Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon
Volume: 05
Issue: 06
Year: 2025
Page: 2987-2998

Citation:
Chamim, M., Widodo, K., Riyadi, S., Achyarsyah, P., & Faisal. (2025). The role of digital evidence in criminal law enforcement: Challenges of authentication and admissibility in court. *Research Horizon*, *5*(6), 2987-2998.

Article History:
Received: September 12, 2025
Revised: October 19, 2025
Accepted: November 15, 2025
Online since: December 31, 2025

The Role of Digital Evidence in Criminal Law Enforcement: Challenges of Authentication and Admissibility in Court

Mochammad Chamim[1], Kusno Widodo[1], Sugeng Riyadi[1], Padri Achyarsyah[1*], Faisal[1]

[1] Universitas Wahid Hasyim, Semarang, Indonesia

[*] *Corresponding author: Padri Achyarsyah (pachyarsyah@gmail.com)*

Abstract

Digital evidence has become a crucial element in modern criminal law enforcement in Indonesia, particularly in addressing cybercrimes such as online gambling, online fraud, and data theft. This study aims to analyze the legal standing of digital evidence, the challenges of its authentication and admissibility in court, and strategies to ensure its reliability in the judicial process. The study uses a normative juridical method with descriptive analysis through statutory and conceptual approaches, based on a study of legal regulations, court decisions, academic literature, and digital forensic guidelines. The results show that digital evidence has been legally recognized through the Criminal Procedure Code (KUHAP), the ITE Law, and Supreme Court regulations, as long as its authenticity and integrity can be proven. However, major challenges remain, including the potential for data manipulation, limited infrastructure, and a lack of competent human resources. Efforts to ensure the reliability of digital evidence include the implementation of standard forensic procedures, capacity building of law enforcement officers, cross-agency collaboration, the use of advanced technology, and strengthening an adaptive legal framework to support effective law enforcement and public trust.

Keywords

Admissibility, Authentication, Cybercrime, Digital Evidence, Forensic Reliability.

1. Introduction

The development of information technology has changed the landscape of criminal law enforcement in Indonesia, particularly with the emergence of digital evidence as a crucial element in the judicial process. Digital evidence, which includes electronic data from devices such as computers, smartphones, social media, online transactions, and Internet of Things (IoT) devices, has become a crucial tool in the investigation and trial of cybercrime cases, including online gambling (Handoko et al., 2015; Aini & Lubis, 2024; Maryam et al., 2024). In Indonesia, the legal framework governing digital evidence is contained in Article 184 of the Criminal Procedure Code (*Kitab Undang Undang Hukum Pidana*/KUHAP), Article 5 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions (*Undang Undang Informasi dan Transaksi Elektronik*/UU ITE), and Supreme Court Regulation No. 1 of 2019 concerning Guidelines for the Examination of Information Technology-Based Criminal Cases (Lasmadi, 2014; Hartono & Yuliartini, 2020). Furthermore, international standards such as the Budapest Convention on Cybercrime (2001) provide guidelines for the collection and authentication of digital evidence in the context of transnational law enforcement (Fahamsyah et al., 2022).

However, the use of digital evidence in the criminal justice system faces significant challenges, particularly regarding authentication (authenticity) and admissibility (admissibility in court). Digital evidence is vulnerable to manipulation, deletion, or falsification, making it difficult for law enforcement to ensure its integrity (Riskiyadi, 2020; Wiarti, 2023; Mursyid et al., 2025). The lack of specific regulations regarding digital forensic procedures in the Criminal Procedure Code, the limited technical capacity of law enforcement officials, and the complexity of transjurisdictional cybercrime are major obstacles (Rahmanto et al., 2019; Awaluddin & Mulyana, 2024). For example, in online gambling cases, digital forensics plays a crucial role in tracing the flow of funds and illegal content, but challenges such as perpetrator anonymity and the use of encryption technology often hamper the investigation process (Mokobombang et al., 2023; Maryam et al., 2024). Furthermore, cybercrimes such as online fraud and money laundering demonstrate the need for stronger authentication standards to ensure digital evidence is admissible in court (Dewi et al., 2023; Munajat & Yusuf, 2024).

