



Legal Analysis of the Use of Electronic Evidence in Providing Evidence in Corruption Cases (Decisions in Indonesia)

Aga Naya Saputra¹, Ghina Salsabila Aven²

^{1,2}Faculty of Economic and Social, Jenderal Achmad Yani Yogyakarta University, Sleman, Indonesia

Abstract: The rapid development of information technology has significantly transformed criminal procedure law, particularly regarding the recognition and use of electronic evidence. In corruption cases, electronic evidence has become a central instrument in uncovering modus operandi, tracing financial flows, and proving the involvement of perpetrators. This study aims to analyze the juridical status, practical application, and challenges of using electronic evidence in proving corruption cases in Indonesia. The research employs normative legal methods with statutory and case approaches, relying on secondary data such as legislation, legal literature, and relevant court decisions. The findings indicate that electronic evidence has obtained normative legitimacy through the Electronic Information and Transactions Law, the Anti-Corruption Law, and progressive judicial decisions. In practice, electronic evidence plays a decisive role in major corruption cases, although its implementation faces challenges related to authenticity, integrity, limited technical capacity of law enforcement officers, and regulatory disharmony. In conclusion, electronic evidence strengthens the evidentiary system in corruption cases, but legal harmonization, forensic technical standards, and capacity-building for law enforcement are required to ensure effectiveness and legal certainty.

Keywords: Corruption; Criminal Procedure Law; Electronic Evidence; Information Technology; Proof

1. Introduction

The development of information technology in the digital era has brought about fundamental changes in the criminal justice system, particularly in relation to the collection and utilization of evidence. In contemporary criminal cases, especially those involving technology-based crimes and corruption, electronic evidence is no longer merely supplementary, but rather serves as a primary instrument of proof (Sibuea, 2020). The increasing urgency of utilizing electronic evidence within Indonesia's criminal justice system has become more apparent in light of the significant surge in corruption cases. Data from Indonesia Corruption Watch (ICW) recorded that in 2023 there were 791 corruption cases involving 1,695 suspects, a sharp increase compared to 2022, which reported 579 cases with 1,396 suspects (Yandwiputra, 2024). This fact illustrates a concerning escalation in corruption offenses, with a 36.6% increase in cases within the span of just one year. Although Indonesia's Corruption Perceptions Index (CPI) in 2024 showed a slight improvement, reaching a score of 37 out of 100—an increase from the previous score of 34—its ranking also rose to 99th out of 180 countries (KPK T., 2025), nevertheless, this condition still places Indonesia among countries with persistently high levels of corruption.

Correspondence:

Name: Aga Naya Saputra

Email: malamsunnah1999@gmail.com

Received: Jul 30, 2025;

Revised: Aug 18 2025;

Accepted: Aug 24, 2025;

Published : Aug 30, 2025;



Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons

Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0) license (

<https://creativecommons.org/licenses/by-nc/4.0/>).

Electronic evidence plays a highly crucial role in the context of handling contemporary corruption cases. This role was particularly evident in the 2020 corruption case involving the Minister of Marine Affairs and Fisheries, Edhy Prabowo, where the bribery scheme related to lobster seed exportation was successfully uncovered by the Corruption Eradication Commission (KPK) through the use of electronic evidence (Harbowo, 2020). Electronic evidence also constituted a primary component in the COVID-19 social assistance corruption case involving the Minister of Social Affairs, Juliari Batubara. Forms of digital communication, electronic bank transfers, and digital documents revealed the flow of social assistance funds (Adhira, 2025). Another case that demonstrates the significance of electronic evidence is the corruption case concerning land procurement for the Ministry of Social Affairs involving the Governor of South Sulawesi, Nurdin Abdullah, in which the flow of bribery payments was successfully proven by the Corruption Eradication Commission (KPK) through electronic evidence (Ferdiansyah, 2021).

