of false news.
Objective: This study analyzes the urgency of digital forensics in investigating the criminal offense of disseminating false news, or *hoax*, through digital platforms at the Cirebon City Police Resort (*Polresta Cirebon*), with a specific focus on investigative capacity and constraints under the framework of the Electronic Information and Transactions Law (*ITE Law*).
Methods: This study employs a normative juridical approach supplemented by empirical field interviews. It analyzes the role of digital forensics in collecting and examining electronic evidence under Law Number 1 of 2024 concerning the Second Amendment to the *ITE Law*. Primary data were obtained through structured interviews with two investigators at *Polresta Cirebon*, while secondary data were derived from legal literature and statutory regulations.
Results: Digital forensics is critically needed to trace digital footprints, verify the authenticity of *hoax* content, reconstruct dissemination chains, and strengthen the admissibility of electronic evidence in court. The key challenges include limited access to overseas servers, perpetrator anonymity through encryption, rapid changes in digital content, a shortage of trained investigators at the *Polres*/*Polsek* level, and insufficient forensic laboratory infrastructure.
Conclusion: This study recommends the establishment of specific digital forensic regulations, grassroots forensic investigation teams, ISO/IEC 17024- and ISO/IEC 17025-certified personnel and laboratories, and cross-platform international cooperation mechanisms to enhance *ITE Law* enforcement against dissemination of false news.

To cite this article: Yasvin, A. N., & Waluyadi. (2026). The Urgency of Digital Forensics in Investigating the Criminal Offense of Disseminating False News at Cirebon City Police Resort. Journal of Law & Social Politics, 4(3), 281-291. https://doi.org/10.59261/jlsp.v4i3.131

INTRODUCTION

The development of information technology in Indonesia is currently advancing very rapidly. The primary purpose of technology is to facilitate human activities. Information technology is widely used to process, manage, and analyze data in order to produce relevant, fast, clear, and accurate information. It has been widely applied in government agencies, private companies, and other institutions (Ahadiyah, 2024). In its development, technology has played an important role; one example is the growth of social media, which aims to help individuals, companies, and other institutions carry out productive activities and obtain the latest information. The increasing number of information technology users has, on the one hand, produced positive

impacts by facilitating communication and other interactions among individuals; however, it has also generated negative impacts (Rachmie, 2020; Rahmadina & Tornado, 2026).

In the current digital era, the development of information and communication technology has made it easier to disseminate information globally in an instant. However, this progress has also triggered the emergence of various new types of crimes committed online, especially through social media platforms and related applications (Sanusi et al., 2024). This speed and convenience are also exploited by some individuals to commit irresponsible acts, such as spreading misleading or false news. Such false news is disseminated intentionally or unintentionally to create unrest, distrust, or other negative impacts.

The dissemination of false news is no longer merely a social problem; it has developed into a criminal offense regulated by law in many countries, including Indonesia. In investigating the criminal offense of disseminating false news, police institutions face significant challenges. False news is usually spread through digital platforms such as social media, instant messaging applications, or websites, all of which generate digital traces that are not always easy to identify, prove, or process.

This is where the role of digital forensics becomes highly important. Digital forensics involves the identification, collection, processing, analysis, and presentation of digital evidence in a lawful manner that is admissible in court. Through digital forensics, investigators can trace perpetrators' digital footprints, verify the authenticity of information, reconstruct the dissemination flow of false news, and produce strong evidence to support legal proceedings.

Referring to the description above, the Indonesian government issued Law of the Republic of Indonesia Number 1 of 2024 concerning Electronic Information and Transactions, which states that electronic information and/or electronic documents and/or their printouts constitute valid legal evidence. Therefore, the role of digital forensics as a method of proving digital crime cases has become increasingly important (Saputra, 2017).

Several previous studies have addressed related issues, such as Rachmie (2020) on digital forensics in website hacking (Rahmadina & Tornado, 2026); Saputra et al. (2017) on drug-related steganography and digital evidence analysis; Haidarrani et al. (2024) on criminal liability for dissemination under the ITE Law; Herman et al. (2024) on the use of digital forensics to prove defamation on social media under the ITE Law; Amsori et al. (2024) on the challenges of digital forensics in law enforcement against cybercrime; Singgih et al. (2024) on technical and legal obstacles in cybercrime investigations; and Annisa et al. (2025) on the influence of forensic technology on the accuracy of suspect identification. This study fills the gap by focusing specifically on the Cirebon City Police Resort (*Polresta Cirebon*).