An analysis of various previous studies reveals significant research gaps. First, most studies focus on the normative aspects of positive law, such as the recognition of digital evidence in the ITE Law and the Criminal Procedure Code (KUHAP) but lack a thorough understanding of its practical implementation in court, particularly regarding digital forensic authentication standards (Helmawansyah, 2021; Sucia & Deswari, 2024). Second, previous studies tend to analyze cybercrime in general without specifically examining the challenges of digital evidence admissibility in specific cases, such as online gambling, which has unique characteristics, including cross-border transactions and perpetrator anonymity (Zaenudin & Faridah, 2022; Riston & Basoddin, 2025). Third, the lack of studies integrating digital forensic technical approaches with the criminal procedural legal framework has led to a shortage of practical solutions to address inconsistencies in judges' assessments of digital evidence (Anggraeni & Salsabila, 2024; Sirait, 2025). Therefore, this study aims to fill this gap by analyzing the legal status of digital evidence, the challenges of its authentication and admissibility, and formulating a digital forensics-based strategy to improve the effectiveness of criminal law enforcement in Indonesia, particularly in the context of cybercrimes such as online gambling. Based on this, this study formulates problems that focus on three main aspects, namely the legal status and recognition of digital evidence in the criminal justice system in Indonesia, the challenges faced in the process of authenticating and proving the admissibility of digital evidence in court, and strategies and best practices that can be applied to

ensure the reliability of digital evidence in the criminal justice process. These problems are important to study to ensure that the use of digital evidence is not only recognized normatively but also applied effectively, accountably, and in accordance with the principles of justice in law enforcement practices.

2. Methods

This research employs a normative juridical method with descriptive analysis, aiming to comprehensively describe the legal status, challenges, and best practices in the use of digital evidence in the Indonesian criminal justice system, particularly in handling cybercrimes such as online gambling. The normative juridical method was chosen because this research focuses on the study of legal norms, principles, and legal doctrines governing criminal evidence amidst the development of information technology. Descriptive analysis is used to describe the empirical conditions of the application of digital evidence as reflected in regulations, court decisions, and law enforcement practices.

The research approach employed includes a statistical approach and a conceptual approach. The statutory approach is conducted by examining relevant legal provisions, including the Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law (UU ITE) and its amendments, and Supreme Court regulations governing the use and examination of digital evidence in criminal proceedings. This approach aims to assess the consistency and adequacy of legal regulations regarding the recognition, evidentiary strength, and formal and material requirements of digital evidence. A conceptual approach is used to understand and analyze the theory of evidence in criminal law, the principles of digital data authentication and integrity, the concept of chain of custody, and the criteria for admissibility of digital evidence in court. This approach is crucial for linking legal norms with developments in digital forensic techniques and evidentiary practices in cybercrime cases.

Research data was obtained through a literature review by examining primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations and court decisions related to the use of digital evidence, particularly in cybercrime cases. Secondary legal materials consist of books, scientific journals, and relevant research results, while tertiary legal materials include legal dictionaries and other supporting sources. Furthermore, digital forensic technical guidelines were used as references to understand digital evidence authentication standards and procedures. Data analysis was conducted qualitatively and descriptively by inventorying, classifying, and interpreting the obtained legal data. The results of the analysis are presented systematically to provide a comprehensive understanding of the application of digital evidence in Indonesian criminal law proceedings, as well as the challenges and efforts to strengthen it.

3. Results and Discussion

3.1. Legal Status and Recognition of Digital Evidence

The development of information technology has significantly transformed the criminal justice system, especially in the process of criminal evidence. In Indonesia, digital evidence has become an essential tool in uncovering modern crimes such as online gambling, online fraud, illegal content distribution, and personal data theft. Criminal activities are no longer carried out only through physical means but increasingly rely on electronic devices, online platforms, and internet networks. This situation requires the Indonesian criminal justice system to adapt by providing legal instruments that recognize and regulate digital evidence.