These high-profile cases not only exemplify the practical use of electronic evidence but also reveal deeper structural and technical challenges that persist in Indonesia's criminal justice system. The reliance on intercepted communications, digital transactions, and electronic documents often exposes vulnerabilities related to authentication, forensic validation, and chain of custody. Moreover, the uneven competence of law enforcement officials and the lack of unified technical standards frequently result in inconsistencies in the evidentiary weight accorded by the courts. Thus, these cases demonstrate that the problem is not merely practical, but rooted in systemic limitations that demand thorough juridical and institutional responses.

Court decisions have increasingly taken a progressive stance in recognizing electronic evidence, as reflected in cases such as Decision No. 1741 K/Pid.Sus/2020, No. 9/Pid.Sus-TPK/2024/PN Yyk, and No. 12/Pid.Sus-TPK/2021/PT Pbr, where digital evidence played a decisive role in uncovering unlawful conduct and state financial losses.

Normatively, electronic evidence has been recognized under Article 26A of Law No. 20 of 2001 concerning the Eradication of Corruption. Nevertheless, its implementation continues to encounter challenges, ranging from issues of authenticity and data integrity, limitations in the competence of law enforcement officials, to inconsistencies in judicial decisions regarding its evidentiary weight. Technical obstacles such as digital forensic validation, chain of custody, and personal data protection further create legal and ethical complexities.

This phenomenon underscores the necessity of a comprehensive juridical study on the use of electronic evidence in corruption cases, encompassing normative, implementative, and technical aspects. Such a study is crucial to promote regulatory reform, strengthen technical guidelines, and enhance the capacity of law enforcement officials, thereby ensuring that the evidentiary system in corruption cases becomes more adaptive, accountable, and aligned with the advancements of digital technology.

2. Materials and Methods

This research employs a normative legal research method with a statute approach and a case approach. This method is chosen because the study focuses on the analysis of positive law, encompassing both the norms codified in legislation and their application in court decisions concerning the use of electronic evidence in criminal cases, particularly corruption offenses. The data utilized consist of secondary data comprising primary legal materials, namely the 1945 Constitution, the Indonesian Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law (ITE Law), the Law on the Eradication of Corruption, as well as relevant court decisions; secondary legal materials, including books, journals, articles, and previous studies; and tertiary legal materials, such as legal dictionaries, encyclopedias, and the Indonesian Dictionary (KBBI). The data were collected through library research by examining and reviewing relevant legal literature, and subsequently analyzed qualitatively in a descriptive manner to illustrate, interpret, and provide arguments regarding the effectiveness and challenges of using electronic evidence within Indonesia's criminal justice system.

The data utilized in this study consist of secondary data. Primary legal materials include the 1945 Constitution, the Indonesian Criminal Procedure Code (KUHAP), the Electronic Information and Transactions Law (ITE Law), the Law on the Eradication of Corruption, and relevant court decisions. Secondary legal materials consist of books, journals, scholarly articles, and previous studies, while tertiary legal materials comprise legal dictionaries, encyclopedias, and the Indonesian Dictionary (KBBI). The data collection technique applied is library research, conducted by systematically examining and reviewing relevant legal literature and judicial decisions related to electronic evidence. The collected data are then analyzed qualitatively using descriptive analysis, aiming to illustrate the legal norms, interpret their application in corruption cases, and provide juridical arguments concerning both the effectiveness and the challenges of using electronic evidence in Indonesia's criminal justice system.

3. Results and Discussion

3.1. *Legal Regulation of Electronic Evidence in the Proof of Corruption Cases under Indonesian Legislation*

The advancement of information and communication technology has fundamentally altered the landscape of criminal law enforcement in Indonesia. Crimes such as corruption, which frequently involve sophisticated financial flows and cross-border networks, increasingly rely on digital platforms as part of their modus operandi. This transformation has necessitated the recognition of electronic evidence as a legitimate means of proof in court. Unlike traditional forms of evidence, electronic evidence encompasses a wide spectrum, ranging from emails, electronic fund transfers, and text messages to recorded conversations and digital transaction data. Its role is particularly crucial in corruption cases, where illicit practices are often concealed within layers of electronic communication and financial systems (Hamzah, 2016).