Although several previous studies have discussed digital forensics, most focus on criminal acts such as fraud, online gambling, and hate speech. Meanwhile, studies addressing the dissemination of false news generally focus on legal analysis from the Criminal Code and criminological perspectives. The urgency of digital forensics in investigating the criminal offense of disseminating false news at the Cirebon City Police Resort has not been widely examined. This gap provides an opportunity for further research to understand the development of technological systems and how digital forensics can influence investigations into such offenses. The novelty of this study lies in its dual contribution: (1) empirically documenting specific investigative challenges and capacity gaps at *Polresta Cirebon*, and (2) normatively analyzing how the ITE Law, KUHAP, and Police Regulation No. 8 of 2014 apply to digital forensic evidentiary processes in false news cases, enabling more targeted and actionable policy recommendations than broader national-level studies (K. N. R. I. Indonesia, 2025).

The Cirebon City Police Resort (*Polresta Cirebon*) is a strategic frontline law enforcement institution serving a densely populated urban area in West Java, Indonesia. As a grassroots policing unit, *Polresta Cirebon* handles an increasing number of cyber-related cases, including the dissemination of false news (hoaxes) through social media platforms. At the *Polres* and *Polsek* levels, the capacity to investigate such cases using digital forensic methods remains limited due to shortages of trained investigators, forensic equipment, and laboratory infrastructure. This study specifically examines these ground-level realities at *Polresta Cirebon*, thereby contributing a localized empirical perspective that complements existing normative legal studies on digital forensics in Indonesia.

This study aims to analyze the urgency of digital forensics as an evidentiary tool in investigating the criminal offense of disseminating false news at the Cirebon City Police Resort. In addition, it seeks to identify the challenges and solutions in applying digital forensics within the context of digital law enforcement at the institution. Furthermore, this study provides strategic recommendations for strengthening digital-forensics-based investigative capacity to improve the effectiveness of law enforcement in the digital era.

This research is expected to contribute to a deeper understanding of the urgency of digital forensics in investigating the criminal offense of disseminating false news at the Cirebon City Police Resort. By understanding this role, more effective strategies can be formulated to prevent and address digital crime, while also contributing positively to law enforcement in an increasingly advanced digital era.

The literature review below presents reference sources related to the research problem. A literature review consists of scholarly citations that support the writing process (Waluyadi & Leliya, 2022). Through the theoretical framework, conclusions or expert opinions can be derived, which are highly useful as a research foundation. This literature review is necessary to ensure that the research has a solid academic basis. The presence of a literature review indicates that the study is conducted using a scientific approach to obtain valid data.

Digital forensics is a field of study that focuses on the identification, collection, analysis, and preservation of digital evidence for investigative purposes. In an increasingly connected digital world, digital evidence has become crucial in uncovering cybercrimes such as fraud, hacking, data breaches, and the dissemination of illegal content.

Based on the definition above, digital forensics is an integrated discipline that applies scientific and systematic methods to identify, preserve, collect, analyze, and present digital evidence that is admissible in court. By emphasizing evidence authenticity, chain of custody, and objectivity, digital forensics plays a crucial role in upholding justice in both criminal and civil technology-related cases, despite challenges such as large data volumes, encryption, and rapid technological advancement.

Article 1 paragraph (5) of Law Number 20 of 2025 concerning the Criminal Procedure Code, as well as Article 1 paragraph (2) of Law Number 8 of 1981 concerning the Criminal Procedure Code, explains that investigation is a series of actions carried out by investigators in accordance with legal procedures to search for and collect evidence in order to clarify a criminal offense and identify the suspect.

Investigation plays a crucial role because it serves as the gateway that determines the direction of case handling and the quality of evidence presented at trial. Therefore, it should not be viewed merely as an administrative procedure, but rather as a complex legal process with implications for the protection of the rights of all parties, and its results form the basis for determining whether a case will be prosecuted in court.

In Indonesia, the criminal offense of disseminating false news is regulated in Law Number 1 of 2024 concerning Electronic Information and Transactions. This law was established as part of government efforts to strengthen regulation in the digital sphere and protect the public from deception or losses caused by false information. In an era of rapid technological advancement, false news spreads more easily and can cause serious impacts. For individuals, it may damage reputation, create anxiety, cause mental health issues, or result in financial losses; for society, it may undermine social cohesion and trust, create tension or unrest, and reduce information literacy; while for the state, it may disrupt the economy, damage national reputation, and interfere with governance and democratic processes. Overall, false news harms not only specific individuals but also the stability of broader social, economic, and political systems.