The main legal basis for the recognition of digital evidence in Indonesia is Law Number 19 of 2016, which amends Law Number 11 of 2008 on Electronic

Information and Transactions (ITE Law). Article 5 paragraph (1) of the ITE Law clearly states that electronic information and/or electronic documents, including their printed versions, are valid legal evidence. Article 5 paragraph (2) further confirms that electronic evidence has the same evidentiary value as conventional evidence under criminal procedural law, allowing its use in civil, administrative, and criminal cases.

This regulation represents an important step in the modernization of evidentiary law in Indonesia. Before the enactment of the ITE Law, criminal proceedings mainly relied on the Criminal Procedure Code (KUHAP). Article 184 paragraph (1) of KUHAP recognizes only five types of legal evidence: witness testimony, expert testimony, documents, indications, and defendant testimony. Since KUHAP was drafted in 1981, when information technology was still limited, it did not specifically regulate electronic evidence. The ITE Law therefore provides legal certainty regarding the position of digital evidence.

In judicial practice, electronic data may function as documentary evidence or indicative evidence, depending on its nature and use. Digital conversation screenshots, electronic transaction records, and online communication logs may be classified as documentary evidence if they meet the requirements of authenticity and relevance. When such data is used to draw conclusions about a sequence of criminal events, it may be treated as indicative evidence. This interpretation expands the scope of evidence under KUHAP without violating its fundamental principles.

The recognition of digital evidence is also supported by judicial decisions, particularly Supreme Court Decision Number 1832 K/Pid/2019. The Court confirmed that digital evidence obtained from electronic media is admissible in criminal proceedings as long as its authenticity can be proven and the chain of custody is properly maintained (Sirait, 2025). This decision shows that digital evidence is not only recognized normatively but also applied in judicial practice.

In addition, the Supreme Court has issued regulations that strengthen the use of digital evidence. Supreme Court Regulation (*Peraturan Mahkamah Agung*/Perma) Number 1 of 2019 on Guidelines for the Examination of Information Technology-Based Criminal Cases provides direction for judges in handling cases involving electronic evidence. Although earlier regulations, such as Perma Number 7 of 2016, focused on electronic civil cases, their principles on authentication, security, and electronic document management remain relevant for criminal cases.

From a philosophical perspective, the recognition of digital evidence reflects the principle of equality before the law, which requires all relevant evidence to be treated equally regardless of its physical form. As long as digital evidence can establish a connection between the offender and the crime and meets the principles of authenticity, integrity, and relevance, it is legally valid. This principle supports the modernization of the evidentiary system to respond to technological developments.

The acceptance of digital evidence also shows a shift in Indonesia's legal system toward a technology-based evidentiary approach. Academic studies describe the ITE Law as a form of legal adaptation to technological progress (Lasmadi, 2014; Handoko et al., 2015; Sucia & Deswari, 2024). Research by Mantik (2022) and Hartono & Yuliartini (2020) further indicates that digital evidence, such as emails, CCTV recordings, electronic transaction data, and online communications, is commonly used in criminal trials.

Furthermore, Article 43 paragraph (2) of the ITE Law provides a legal basis for the investigation and prosecution of information technology-related crimes by regulating procedures for collecting, storing, and presenting electronic data. This provision strengthens the role of digital evidence at all stages of the criminal justice process, from investigation to trial (Rahmanto et al., 2019; Zaenudin & Faridah, 2022).

At the international level, the recognition of digital evidence is influenced by the Budapest Convention on Cybercrime (2001), which encourages the adoption of global standards for handling digital evidence. Although Indonesia has not ratified the Convention, its principles are often used as references in legal policies and investigative guidelines, especially regarding data interoperability and electronic evidence verification (Fahamsyah et al., 2022).

At the national level, law enforcement institutions such as the Indonesian National Police, the Attorney General's Office, and the National Cyber and Crypto Agency have issued internal guidelines to support the lawful use of digital evidence. Although administrative in nature, these guidelines play an important role in ensuring the legitimacy of digital evidence and maintaining procedural fairness.