The legal foundation for electronic evidence in Indonesia can be found in Article 5 of Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which explicitly acknowledges electronic information and electronic documents, including

their printouts, as valid legal evidence. This recognition is further reinforced by Article 26A of Law No. 20 of 2001 on the Eradication of Corruption, which broadens the evidentiary scope to cover electronically recorded information. These provisions demonstrate a deliberate effort to modernize procedural law to remain relevant amidst technological progress, thereby ensuring that corruption, a crime often conducted digitally, can still be effectively prosecuted (Diantha, 2018).

Nevertheless, the position of electronic evidence in criminal procedure reveals a structural gap. The Indonesian Criminal Procedure Code (KUHAP), which was enacted long before the digital era, still recognizes only five conventional forms of evidence: witness testimony, expert testimony, documents, indications, and the defendant's statement. Electronic evidence is absent from this enumeration. Judges and law enforcement authorities therefore often interpret electronic data as falling under the categories of "documents" or "indications," provided it meets authenticity and integrity requirements (Mulyadi, 2018). This condition underscores the necessity of revising KUHAP so that electronic evidence can be explicitly and unambiguously incorporated into the evidentiary framework (Rosadi, 2019).

The explicit recognition of electronic evidence in the Anti-Corruption Law and the ITE Law represents a significant milestone in Indonesia's evidentiary system. By placing electronic evidence on equal footing with traditional forms of proof, the legislature has expanded the scope of admissible evidence. This expansion facilitates law enforcement, particularly in cases involving complex, cross-border, or technologically mediated crimes such as corruption, cybercrime, and narcotics offenses (Arief, 2018).

For example, recorded conversations and email exchanges can now be used in the same way as written documents or witness testimony. Such recognition not only enhances the effectiveness of proof but also reflects the principle that procedural law must adapt to evolving social and technological realities (Makarim, 2008).

While recognition has been granted, the validity of electronic evidence hinges upon authenticity and integrity. Authenticity ensures that electronic data originates from a legitimate source, while integrity guarantees that the data remains unaltered since its creation. Without fulfilling these conditions, electronic evidence risks being dismissed as unreliable or manipulated. Accordingly, the ITE Law emphasizes that electronic evidence must undergo forensic examination and adhere to a verifiable chain of custody (Djaja, 2020).

These requirements reflect broader principles of modern evidence law, which prioritize relevance and reliability. For instance, in corruption cases, intercepted phone conversations may serve as key evidence, but only if law enforcement can establish that the recordings have not been tampered with. Thus, forensic methodology and technological verification play a pivotal role in transforming electronic data into persuasive legal evidence (Harahap, 2019).

Beyond the ITE Law, sectoral legislation has strengthened the recognition of electronic evidence. Law No. 8 of 2010 on Money Laundering, for example, explicitly includes electronic information as admissible evidence, recognizing the digital nature of financial transactions underlying such crimes. Similarly, the Terrorism Law (Law No. 15 of 2003 as amended by Law No. 5 of 2018) and customs regulations accommodate

electronic records, communication metadata, and digital transactions as part of evidentiary frameworks (Pribadi, 2018).

These developments show a trend: Indonesian law is moving from mere tolerance of digital evidence to active accommodation. Supreme Court Regulation (PERMA) No. 4 of 2020 (as amended by PERMA No. 8 of 2022) further institutionalizes this by providing procedural standards for electronic criminal trials, from system seizures to courtroom presentation of digital evidence. Collectively, these provisions ensure that electronic evidence is not only admissible but also reliable and legally robust.