Article 28 paragraph (1) of Law Number 1 of 2024 concerning Electronic Information and Transactions regulates the prohibition of disseminating information containing false or misleading content. This provision aims to protect the public from misinformation that may cause unrest, hatred, or conflict in society (Haidarrani et al., 2024).

In general, the criminal offense of disseminating false news refers to any person who intentionally disseminates electronic information and/or electronic documents containing false statements that cause harm. This offense includes several essential elements: the perpetrator is any person; the act is conducted intentionally; the conduct involves dissemination of electronic information or documents; the content contains false information; and it results in losses to

others.

Polresta (*Kepolisian Resor Kota*) is a structural command unit of the Indonesian National Police at the regency/city level. A police resort located in an urban area or a region with high vulnerability is commonly referred to as a *Kepolisian Resor Kota* (City Police Resort/*Polresta*). *Kepolisian Republik Indonesia* (kabupaten/kota)

Based on the definition above, *Polresta* (*Kepolisian Resor Kota*) is a designation for a Police Resort (*Polres*) located in a major urban area or a region with high vulnerability. It is responsible for maintaining security and public order and enforcing the law at the regency/city level, operating under the Regional Police (*Polda*), and overseeing several Sector Police units (*Polsek*) within its jurisdiction.

METHOD

Type of Research

This study employed a combined normative-empirical juridical approach. The normative dimension used a literature study method in which statutes and regulations served as the primary objects of doctrinal legal analysis. The empirical dimension involved structured field interviews to obtain primary data on the practical application of digital forensics at Polresta Cirebon. This dual approach bridged the gap between the normative legal framework governing digital evidence and the practical realities of its implementation at the grassroots policing level, particularly in relation to the urgency of digital forensics in investigating the criminal offense of disseminating false news.

Research Approach

This study applied qualitative legal research. Qualitative research is a method that uses a naturalistic approach to seek and understand meaning within a specific contextual setting. In this study, the approach focused on respondents' perspectives, experiences, and behavior, and used descriptive analysis to explore the urgency of digital forensics in investigating the criminal offense of disseminating false news.

Sources of Legal Materials

Primary Legal Materials

Primary legal materials are binding legal sources, including laws and regulations as well as legal instruments from the colonial period that remain in force and have permanent legal authority. This study used the following legal instruments:

1) Law Number 1 of 2024 concerning the Amendment to Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions ((UU), 2016; UU, 2024; UU 19 tahun 2004, 2004).
2) Law Number 1 of 2023 concerning the Amendment to Law Number 1 of 1946 concerning the Criminal Code (Presiden Republik Indonesia, 2023).
3) Law Number 20 of 2025 concerning the Amendment to Law Number 8 of 1981 concerning the Criminal Procedure Code (U. Indonesia & Indonesia, 1945).
4) Regulation of the Chief of the Indonesian National Police Number 8 of 2014 concerning the Amendment to Regulation of the Chief of the Indonesian National Police Number 10 of 2010 on Procedures for Managing Evidence within the Indonesian National Police (K. N. R. I. Indonesia, 2025).

Secondary Legal Materials

Secondary legal materials were obtained through the inventory and review of books, papers, articles, journals, and research findings related to the topic under study. These materials were then examined for relevance to support scientifically valid conclusions.

Non-Legal Materials

Non-legal materials included internet sources and non-legal research reports and journals, insofar as they were relevant to the topic under investigation.

Tertiary Legal Materials

Tertiary legal materials provided guidance or explanations regarding primary and secondary legal materials, such as legal dictionaries, encyclopedias, and other reference works.

Primary Data

Primary data were obtained through structured interviews with two key informants selected using purposive sampling based on their direct investigative roles at Polresta Cirebon: Bripda Arman Yudiansyah and Aiptu Dedi Cahyadi. The interview instrument covered: (1) types of digital evidence encountered in false news cases; (2) digital forensic procedures applied during investigations; (3) challenges in accessing, processing, and presenting electronic evidence; and (4) institutional capacity and infrastructure constraints.

Interviews were conducted in person at Polresta Cirebon, with informed consent obtained from each participant. Interview transcripts were analyzed using thematic coding to identify patterns aligned with the research objectives. Although the sample was limited to two informants, this was appropriate for a normative-empirical qualitative study aimed at in-depth institutional documentation rather than statistical generalization.

Analysis of Legal Materials

This study processed legal materials through interpretation of written literature and other documentary sources. A qualitative analytical perspective was applied, emphasizing in-depth understanding of social and legal phenomena through the exploration of non-numerical data such as interviews, observations, and document analysis. The aim was to reveal meanings, contexts, and subjective patterns underlying human behavior rather than producing quantitative measurements.