In conclusion, digital evidence has been formally recognized and has strong legal legitimacy within Indonesia's criminal justice system. This recognition is supported by the ITE Law, interpretations of KUHAP, Supreme Court decisions, and implementing regulations. Digital evidence has therefore become an integral part of the criminal evidentiary system, reflecting the state's commitment to legal adaptation in order to uphold justice, legal certainty, and public benefit in the digital era (Al Faraby, 2024; Budianto, 2025).

3.2. Challenges of Authentication and Admissibility of Digital Evidence

Authentication and admissibility are fundamental aspects in assessing the validity of digital evidence in court. Although Indonesian law formally recognizes electronic evidence, the main challenge lies in ensuring that such evidence is authentic, intact, and legally admissible. The inherent characteristics of digital data easily altered, duplicated, or deleted pose serious risks to the integrity of the judicial process. Consequently, authentication and admissibility require not only technical accuracy but also methodological caution to preserve fairness and legal certainty.

Authentication refers to the verification process ensuring that electronic data originates from a legitimate source, has not been manipulated, and maintains its integrity from acquisition to presentation in court. Within the criminal justice system, authentication is a prerequisite for evidentiary reliability. However, digital data is volatile and can be modified without leaving visible traces, making authentication particularly challenging (Riskiyadi, 2020; Aini & Lubis, 2024). In online fraud cases, for example, electronic messages, transaction logs, and digital communications are highly susceptible to manipulation and therefore require forensic verification.

To ensure authenticity, investigators must use specialized forensic tools such as Forensic Toolkit (FTK) Imager, which allows data acquisition without altering the original evidence (Riskiyadi, 2020; Maryam et al., 2024). Nevertheless, technical limitations often hinder this process, particularly when data is protected by advanced encryption systems such as BitLocker. In such cases, investigators may be unable to access encrypted data fully, significantly obstructing evidentiary efforts.

Beyond technical matters, authentication reliability depends heavily on maintaining a proper chain of custody. The chain of custody refers to documented control over evidence from collection through courtroom presentation (Hartono & Yuliartini, 2020; Mantik, 2022). Every handling and transfer of digital evidence must be recorded to prevent unauthorized alteration. Even minor procedural inconsistencies may undermine the credibility of the evidence and lead courts to question its authenticity.

Errors frequently occur when investigators or expert witnesses access data without adhering to forensic protocols, potentially altering metadata or file structures (Mantik, 2022; Sirait, 2025). Such procedural lapses can render otherwise valid evidence unreliable before the court. These challenges are amplified in regions with limited forensic infrastructure, particularly outside Java. In areas such as Sumatra, investigators often rely on private forensic services, raising concerns about

objectivity, standardization, and data security (Dhiya, 2025; Riston & Basoddin, 2025).

Human resource limitations further exacerbate authentication challenges. Many law enforcement officers lack sufficient technical expertise in digital data extraction, analysis, and verification (Awaluddin & Mulyana, 2024; Rohman et al., 2024). This deficiency increases the risk of procedural errors or data loss during investigations. Therefore, digital evidence authentication is not merely a technological issue but also reflects institutional readiness and professional capacity.

Data integrity is inseparable from authentication. Any alteration intentional or accidental can significantly reduce evidentiary value. Consequently, documentation of data collection, storage, and analysis must be systematic and transparent. Challenges arise when law enforcement agencies lack uniform technical guidelines to safeguard evidence integrity, leaving room for potential manipulation (Hartono & Yuliartini, 2020).

In practice, chain of custody documentation is often incomplete. In cybercrime cases involving server logs or mobile phone data, evidence is frequently transferred between agencies without formal digital records. These gaps provide opportunities for defense counsel to challenge authenticity (Mantik, 2022; Sirait, 2025), ultimately weakening prosecutorial credibility.

Another critical issue concerns the limited infrastructure for secure digital evidence storage. In some regions, evidence is still stored on conventional media without layered security systems, increasing risks of data loss, physical damage, or unauthorized modification (Dhiya, 2025). Thus, safeguarding digital evidence integrity requires equal attention alongside authentication procedures.