Despite progress, challenges persist. From the perspective of evidentiary theory, Indonesia adheres to the negative statutory proof system (*negatief wettelijk bewijstheorie*), under which a conviction requires at least two lawful forms of evidence and the judge's inner conviction (Mulyadi, 2018). Thus, electronic evidence is not sufficient merely to be formally recognized under the law; it must also be capable of providing the judge with conviction regarding the material truth of a criminal event. The presence of electronic evidence within this theoretical framework serves as a test of whether judges are able to relate digital evidence to existing legal constructions, while at the same time assessing its reliability as the basis for a judgment.

Furthermore, the regulation of electronic evidence is not limited to juridical legitimacy under Law Number 11 of 2008 on Electronic Information and Transactions (the EIT Law), but also encompasses methodological aspects in courtroom examination. This includes procedures of seizure, digital forensic examination, as well as the involvement of information technology experts to ensure the validity of such evidence (Huda, 2012). Without strict procedures, electronic evidence may lose its probative value as it is highly susceptible to disputes concerning its authenticity and integrity. Accordingly, the paradigm of proof in Indonesian criminal procedure law is undergoing a shift from a traditional approach toward an adaptation to the digital era. This shift requires judges not only to adhere to the formal legality of evidence but also to consider the technical and substantive aspects of electronic evidence in order to establish their conviction (Hamzah, 2016). Therefore, the role of judges within the system of negative statutory proof (*negatief wettelijk bewijstheorie*) becomes increasingly important, as judicial conviction must be built through a comprehensive assessment of the validity and relevance of electronic evidence in relation to the criminal act under examination. Although, normatively, there has been recognition of electronic evidence as a valid means of proof within the Indonesian legal system, its implementation still faces several fundamental weaknesses.

First, the main issue lies in the overlap and disharmony among statutory regulations. The Indonesian Code of Criminal Procedure (KUHAP), as the *lex generalis* of criminal procedure law, does not explicitly regulate electronic evidence. KUHAP still relies on classical terminology, namely documentary evidence, witnesses, experts, indications, and the confession of the defendant. In contrast, the development of sectoral regulations, such as the Law on Electronic Information and Transactions (EIT Law) and the Law on the Eradication of Corruption (Anti-Corruption Law), explicitly acknowledges the validity of electronic evidence as admissible proof. This lack of synchronization has created divergent interpretations in judicial practice, whereby some judges remain

firmly bound to the formalism of KUHAP, while others accommodate newer *lex specialis* provisions. Ultimately, such disharmony may undermine the principle of legal certainty, which constitutes one of the essential pillars of the rule of law in Indonesia (Hamzah, 2016).

Second, another weakness lies in the absence of detailed provisions regarding the technical standards for the authentication and validation of electronic evidence. The characteristics of electronic evidence in the form of digital data are highly vulnerable to modification, duplication, and deletion. Unlike conventional forms of evidence such as written documents, which possess a physical form, electronic evidence can be easily manipulated through certain technologies without leaving any visible traces. Therefore, standardized procedures for digital forensic examination should be explicitly regulated within procedural law in order to ensure the authenticity, integrity, and reliability of electronic evidence. The absence of such technical standards has the potential to create disputes in the evidentiary process in court, particularly concerning the validity of digital forensic results presented as evidence (Qamar, 2012).

Thirdly, an equally important aspect is the protection of human rights, particularly the rights to privacy and personal data, in the process of collecting and utilizing electronic evidence. In practice, investigators often carry out seizures or interceptions of electronic communications without adequately considering the boundaries of these fundamental rights protections. In fact, the Indonesian Constitution, through Article 28G paragraph (1) of the 1945 Constitution, guarantees every individual the right to protection of their personal self, family, honor, dignity, and property, including within the context of digital data (Asshiddiqie, 2005). If the collection of electronic evidence is conducted in a manner that violates privacy without clear legal procedures, it not only risks undermining the principle of due process of law but may also lead to the abuse of authority by law enforcement officers. Accordingly, a more comprehensive regulation regarding the protection of personal data in the context of criminal evidence is an urgent necessity.