Within this qualitative framework, a statutory approach was used to examine consistency and coherence among legal instruments, including relationships between laws, the Constitution, and derivative regulations and their parent statutes. The results of this interpretive analysis formed substantive scientific arguments to address the legal issues under investigation.

RESULTS AND DISCUSSION

Results

This study reveals that digital forensics holds high urgency as an evidentiary instrument in investigating the criminal offense of disseminating false news at the Cirebon City Police Resort, as demonstrated by official interview results with Bripda Arman Yudiansyah and Aiptu Dedi Cahyadi from the Cirebon City Police Resort. The first finding emphasizes the use of physical digital evidence, such as smartphones, laptops, flash drives, and similar devices, alongside data evidence in the form of photos, videos, and digital files. This is supported by comprehensive forensic analysis results. The urgency of digital forensics arises from the fact that cases of false-news dissemination are difficult to resolve without valid digital evidence, which facilitates the identification of perpetrators and the elucidation of dissemination mechanisms through digital platforms.

Further interview results indicate that the implementation of digital forensics still faces significant challenges, including difficulties in accessing data from overseas servers protected by privacy regulations, perpetrators' ability to remove traces through anonymity or encryption techniques, and the rapid dynamics of content changes on online platforms. Additionally, there are limitations in human resources and infrastructure, such as a shortage of trained investigators at the Polres/Polsek level, insufficient disk-imaging tools, advanced storage-media readers, updated forensic software, and high-performance computing resources necessary for encryption analysis.

Discussion

This study reveals that digital forensics has a high degree of urgency as an evidentiary instrument in investigating the criminal offense of disseminating false news at the Cirebon City Police Resort, as shown by official research interviews with Bripda Arman Yudiansyah and Aiptu Dedi Cahyadi of the Cirebon City Police Resort. The first finding emphasizes the use of physical digital evidence, including smartphones, laptops, flash drives, and similar devices, as well as

digital data evidence such as photos, videos, and electronic files. This is in accordance with Law Number 1 of 2024 (UU, 2024) concerning the Amendment to Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. Article 5 implicitly provides a legal basis for the use of digital forensics in analyzing evidence in criminal offenses involving electronic systems; therefore, Law Number 1 of 2024 concerning the Amendment to Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions serves as a legal foundation for digital forensic practice.

In handling criminal offenses, strong evidence is required, and such evidence can now be obtained through the use of information technology. The evidentiary system under Law Number 20 of 2025 concerning the Amendment to Law Number 8 of 1981 concerning the Criminal Procedure Code adopts a negative legal proof system (*negatief wettelijk bewijsstelsel*), in which only evidence legally recognized by law may be used to prove a case. The types of lawful evidence are regulated in Article 184 paragraph (1) of Law Number 20 of 2025 concerning the Amendment to Law Number 8 of 1981 concerning the Criminal Procedure Code , including witness testimony, expert testimony, documents, indications, and the defendant's statement. Therefore, evidence outside these provisions cannot be considered valid. Although Law Number 20 of 2025 concerning the Amendment to Law Number 8 of 1981 concerning the Criminal Procedure Code regulates the types of valid evidence, further elaboration is now contained in various other laws and regulations. One of them is Law Number 1 of 2024 (UU, 2024) concerning the Amendment to Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, which specifically regulates the status of electronic evidence. Article 5 paragraph (1) of Law Number 1 of 2024 (UU, 2024) concerning the Amendment to Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions states that “electronic information and/or electronic documents and/or their printouts constitute valid legal evidence.” This provision expands and supplements the types of valid evidence that were previously not explicitly regulated in Law Number 20 of 2025 concerning the Amendment to Law Number 8 of 1981 concerning the Criminal Procedure Code.

All of this is supported by comprehensive forensic analysis results. The urgent nature of this research arises from the fact that cases of false news dissemination are difficult to resolve without valid digital evidence, which is essential for identifying perpetrators and uncovering dissemination mechanisms across various digital platforms. This process is fully aligned with the national legal framework, namely Article 184 on types of evidence in Law Number 20 of 2025 concerning the Amendment to Law Number 8 of 1981 concerning the Criminal Procedure Code (U. Indonesia & Indonesia, 1945), Article 186 concerning expert testimony in Law Number 1 of 2023 concerning the Amendment to Law Number 1 of 1946 concerning the Criminal Code (Presiden Republik Indonesia, 2023), and Regulation of the Chief of the Indonesian National Police Number 8 of 2014 concerning the Amendment to Regulation of the Chief of the Indonesian National Police Number 10 of 2010 concerning Procedures for Managing Evidence within the Indonesian National Police (K. N. R. I. Indonesia, 2025), which regulates professional procedures for managing digital evidence.