Following authentication, admissibility becomes the next legal challenge. Admissibility concerns whether judges accept and consider digital evidence as legally valid. Although Article 5 paragraph (1) of the ITE Law explicitly recognizes electronic information and documents as valid legal evidence, the Criminal Procedure Code (KUHAP) does not provide specific procedural standards for digital authentication. As a result, judicial assessments of digital evidence often vary and remain inconsistent (Lestari & Damayanti, 2018; Mursyid et al., 2025).

In many cases, judges rely heavily on digital forensic expert testimony to understand technical processes such as hashing, metadata verification, and data acquisition. In cases involving voice recordings, transaction logs, or mobile phone data, expert explanations are crucial for judicial evaluation (Wicaksono et al., 2020; Zaenudin & Faridah, 2022). However, the limited number of qualified experts often delays proceedings.

Admissibility challenges become more complex in cross-jurisdictional cybercrime cases. Digital evidence is frequently stored on overseas servers, requiring international cooperation. Indonesia has not fully adopted international standards such as the Budapest Convention on Cybercrime, which governs cross-border electronic evidence handling (Fahamsyah et al., 2022; Mokobombang et al., 2023). Consequently, courts may hesitate to admit foreign-sourced evidence due to differing authentication standards.

At the domestic level, inconsistent judicial interpretations further complicate admissibility. Some judges require comprehensive forensic verification for all digital evidence, while others accept simpler technical proof (Maryam et al., 2024; Sucia & Deswari, 2024). This inconsistency highlights the absence of a comprehensive national Standard Operating Procedure (SOP) governing digital evidence.

Institutional and perceptual factors also influence admissibility. Not all judges possess sufficient understanding of digital forensic concepts, encryption mechanisms, data formats, or hash-based authentication (Helmawansyah, 2021; Al Faraby, 2024). Consequently, digital evidence is sometimes regarded as

supplementary rather than primary, despite its central role in modern crimes such as cybercrime, corruption, and money laundering (Dewi et al., 2023; Putra, 2024).

Thus, challenges surrounding the authentication and admissibility of digital evidence in Indonesia involve interconnected technical, procedural, and institutional dimensions. Authentication demands rigorous verification and integrity safeguards, while admissibility depends on consistent procedures and judicial comprehension. Limitations in human resources, forensic infrastructure, and standardized regulations widen the gap between technological advancement and legal readiness. Strengthening technical capacity, enforcing chain-of-custody standards, and enhancing digital literacy among judicial actors are therefore essential to ensure that digital evidence functions as a credible and reliable instrument within Indonesian criminal courts.

3.3. Strategies and Practices for Ensuring the Reliability of Digital Evidence

The reliability of digital evidence constitutes a fundamental pillar of criminal proof in the digital era. Electronic evidence derived from devices, networks, and online platforms can only be legally recognized if its authenticity and integrity are assured. Accordingly, consistent strategies and best practices in the collection, storage, and analysis of digital evidence must be applied in line with international forensic standards to preserve evidentiary value.

A core strategy for ensuring reliability is the strict application of standardized forensic procedures at every stage of evidence handling. These procedures include identifying digital data sources, acquiring evidence using forensic methods, analyzing the data, and securely storing the results. Comprehensive documentation is mandatory at each phase, including details on time, location, and acquisition methods. To safeguard integrity, each digital file must be accompanied by a hash value, which functions as a digital fingerprint to verify that the data has not been altered from acquisition to courtroom presentation. This mechanism serves as objective proof of data authenticity and integrity.

Human resource capacity is equally crucial. Continuous training for investigators, prosecutors, and judges is necessary to ensure understanding of digital authentication, data integrity, and forensic auditing methods. Such training helps minimize procedural errors and enhances the objective evaluation of digital evidence (Hartono & Yuliartini, 2020; Wiarti, 2023). In practice, officers must comprehend the four main parameters of digital evidence accessibility, visibility, integrity, and accountability which serve as benchmarks for evidentiary admissibility.