3.2. The Application of Electronic Evidence in the Adjudication of Corruption Cases in Indonesia and the Legal and Technical Challenges Encountered in its Admission and Use

In the adjudication of corruption cases in Indonesia, electronic evidence no longer functions merely as supplementary proof but has become the backbone of modern evidentiary processes. Digital traces—such as instant messaging conversations, emails, system access logs, banking transactions, and audiovisual recordings—enable law enforcement authorities to reconstruct the *modus operandi*, map the involvement of perpetrators, and trace the flow of funds in a forensic manner. This development is consistent with the recognition of electronic evidence under the Electronic Information and Transactions Law (UU ITE), which places it on equal footing with conventional evidence under the Indonesian Criminal Procedure Code (Mulyadi, 2010). This development is grounded in the Electronic Information and Transactions Law (UU ITE), which explicitly recognizes electronic information/documents and their printed outputs

as valid evidence alongside traditional means of proof under Article 184 of the Criminal Procedure Code (KUHAP).

First, in reconstructing the *actus reus*, electronic artifacts provide chronological narratives through timestamps and metadata. Online conversations and file transfers can establish contacts between bribers and officials, as well as negotiation stages preceding transactions. Courts have accepted electronic recordings—if proven authentic and reliable—on equal footing with conventional evidence, often reinforced by expert testimony in digital forensics (Supardi, 2021).

Second, electronic evidence is vital in mapping the nexus of actors and their intent (*mens rea*). Forensic analysis of devices and accounts, supported by geo-location and communication pattern analysis, enables the identification of coordination among perpetrators. Such evidence gains probative force when combined with witness testimony, physical documents, or expert statements, creating a coherent chain of corroboration (Supardi, 2021).

Third, digital banking records—such as SWIFT messages, e-banking logs, and system-generated statements—are indispensable in tracing state financial losses. Investigators employ audit trails and transactional analytics to uncover layering and placement schemes common in corruption-linked money laundering. The evidentiary regime has also been reinforced through Supreme Court Regulation (PERMA) No. 4 of 2020 (amended by PERMA No. 8 of 2022), which provides procedural certainty for the submission and examination of electronic evidence in court (Makarim, 2019). Scholars emphasize that authenticity, reliability, and expert competence are essential prerequisites for admissibility (Arief, 2018).

Several major cases illustrate the centrality of electronic evidence. In the Edhy Prabowo case (2020) concerning lobster larvae export, the Corruption Eradication Commission (KPK) relied on digital communications and banking transfers to map bribery flows (Hamzah, 2016). The Juliari Batubara case (2020) involving COVID-19 social aid corruption also highlighted the role of digital records and banking data in tracing illicit transactions (Suhariyanto, 2012). Similarly, in the Nurdin Abdullah case (2021), instant messaging records served as direct evidence of bribery practices (Makara, 2015). These cases demonstrate that electronic evidence functions not merely as corroborative but as primary proof.

Judicial precedents further reinforce this development. In Case No. 1741 K/Pid.Sus/2020, the Supreme Court recognized printed email correspondence as valid evidence (Harahap, 2019). Likewise, Case No. 9/Pid.Sus-TPK/2024/PN Yogyakarta admitted a computer as a container of digital evidence to trace village fund flows (Ramli, 2013), while Case No. 12/Pid.Sus-TPK/2021/PT Pekanbaru accepted bank-generated electronic statements as authentic evidence of fund manipulation (Suhariyanto, 2014). Such rulings indicate a paradigmatic shift from conventional proof to technology-based evidence (Reksodiputro, 2019).

Despite these advances, significant legal and technical challenges persist. The most critical issue lies in ensuring the authenticity and integrity of digital data, which are intangible and prone to alteration. Strict application of chain of custody and forensic procedures is required to maintain evidentiary reliability (Hamzah, 2016). Moreover,

disharmony between UU ITE and KUHAP often leads to judicial uncertainty, as some courts accept electronic evidence while others reject it due to authenticity concerns (Arief, 2018).