In 2023, Polresta Cirebon investigated the dissemination of a fabricated video on WhatsApp and Instagram falsely claiming that a local government official had committed financial fraud. The video had been manipulated using basic editing software and triggered public unrest. Investigators conducted a digital forensic examination of the suspect’s smartphone following lawful seizure and judicial authorization. Data imaging and metadata analysis revealed that the original file was created on the suspect’s device, with timestamps confirming that editing occurred hours before initial dissemination. Account traceability through formal requests to Meta Indonesia confirmed that the content originated from the suspect’s Instagram account. Log analysis documented dissemination across multiple WhatsApp groups. The suspect was charged under Article 28(1) of the ITE Law No. 1/2024. Notably, the investigation was constrained by delays in platform cooperation and the absence of dedicated forensic software at Polresta Cirebon, requiring referral to the Regional Cyber Crime Investigation Unit (*Subdit Siber Polda Jabar*), illustrating the institutional capacity gap this study addresses.

Illustrative Case Study: False News Handling at Polresta Cirebon

The technical process follows a structured, multi-stage procedure aligned with international standards (NIST SP 800-86; SWGDE Guidelines): (1) Identification and Seizure devices are secured with proper judicial authorization to prevent remote wiping; (2) Data Imaging forensic copies are created using write-blocking tools, and hash values are generated; (3) Hash Verification MD5/SHA-256 comparisons are conducted to confirm data integrity; (4) Log Analysis system, application, and network logs are examined to reconstruct event timelines; (5) Account Traceability IP addresses and device identifiers are cross-referenced with platform records through bilateral data request mechanisms; (6) Transmission Chain Reconstruction content propagation is mapped through metadata, forwarding records, and network traffic analysis; (7) Cloud Data Retrieval formal requests via MLAT or platform cooperation mechanisms are initiated for overseas-hosted content; (8) Chain of Custody Preservation all evidence handling is documented in accordance with Perkap No. 8/2014 (K. N. R. I. Indonesia, 2025).

Technical Forensic Process in False News Investigations

Digital forensics establishes each constituent element of Article 28(1) of the ITE Law No. 1/2024 as follows: (1) Perpetrator Identity device seizure, data imaging, IP/MAC address extraction, and account traceability through platform requests, supported by hash verification (MD5/SHA-256) to ensure integrity; (2) Subjective Intent log analysis of device activity, search history, and communication patterns indicates deliberate dissemination, while metadata analysis supports inference of premeditation; (3) Dissemination Behavior transmission chain reconstruction maps content trajectories across platforms through forwarding logs, post histories, and server access logs; (4) Falsity of Information collaboration with domain experts and screenshot/video authentication confirms content inaccuracy or manipulation; (5) Resulting Damages OSINT techniques and platform engagement metrics are used to document real-world impact; (6) Chain of Custody strict documentation under Perkap No. 8/2014 ensures the admissibility of all evidence from collection through to courtroom presentation (K. N. R. I. Indonesia, 2025).

How Digital Forensics Proves the Elements of the False News Crime

In addition, digital forensics functions as a key reinforcement in the judicial process, especially when perpetrators deny or evade accusations. The use of digital evidence has begun to raise complex issues; however, the most fundamental concern is its authenticity and integrity, which determine whether such evidence can be trusted. To address this, an investigative process known as digital forensics has emerged. Digital forensics is an investigative method that applies scientific and technological principles to examine and analyze digital evidence. This discipline, which is part of the field of computer security, has developed rapidly alongside technological advancement. The digital forensic process identifies digital evidence from electronic systems, which is then analyzed so that it can become reliable and admissible evidence (Herman et al., 2024). By involving specialized forensic experts (such as experts in handwriting analysis, document examination, and digital data analysis) a strict verification process makes it possible to distinguish original evidence from material that has been manipulated or falsified. This not only ensures the validity of evidence in court but also limits opportunities for perpetrators to dispute established facts. Without the contribution of digital forensics, investigators' evidentiary position becomes weak, potentially obstructing justice and allowing perpetrators to escape responsibility.