Capacity building should also include specialized investigative techniques for cyber-related crimes such as e-commerce fraud, hacking, and online intellectual property violations (Rahmanto et al., 2019; Aini & Lubis, 2024). Cross-institutional collaboration strengthens this effort. Cooperation between investigators and digital forensic experts has proven effective, for example, in uncovering online trafficking of protected wildlife (Maryam et al., 2024; Dhiya, 2025). Such collaboration enhances technical accuracy while ensuring evidence is handled by qualified and impartial experts.

The strict application of the chain-of-custody principle is another essential measure. This principle requires comprehensive records of who accessed the evidence, when, and for what purpose. Every transfer of digital evidence must be formally documented to prevent unauthorized intervention. The implementation of secure digital documentation systems, hash verification, and routine audits significantly strengthens custody control and helps detect any data alteration (Handoko et al., 2015; Mursyid et al., 2025).

At the international level, cooperation is vital when digital evidence is stored beyond national jurisdictions. The Budapest Convention on Cybercrime provides a framework for cross-border access to electronic data while upholding the principle of aut dedere aut judicare (Fahamsyah et al., 2022; Mokobombang et al., 2023).

Although not yet ratified by Indonesia, alignment with its principles supports harmonization of forensic standards and strengthens the handling of transnational digital evidence.

Technological advancement also plays a critical role in enhancing evidentiary reliability. Digital forensic tools such as FTK Imager and Autopsy enable effective data acquisition, analysis, and recovery of deleted files (Riskiyadi, 2020; Wicaksono et al., 2020). Additionally, advanced voice recognition techniques using Itakura Saito Distance and neural networks can achieve accuracy rates exceeding 95%, strengthening the objectivity of voice-based evidence (Wicaksono et al., 2020; Awaluddin & Mulyana, 2024). Institutional integration of digital forensic standards into law enforcement operational guidelines is equally important. Uniform procedures across police, prosecutors, and courts ensure consistency in evidence handling. Proposals to establish national forensic standards integrating digital forensics into the criminal justice system, as suggested by Rohman et al. (2024) and Anggraeni & Salsabila (2024), represent significant steps toward accountability and standardization.

Emerging technologies such as Artificial Intelligence (AI) and big data analytics further strengthen the reliability of digital evidence. These tools enable real-time detection of suspicious activities, particularly in cases of money laundering and corruption (Munajat & Yusuf, 2024; Putra, 2024). AI-assisted analysis helps identify transactional patterns and relationships among devices, perpetrators, and online activities, thereby enhancing evidentiary completeness. The adoption of e-Court systems also supports reliability by enabling electronic submission and verification of evidence (Dewi et al., 2023; Pradipa, 2025). However, effective implementation requires adequate technical capacity among legal practitioners and collaboration with professional institutions such as the Indonesian Digital Forensics Association (Awaluddin & Mulyana, 2024; Budianto, 2025).

Public education constitutes an additional strategic element. Increased digital literacy helps the public preserve electronic data, report cybercrime effectively, and maintain evidentiary records (Zuhri & Fadil, 2024; Al Faraby, 2024). This preventive approach strengthens societal participation in safeguarding judicial integrity. Regular independent audits and evaluations are essential to maintain system relevance and responsiveness to technological developments. Through continuous assessment, weaknesses can be identified and corrected before undermining evidentiary credibility.

The reliability of digital evidence depends on the synergy between advanced technology, skilled human resources, and an adaptive legal framework. By implementing standardized procedures, strengthening institutional capacity, and fostering cooperation at national and international levels, Indonesia can ensure that digital evidence functions as a credible and legitimate instrument in combating cybercrime (Lestari & Damayanti, 2018; Pahrudin, 2020; Zaenudin & Faridah, 2022; Mantik, 2022).

4. Conclusion

Digital evidence has become a crucial component of criminal law enforcement in Indonesia, particularly in addressing technology-based crimes such as online gambling, online fraud, and cybercrime. The main findings indicate that the legal status and recognition of digital evidence have gained strong legitimacy under the Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law (UU ITE), as well as Supreme Court regulations and decisions, provided that the principles of authenticity and data integrity are met. This directly addresses the research objectives regarding legal certainty and the equal status of digital evidence within the criminal justice system.