Another challenge concerns the limited technical expertise of law enforcement. Handling electronic evidence requires advanced knowledge in digital forensics, yet not all investigators, prosecutors, or judges possess such capacity. This results in inconsistent judicial attitudes and threatens legal certainty (Ramli, 2017). Strengthening human resources through specialized training and standardized guidelines is therefore crucial.

Infrastructure gaps also pose major obstacles. Digital forensic laboratories remain concentrated in large cities, leaving rural law enforcement with limited access to proper facilities. This disparity undermines both investigative efficiency and evidentiary reliability (Arief, 2018). Expanding forensic infrastructure is essential to preserve public trust in the justice system.

Furthermore, the use of electronic evidence raises concerns regarding privacy and human rights. Seizure of personal data, wiretapping, or access to private communications must adhere to due process and judicial oversight. Without clear legal safeguards, electronic evidence risks violating constitutional rights (Ramli, 2019). The lack of harmonization between UU ITE and KUHAP exacerbates this issue, highlighting the need for specific procedural rules governing electronic evidence to balance effective law enforcement with human rights protection.

In sum, Indonesian judicial practice has increasingly legitimized electronic evidence in corruption adjudication, both normatively under UU ITE and concretely through case law. While it now serves as a decisive tool in exposing corruption, unresolved challenges regarding authenticity, infrastructure, technical expertise, and human rights must be addressed. Establishing uniform standards, enhancing forensic capacity, and harmonizing legislation are crucial steps toward ensuring that electronic evidence strengthens the fight against corruption while upholding the principles of justice.

4. Conclusions

Normative regulations have provided a sufficiently strong legitimacy through the Electronic Information and Transactions Law (UU ITE), the Anti-Corruption Law (UU Tipikor), and the Criminal Procedure Code (KUHAP) as progressively interpreted. Judicial decisions have demonstrated that electronic evidence is recognized as admissible, provided it meets the requirements of authenticity, integrity, and relevance. This underscores a paradigm shift in the evidentiary system, which previously focused solely on conventional forms of proof but has now evolved to accommodate digital evidence. Despite the clarity of normative recognition, a number of practical obstacles remain, including limitations in digital forensic infrastructure, the capacity of law enforcement officials, and potential judicial doubts regarding the authenticity of electronic data. Nevertheless, in practice, courts have continued to rely on electronic evidence as the basis for judicial reasoning, even in major corruption cases. This indicates that electronic evidence has played a central role in uncovering increasingly complex modes of corruption.

Building on these findings, this research contributes directly to the formulation of more harmonious regulations by emphasizing the urgency of revising KUHAP to explicitly incorporate electronic evidence as an autonomous category of proof, thereby eliminating inconsistencies with sectoral legislation. It also highlights the importance of establishing detailed procedural standards on authentication, chain of custody, and forensic validation, as well as integrating personal data protection principles into evidentiary law. These recommendations provide a concrete juridical foundation for legislative reform, ensuring that the regulatory framework for electronic evidence becomes more coherent, reliable, and responsive to the challenges of corruption adjudication in the digital era.