In practice, digital forensics functions to assess the validity of electronic evidence in court. Based on the principle that "every piece of evidence speaks," digital forensic experts play a central role in making electronic evidence "speak" through reconstruction processes. This approach ultimately provides clarity in resolving cases during trial (Anggraeni & Salsabila, 2024). The role of digital forensics is crucial in revealing electronic evidence, considering that such evidence is vulnerable to modification or manipulation by perpetrators of information and electronic transaction–based crimes who attempt to erase their digital traces. As a result, the authenticity of such evidence is often questioned, creating difficulties for law enforcement officials in the evidentiary process before the court.

Nevertheless, as stated in official research interviews with Bripda Arman Yudiansyah and

Aiptu Dedi Cahyadi, the implementation of digital forensics still faces a number of concrete challenges. These include difficulties in accessing data from overseas servers protected by strict privacy regulations, perpetrators' ability to erase traces through anonymity or advanced encryption techniques, and the rapid dynamics of content changes on websites and online platforms that affect the validity of evidence. In cases involving electronic and digital media, proof becomes a complex challenge. Law enforcement officers in Indonesia often experience difficulties in prosecuting perpetrators in such cases due to obstacles in fulfilling the requirements of Indonesian criminal procedural law. However, although prosecuting digital crime perpetrators is important, expanding the scope and effectiveness of evidence handling is a necessary solution for law enforcement. In this context, digital forensics, as a scientific method, plays an important role in the process of proving criminal cases, and its position in Indonesian evidentiary law is a significant parameter. Digital forensics is not direct evidence but rather a method applied by experts to assist law enforcement officers in enforcing the law (Awaluddin & Mulyana, 2024). Although these challenges are significant, they can be addressed through appropriate technical strategies such as international collaboration and the use of lawful decryption tools, ensuring that evidence continues to meet admissibility standards in court.

Further research interview results identify limited human resources and digital forensic laboratory capacity as the main obstacles. The shortage of skilled personnel in digital forensics, technological limitations, and legal barriers, including the need for regulatory reform, may cause cybercrime to develop into a systemic threat that is difficult to control. Indonesia also needs a legal framework and investigative mechanism aligned with international standards, such as the Budapest Convention on Cybercrime, to prevent the country from becoming a weak point in the global security network (Wibowo & Munawar, 2024). Investigations of criminal offenses using electronic and digital media in Indonesia are often hindered by technical constraints, resulting in slow handling and inaccurate analysis of digital evidence. Such evidence is vulnerable to manipulation, deletion, or loss due to limited storage duration and therefore requires rapid response. However, its complexity across global platforms with high-security systems, especially foreign-based cloud and social media services, requires international cooperation that is difficult to obtain without bilateral legal agreements. In addition, the concentration of trained digital forensic investigators at the Regional Police level causes case handling at the Polres or Polsek level to be less than optimal, especially in crimes such as the dissemination of false news through electronic media. Infrastructure shortages (such as disk-imaging tools, advanced storage media readers, updated forensic software for various operating systems, and high-performance computing resources for encryption analysis) further weaken the ability to keep pace with increasingly sophisticated methods of digital crime.

Technological development and the complexity of cybercrime require an adaptive criminal justice system through coherent regulatory reform and the application of adaptive legality principles. Strengthening the competence of law enforcement officers, together with scientific procedures and technical certification, is a key prerequisite for the successful integration of digital forensics into the criminal justice system (Mursyid et al., 2025). Therefore, the presence of digital forensic experts is needed to reduce technology-based crime while providing legal support for the enforcement of justice through evidence obtained from electronic devices, digital data, and other related elements. This aims to obtain indications of truth in a case (Anneke Mawlidya, 2024).

The use of electronic evidence in judicial proceedings depends greatly on the understanding and skills of law enforcement officers (APH). Therefore, digital forensic training plays a crucial role in improving the quality of case handling, especially cases involving technology. The implementation of such training is highly necessary, particularly within police institutions as the front line of the criminal justice system. At the investigation stage, police officers who have received such training demonstrate improved ability in understanding, collecting, and analyzing electronic evidence more effectively and accurately. This advantage is reflected in their ability to identify digital traces using software appropriate to the characteristics of the evidence being analyzed (Cantika et al., 2025). The results of digital forensic analysis in court proceedings produce not only documentary evidence but also expert testimony. Digital forensic experts must understand computer science and legal procedures recognized nationally

and internationally. In addition, they must have experience in relevant theories related to digital evidence and master forensic software or applications so that digital evidence can be examined accurately and precisely (Medeline et al., 2022).