The implications of these findings reveal that despite clear normative recognition, significant challenges remain in the authentication and admissibility of digital evidence due to limited infrastructure, insufficient technical expertise, and procedural inconsistencies. Therefore, this study recommends strengthening digital forensic standards, improving the technical competence of law enforcement officials, and optimizing the use of advanced technologies such as artificial intelligence and e-Court systems. Future research is encouraged to adopt an empirical approach to examine courtroom practices in digital evidence assessment to evaluate consistency, effectiveness, and the practical impact of existing legal and forensic frameworks.

References

Aini, N., & Lubis, F. (2024). Tantangan pembuktian dalam kasus kejahatan siber. *Judge: Jurnal Hukum*, *5*(2), 55–63.

Al Faraby, A. H. (2024). Perkembangan teknologi informasi dan transaksi elektronika (ITE) di Indonesia (Suatu kajian dari peran penyidik kepolisian dalam menangani penyalahgunaan informasi dan transaksi elektronika). *Meraja Journal*, *7*(1), 48–62.

Anggraeni, D. R., & Salsabila, M. (2024). Analisis yuridis peran digital forensik dalam pembuktian tindak pidana di Indonesia. *Media Hukum Indonesia (MHI)*, *2*(2), 101–115.

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

Budianto, T. Y. A. (2025). Peran digital forensik dalam penegakan hukum terhadap kejahatan konvensional. *Lex Progressium: Jurnal Kajian Hukum dan Perkembangan Hukum*, *2*(1), 45–55.

Dewi, G. V., Fitria, A., Anjasmara, R., & Enggarsasi, U. (2023). Peran digital evidence dalam kasus money laundering. *Jurnal Risalah Kenotariatan*, *4*(2), 89–102.

Dhiya, A. (2025). *Peranan digital forensik dalam penyidikan tindak pidana perdagangan satwa dilindungi oleh penyidik pegawai negeri sipil* (Disertasi doktoral). Universitas Andalas.

Fahamsyah, E., Taniady, V., Rachim, K. V., & Riwayanti, N. W. (2022). Penerapan prinsip *aut dedere aut judicare* terhadap pelaku cybercrime lintas negara melalui ratifikasi Budapest Convention. *Jurnal Hukum dan Syariah De Jure*, *14*(1), 1–18.

Handoko, C., Surbakti, S. H. N., Kurnianingsih, S. H. M., & MH, M. K. (2015). *Kedudukan alat bukti digital dalam pembuktian cyber crime di pengadilan* (Disertasi doktoral). Universitas Muhammadiyah Surakarta.

Hartono, M. S., & Yuliartini, N. P. R. (2020). Penggunaan bukti elektronik dalam peradilan pidana. *Jurnal Komunikasi Hukum*, *6*(1), 281–302.

Helmawansyah, M. (2021). Penggunaan barang bukti elektronik yang dijadikan alat bukti dalam perkara pidana. *Journal of Law (Jurnal Ilmu Hukum)*, *7*(2), 527–541.

Lasmadi, S. (2014). Pengaturan alat bukti dalam tindak pidana dunia maya. *Jurnal Ilmu Hukum Jambi*, *5*(2), 43–57.

Lestari, A. D., & Damayanti, M. (2018). Cakupan alat bukti sebagai upaya pemberantasan kejahatan siber. *Al-Ahkam: Jurnal Ilmu Syari'ah dan Hukum*, *3*(1), 47–68.

Mantik, V. (2022). Tinjauan yuridis tentang kedudukan alat bukti digital dalam tindak pidana kejahatan mayantara (cyber crime). *Lex Privatum*, *10*(5), 112–124.

Maryam, T. A., Maharani, M. A., Fahrezi, T. A., & Nugroho, A. A. (2024). Peran digital forensik dalam pengumpulan bukti pada kasus judi online di Kabupaten Demak. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *1*(3), 33–43.