References

- Adhira, R. D. (2025, Januari 8). Tindak Pidana Korupsi di Era Digital: Transformasi Kejahatan dan Respons Publik di Media Sosial. Indonesia.
- Adji, I. S. (2005). *Hukum Pembuktian dalam Perkara Pidana*. Jakarta: Diadit Media.
- Arief, B. N. (2018). *Bunga Rampai Kebijakan Hukum Pidana*. Jakarta: Kencana.
- Asshiddiqie, J. (2005). *Konstitusi dan Hak Asasi Manusia*. Jakarta: Konstitusi Press.
- Diantha, I. G. (2018). Urgensi Alat Bukti Elektronik dalam Pembuktian Tindak Pidana Korupsi. *Jurnal Magister Hukum Udayana*, 164.
- Djaja, E. (2020). *Hukum Pembuktian dalam Sistem Peradilan Pidana (Jakarta: , 2020*. Jakarta: Prenadamedia.
- Effendi, E. (2017). Pembuktian Tindak Pidana Korupsi dengan Alat Bukti Elektronik. *Jurnal Hukum IUS QUIA IUSTUM*, 457-474.
- Ferdiansyah, B. (2021, April 14). Kasus Nurdin Abdullah, KPK amankan bukti barang elektronik. Indonesia.
- Fuady, M. (2012). *Teori Hukum Pembuktian: Pidana dan Perdata*. Bandung: Citra Aditya Bakti.
- Hamdan, M. (2012). Bukti Elektronik dalam Sistem Pembuktian Hukum Acara Pidana di Indonesia. *Jurnal Hukum Ius Quia Iustum*.
- Hamzah, A. (2016). *Hukum Acara Pidana Indonesia*. Jakarta: Sinar Grafika.
- Hamzah, A. (2016). *Hukum Acara Pidana Indonesia*. Jakarta: Sinar Grafika.
- Harahap, Y. (2017). *Pembahasan Permasalahan dan Penerapan KUHAP: Pemeriksaan Sidang, Banding, Kasasi, dan Peninjauan Kembali*. Jakarta: Sinar Grafika.
- Harahap, Y. (2019). *Pembahasan Permasalahan dan Penerapan KUHAP*. Jakarta: Sinar Grafika.
- Harbowo, N. (2020, November 28). Ketua KPK: Kasus Edhy Prabowo Tak Bermuatan Politik. Indonesia.
- Hidayati, E. F. (2020, September 25). Keabsahan Pembuktian Elektronik dalam Persidangan Perdata di Pengadilan Agama. Indonesia.
- Huda, C. (2012). Kekuatan Pembuktian Alat Bukti Elektronik dalam Proses Peradilan Pidana. *Jurnal Rechts Vinding*, 245.
- Hukumonline. (2024, Juni 25). Mempertanyakan Bukti Elektronik sebagai Alat Bukti dalam Kasus Pidana. Indonesia.
- Indonesia, K. R. (2023). *Laporan Evaluasi Kapasitas Digital Forensik . 2023*: Divisi Humas Polri.
- Indonesia, K. R. (2024). *Laporan Tahunan Kejahatan Siber di Indonesia*. Jakarta: Divisi Humas Polri.
- Indriani, S., & Emirzon, J. (2020). Bukti Elektronik Sebagai Alat Pembuktian Dalam Transaksi Elektronik. *Lex Lata Jurnal Ilmiah Ilmu Hukum*, 388.
- KPK. (2024, Desember 9). KPK Gelar Lokakarya Strategi Penyajian Alat Bukti Elektronik di Hakordia 2024. Indonesia.
- KPK, T. (2025, Februari 10). Skor IPK 2024 Meningkatkan, KPK Dorong Penguatan Pemberantasan Korupsi.
- Makarao, M. T. (2015). *Hukum Acara Pidana dalam Teori dan Praktek*. Jakarta: Ghalia Indonesia.