Based on these findings, this study recommends systematic capacity-strengthening measures. First, the establishment of national standards and binding regulations governing the use of forensic technology and digital evidence. Second, strengthening the competence of investigators and forensic technicians so that they not only operate tools but also understand procedures and ethical aspects, along with establishing digital forensic investigation teams at every level of the police (from Polres to Polsek) through training and international-standard certification such as ISO/IEC 17024. Third, increasing the number of ISO/IEC 17025-accredited digital forensic laboratories in various regions to support fast and accurate analysis, as well as developing audit mechanisms and digital evidence documentation systems that are transparent to supervisory institutions and the public to ensure investigative accountability. Fourth, formulating standardized technical regulations on the collection, management, and analysis of digital evidence, including strict emphasis on the chain of custody to maintain evidence integrity. Fifth, procuring complete equipment such as specialized hardware for encryption analysis, digital content verification, and access to global server data (Parawangsa et al., 2025). The implementation of these recommendations is expected to improve investigative effectiveness, strengthen evidentiary value in accordance with Law Number 1 of 2024 (UU, 2024) concerning the Second Amendment to Law Number 19 of 2016, which amends Law Number 11 of 2008 concerning Electronic Information and Transactions, as well as Law Number 1 of 1946 concerning the Criminal Code, and minimize opportunities for perpetrators to deny wrongdoing, thereby supporting fairer and more efficient digital law enforcement.

Sixth, the establishment of a dedicated cross-platform data retrieval mechanism through bilateral MLAT agreements and direct platform cooperation, enabling timely access to server data held by overseas social media providers. Seventh, the formalization of a national certified expert witness registry for digital forensics accessible to Polres units lacking in-house expertise.

CONCLUSION

This study concludes that digital forensics has high urgency as a primary evidentiary instrument in investigating the criminal offense of disseminating false news, as confirmed through interviews with Bripda Arman Yudiansyah and Aiptu Dedi Cahyadi. The findings show that digital evidence, such as physical devices (smartphones, laptops, and flash drives) and data (photos, videos, and files), is strengthened by comprehensive forensic analysis, which aligns with the national legal framework, including Article 5 of Law Number 1 of 2024 concerning the Amendment to Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Articles 184 and 186 of Law Number 20 of 2025 concerning the Amendment to Law Number 8 of 1981 concerning the Criminal Procedure Code, and Regulation of the Chief of the Indonesian National Police Number 8 of 2014 concerning the Amendment to Regulation of the Chief of the Indonesian National Police Number 10 of 2010 concerning Procedures for Managing Evidence within the Indonesian National Police. Digital forensics not only strengthens the validity of evidence in court by ensuring integrity and authenticity but also facilitates perpetrator identification and reconstruction of the crime mechanism, in accordance with the principle that “every evidence can speak.”

Implementation remains constrained by cross-border server access restrictions, advanced encryption, limited trained personnel at the Polres/Polsek level, and insufficient laboratory infrastructure. This study therefore recommends: (1) specific binding digital forensic regulations with standardized SOPs; (2) ISO/IEC 17024-certified forensic units at every Polres level; (3) ISO/IEC 17025-accredited regional laboratories; (4) ISO/IEC 27037 standards for digital evidence management; (5) cross-platform MLAT-based data retrieval mechanisms; and (6) a national registry of certified digital forensic expert witnesses. These measures are expected to substantially improve the effectiveness and fairness of ITE Law enforcement in addressing false news dissemination in Indonesia.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Universitas Swadaya Gunung Jati, Cirebon, for their academic support and research facilities that contributed to the completion of this study. Appreciation is also extended to the Cirebon Police Resort and relevant stakeholders for their assistance and insights related to digital forensic investigations in cases involving the dissemination of false news.

AUTHOR CONTRIBUTION STATEMENT

Nur Abida Yasvin contributed to the conceptualization, data collection, legal analysis, and drafting of the original manuscript. Waluyadi contributed to supervision, methodological guidance, critical review, and validation of the research findings. Both authors collaboratively developed the research framework, revised the manuscript, and approved the final version, taking full responsibility for the integrity and accuracy of the study.

REFERENCES

Ahadiyah, F. N. (2024). Perkembangan Teknologi Infomasi Terhadap Peningkatan Bisnis Online. *INTERDISIPLIN: Journal of Qualitative and Quantitative Research*, *1*(1), 41–49.

Anggraeni, D. R., & Salsabila, M. (2024). Analisis yuridis peran digital forensik dalam pembuktian tindak pidana di Indonesia. *Media Hukum Indonesia (MHI)*, *2*(2).