Mokobombang, M., Darwis, Z., & Mokodenseho, S. (2023). Pemberantasan tindak pidana cyber di Provinsi Jawa Barat: Peran hukum dan tantangan dalam penegakan hukum terhadap kejahatan digital. *Jurnal Hukum dan HAM Wara Sains*, *2*(6), 517–525.

Munajat, A. A., & Yusuf, H. (2024). Peran teknologi informasi dalam pencegahan dan pengungkapan tindak pidana ekonomi khusus. *Jurnal Intelek Insan Cendikia*, *1*(9), 4853–4865.

Mursyid, M., Putera, A., & Jannah, M. (2025). Rekonstruksi peran digital forensik dalam penyidikan tindak pidana siber. *Jurnal Tana Mana*, *6*(2), 289–296.

Pahrudin, P. (2020). Cybercrime in the context of cellular telephone scams. *Jurnal Penelitian Pos dan Informatika*, *10*(1), 73–85.

Pradipa, A. (2025). Analisis terhadap kedudukan alat bukti elektronik dalam pembuktian perkara perdata pasca UU ITE dan perkembangan e-court. *Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi*, *2*(3), 191–203.

Putra, S. S. (2024). *Kekuatan bukti elektronik dalam pembuktian perkara tindak pidana korupsi di Indonesia* (Disertasi doktoral). Universitas Islam Sultan Agung Semarang.

Rahmanto, T. Y., Kav, J. H. R. S., & Kuningan, J. S. (2019). Penegakan hukum terhadap tindak pidana penipuan berbasis transaksi elektronik. *Jurnal Penelitian Hukum De Jure*, *19*(1), 31–45.

Riskiyadi, M. (2020). Investigasi forensik terhadap bukti digital dalam mengungkap cybercrime. *Cyber Security dan Forensik Digital*, *3*(2), 12–21.

Riston, R., & Basoddin, B. (2025). Fungsi digital forensik dalam pembuktian tindak pidana siber. *Sultra Law Review*, *3*(2), 3744–3756.

Rohman, R., Muliadi, M., Pratama, F., Saputra, I., Firmansyah, A., Marwan, T., & Irfandi, I. (2024). Sistem pembuktian dalam hukum pidana Indonesia dan tantangan dalam proses peradilan. *JIMMI: Jurnal Ilmiah Mahasiswa Multidisiplin*, *1*(3), 279–292.

Sirait, M. P. (2025). *Penggunaan teknologi forensik dalam penegakan hukum pidana: Tinjauan terhadap keandalan bukti elektronik* (Disertasi doktoral). Universitas Malikussaleh.

Sucia, Y., & Deswari, M. P. (2024). Bukti elektronik dalam sistem peradilan: Memahami peran dan validitasnya. *Innovative: Journal of Social Science Research*, *4*(4), 13729–13741.

Wiarti, J. (2023). Legality of electronic evidence in cybercrime cases. *Ahmad Dahlan Indonesian Law Journal*, *1*(2), 11–19.

Wicaksono, A., Adinandra, S., & Prayudi, Y. (2020). Penggabungan metode Itakura Saito distance dan backpropagation neural network untuk peningkatan akurasi suara pada audio forensik. *Juita: Jurnal Informatika*, *8*(2), 225–233.

Zaenudin, F. R., & Faridah, H. (2022). Pertanggungjawaban pidana terhadap afiliator aplikasi opsi biner ilegal dalam hukum pidana Indonesia. *Jurnal Hukum Sasana*, *8*(1), 55–70.

Zuhri, S., & Fadil, C. (2024). Peran media digital dalam penegakan hukum di masyarakat. *Crossroad Research Journal*, *1*(4), 118–139.

Acknowledgment
We gratefully acknowledge the contributions of individuals who supported the completion of this article.

Funding Information
This research did not receive any funding.

Conflict of Interest Statement
The authors declare that there is no conflict of interest.

Ethical Approval and Originality Statement
Ethical approval was obtained for this study. The manuscript represents original work and has not been previously published, nor is it under consideration by another journal.

Data Disclosure Statement
The data that support the findings of this study are available from the corresponding author upon reasonable request.