- Makarim, E. (2008). Kedudukan Alat Bukti Elektronik dalam Sistem Peradilan Pidana. *Jurnal Hukum & Pembangunan*, 414–416.
- Makarim, E. (2019). *Kompendium Hukum Telematika*. Jakarta: Rajawali Pers.
- Mardiah, A. (2022, November 11). Memahami Bukti Elektronik sebagai Alat Bukti yang Sah. Indonesia.
- Marzuki, P. M. (2017). *Penelitian Hukum, 13th ed.* . Jakarta: Kencana Prenadamedia Group.
- Mulyadi, L. (2010). *Hukum Pembuktian dalam Perkara Pidana*. Bandung: Citra Aditya Bakti.
- Mulyadi, L. (2018). *Hukum Acara Pidana: Teori dan Praktik Peradilan Indonesia*. Jakarta: PT Alumni.
- Priatmaja, A. H. (2025, Juni 14). Korupsi Kolosal E-KTP yang Mencedakakan Negara. Indonesia.
- Pribadi, I. (2018). Legalitas Alat Bukti Elektrnonik Dalam Sistem Peradilan Pidana. *Lex Renaissance*, 119-120.
- Qamar, N. (2012). Kedudukan Alat Bukti Elektronik dalam Sistem Hukum Acara Pidana. *Jurnal Ilmu Hukum Amanna Gappa*, 158.
- Rahardjo, S. (2006). *Ilmu Hukum*. Bandung: Citra Aditya Bakti.
- Rahardjo, S. (2019). *Penegakan Hukum: Suatu Tinjauan Sosiologis*. Yogyakarta: Genta Publishing.
- Ramli, A. M. (2013). Bukti Elektronik dalam Sistem Peradilan Pidana di Indonesia. *Jurnal Hukum IUS QUIA IUSTUM*, 561–580.
- Ramli, A. M. (2017). Urgensi Pembuktian Elektronik dalam Sistem Peradilan Pidana. *Jurnal Hukum IUS QUIA IUSTUM*, 203-205.
- Ramli, A. M. (2019). Perlindungan Hak Privasi dalam Era Digital: Perspektif Hukum Indonesia. *Jurnal Hukum Ius Quia Iustum*, 515–534.
- Reksodiputro, M. (2019). *Kriminologi dan Sistem Peradilan Pidana*. Jakarta: Pusat Pelayanan Keadilan dan Pengabdian Hukum Universitas Indonesia.
- Riyanto, R. B. (2018). Tantangan Pembuktian dengan Alat Bukti Elektronik dalam Peradilan Pidana. *Jurnal Hukum dan Pembangunan* , 289–306.
- Rosadi, S. D. (2019). Kekuatan Alat Bukti Elektronik dalam Sistem Pembuktian Pidana di Indonesia. *Jurnal Hukum dan Pembangunan*, 654.
- Rum, G. W. (2025). Penggunaan Alat Bukti Elektronik Dalam Proses Peradilan Perdata. *Jurnal Multidisiplin Ilmu Akademik*, 63.
- Rusydi, M. T. (2025). *Pengantar Hukum Teknologi*. Surakarta: Naga Pustaka.
- Sibuea. (2020). *Hukum Pembuktian Digital dalam Peradilan Pidana*. Jakarta: Prenada Media.
- Sidharta, A. (2018). Pengakuan dan Kedudukan Bukti Elektronik dalam Proses Peradilan. *Jurnal Hukum dan Pembangunan*, 62.
- Suhariyanto, B. (2012). *Tindak Pidana Teknologi Informasi: Cybercrime Regulation* . Jakarta: Raja Grafindo Persada.
- Suhariyanto, B. (2014). *Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya*. Jakarta: Raja Grafindo Persada.
- Supardi. (2021). Mengukur Kekuatan Alat Bukti Elektronik dalam Pembuktian Perkara Tindak Pidana Korupsi. *Syntax Literate (UPN Veteran Jakarta)*.
- Susanto, A. (2020). *Hukum dan Teknologi Informasi: Perspektif Teori dan Praktik*. Jakarta: Kencana.
- Tanoto, E., Tandy, J., & Banke, R. (2024). Kekuatan Alat Bukti Elektronik dalam Proses Pembuktian di Peradilan Pidana. *Jurnal Ilmu Hukum*, 95.
- Taqiyya, S. A. (2021, Agustus 18). Syarat dan Kekuatan Hukum Alat Bukti Elektronik. Indonesia.
- Waruwu, R. P. (2019, Juni 4). Eksistensi Dokumen Elektronik di Persidangan Perdata. Indonesia.
- Yandwiputra, A. R. (2024, Mei 20). ICW Catat Sepanjang 2023 Ada 791 Kasus Korupsi, Meningkatkan Singnifikan 5 Tahun Terakhir. Indonesia.