Anneke Mawlidya. (2024). Penerapan Digital Forensik Dalam Mengidentifikasi Pelaku Penipuandan Peran Digital Forensik Sebagai Alat Bukti. *Causa: Jurnal Hukum Dan Kewarganegaraan*, *5*(8), 1–10. https://doi.org/Prefix doi.org/10.3783/causa.v2i9.2461

Awaluddin, F., & Mulyana, M. (2024). Tantangan dan peran digital forensik dalam penegakan hukum terhadap kejahatan di ranah digital. *Humaniorum*, *2*(1), 14–19.

Cantika, G., Yunara, E., & Trisna, W. (2025). Kebijakan hukum pidana terhadap bukti elektronik: Antara eksistensi, hambatan penggunaan, dan urgensi pengaturannya dalam kitab undang-undang hukum acara pidana. *Acta Law Journal*, *3*(2), 103–125.

Haidarrani, A., Hairani, J., Mubarokah, W., & Sulistianingsih, D. (2024). Pertanggungjawaban pidana pelaku forward berita hoax: Telaah dalam perspektif Undang-Undang ITE. *Bookchapter Hukum Dan Politik Dalam Berbagai Perspektif*, *3*, 76–120.

Herman, Handrawan, Hari, O. K., Abdullah, S. A., Rizky, A., & Indah, S. R. (2024). Penggunaan Digital Forensik dalam Pembuktian Tindak. *Halu Oleo Legal Research*, *6*(2), 588–603.

Indonesia, K. N. R. I. (2025). *Peraturan Perundang-undangan*. *2*, 306–312.

Indonesia, U., & Indonesia, U. (1945). Tahun 1945 (1945). *Jakarta: UUD*, *116287*.

Medeline, F., Rusmiati, E., & Ramadhani, R. H. (2022). Forensik Digital dalam Pembuktian Tindak Pidana Ujaran Kebencian di Media Sosial. *PAMPAS: Journal of Criminal Law*, *3*(3), 310–325.

Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi peran digital forensik dalam penyidikan tindak pidana siber: Analisis kritis terhadap konstruksi hukum pidana di Indonesia. *Jurnal Tana Mana*, *6*(2), 289–296.

Parawangsa, A. N. I., Putri, C. R., & Wahyuningbudi, A. J. (2025). Pengaruh Penggunaan Teknologi Forensik Terhadap Akurasi Identifikasi Tersangka Dalam Proses Penyidikan. *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, *2*(1), 132–141.

Presiden Republik Indonesia. (2023). Undang-undang Republik Indonesia Nomor 1 Tahun 2023 Tentang Kitab Undang-Undang Hukum Pidana. *Direktorat Utama Pembinaan Dan Pengembangan Hukum Pemeriksaan Keuangan Negara Badan Pemeriksa Keuangan*, *16100*, 1–345.

Rachmie, S. (2020). Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website. *Litigasi*, *21*(1), 104–127.

Rahmadina, N. A., & Tornado, A. S. (2026). Analisis Hukum Pembuktian Digital Forensik Dalam Tindak Pidana Cyber Crime. *Iuris Studia: Jurnal Kajian Hukum*, *7*(2), 487–500.

Sanusi, S., Maulida, I., & Putri, D. I. (2024). Penegakan Hukum Dalam Tindak Pidana Penipuan Penawaran Kerja Berbasis Media Elektronik (Whatsapp). *Hukum Dan Masyarakat Madani*, *14*(1), 133–143.

Saputra, A. P. (2017). Analisis Digital Forensik pada File Steganography (Studi kasus: Peredaran Narkoba). *Jurnal Teknik Informatika Dan Sistem Informasi*, *3*(1).

UU. (2016). Undang-undang (UU) Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. In *Undang-Undang 19 Tahun 2016* (Vol. 44, Issue 8, p. 287).

UU. (2024). Undang-Undang (UU) RI Nomor 1 Tahun 2024. *Journal of Physics A: Mathematical and Theoretical*, *44*(8), 287.

UU. (2004). Undang-undang (UU) Nomor 19 Tahun 2004 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2004 tentang Perubahan atas Undang-Undang Nomor 41 Tahun 1999 tentang Kehutanan Menjadi Undang-Undang.

Waluyadi, W., & Leliya, L. (2022). Cara praktis menulis skripsi dan tesis ilmu hukum. *Yogyakarta: Deepublish*.

Wibowo, M. S. I., & Munawar, A. (2024). Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia. *Jurnal Hukum Lex Generalis*, *5*(7).