DOI: 10.46924/jihk.v7i1.323

Can Electronic Evidence Constitute Sufficient Grounds for Criminal Liability?

Atang Suryana[1*] & Marius Suprianto Sakmaf[2]

[1,2]Sekolah Tinggi Ilmu Hukum Manokwari, Indonesia

Correspondence

Atang Suryana, Sekolah Tinggi Ilmu Hukum Manokwari, Indonesia, Jl. Karya Abri No.2, Sanggeng, Kec. Manokwari Barat, Kabupaten Manokwari, Papua Barat. 98312, e-mail: stihatangsuryana@gmail.com

How to cite

Suryana, Atang. & Sakmaf, Marius Suprianto. 2025. Can Electronic Evidence Constitute Sufficient Grounds for Criminal Liability? *Jurnal Ilmu Hukum Kyadiren* 7(1), 587-601. https://doi.org/10.46924/jihk.v7i1.323

Original Article

Abstract

The advancement of information technology has triggered a paradigm shift in the evidentiary system of criminal law, particularly concerning the legality and authenticity of electronic evidence. This study seeks to examine the legal standing of electronic evidence within the Indonesian criminal procedure framework, assess the impact of Constitutional Court Decision No. 20/PUU-XIV/2016, and evaluate the admissibility of such evidence in light of evidentiary principles and the role of digital forensics. Employing a normative juridical approach, the analysis is based on statutory regulations, judicial decisions, and relevant legal scholarship. The findings reveal that while electronic evidence has been formally acknowledged through the Electronic Information and Transactions (ITE) Law and reinforced by the Constitutional Court's decision, significant challenges persist in both its technical implementation and legal admissibility in court proceedings. Digital forensics plays a critical role in safeguarding the integrity and reliability of electronic evidence. The study concludes that reforming the Indonesian Criminal Procedure Code and developing standardized digital evidence protocols are essential to ensuring justice and legal certainty.

Keywords: *Legality; Law of Evidence; Electronic Evidence; Indonesian Legal System*

Abstrak

Perkembangan teknologi informasi telah mendorong pergeseran paradigma dalam sistem pembuktian hukum pidana, khususnya terkait legalitas dan keautentikan alat bukti elektronik. Penelitian ini bertujuan untuk mengidentifikasi posisi hukum alat bukti elektronik dalam sistem hukum acara pidana Indonesia, menganalisis pengaruh Putusan Mahkamah Konstitusi No. 20/PUU-XIV/2016, serta mengkaji keabsahan bukti elektronik berdasarkan prinsip pembuktian dan peran digital forensik. Metode yang digunakan adalah pendekatan yuridis normatif dengan analisis terhadap peraturan perundang-undangan, putusan pengadilan, dan literatur hukum relevan. Hasil penelitian menunjukkan bahwa alat bukti elektronik telah diakui secara normatif melalui UU ITE dan putusan MK, namun masih menghadapi hambatan penerapan teknis dan yuridis di pengadilan. Digital forensic menjadi instrumen penting dalam memastikan integritas dan keotentikan bukti elektronik. Penelitian ini menyimpulkan bahwa reformasi KUHAP dan penyusunan standar pembuktian digital diperlukan untuk menjamin keadilan dan kepastian hukum.

Kata kunci: *Legalitas, Hukum Pembuktian, Alat Bukti Elektronik, Hukum Indonesia*

1. INTRODUCTION

The rapid advancement of information and communication technology over the past two decades has profoundly transformed various aspects of life, including the criminal justice system in Indonesia. Amid a surge in cyber-related crimes—such as online fraud, digital hate speech, and money laundering via electronic networks—there is an urgent demand for legal instruments capable of addressing these emerging realities. One of the most critical components of contemporary law enforcement is the incorporation of electronic evidence as an integral element within the evidentiary system.

In the Indonesian legal framework, the evidentiary system in criminal proceedings remains grounded in the Criminal Procedure Code (KUHAP), enacted in 1981. Article 184 of KUHAP enumerates five recognized forms of evidence: witness testimony, expert opinion, documents, indications, and the statements of the accused. Notably, it does not explicitly recognize electronic evidence as a distinct category. This omission creates a normative dilemma, especially in cases that heavily rely on digital evidence—such as recordings, emails, metadata, instant messaging logs, and data from electronic information systems.

Although Law No. 11 of 2008 on Electronic Information and Transactions (ITE), as amended by Law No. 1 of 2024, affirms the validity of electronic information and documents as admissible evidence, it operates as a *lex specialis* and has not been fully harmonized with the KUHAP as lex generalis. This legal disharmony has sparked considerable debate among scholars, practitioners, and law enforcement authorities regarding the status, form, probative value, and procedural acceptance of electronic evidence in criminal proceedings.

The Constitutional Court's Decision No. 20/PUU-XIV/2016 marked a pivotal development in Indonesia's criminal procedural law. The Court interpreted Article 5(1) and (2) of the ITE Law to affirm that electronic evidence may carry probative value equivalent to written or indicative evidence, provided it satisfies the principles of functional equivalence and the integrity of the underlying electronic system. However, despite this normative recognition, inconsistencies persist in judicial practice—particularly in evaluating the authenticity, admissibility, and probative strength of electronic evidence in the absence of robust digital forensic verification.

Evidence plays a foundational role in the Indonesian legal system, serving as the basis for judicial reasoning and decision-making in both civil and criminal cases. Article 184(1) of the KUHAP explicitly defines valid evidence, yet this definition has been increasingly challenged by the rise of digital technologies. As Imron and Iqbal emphasize, evidence serves to clarify the legal positions of parties in litigation and to

bridge legal reasoning with factual reality.[1] According to Subekti, evidence encompasses any means capable of convincing the judge of the truth of a legal event.[2]

Recent scholarship supports the evolving legitimacy of electronic evidence. Research by Wirawan et al. highlights that although electronic evidence is not enumerated in the KUHAP, it is recognized under the ITE Law and may stand as independent evidence if it fulfills the principle of functional equivalence.[3] Similarly, Gunawan and Bhakti underscore the recognition of electronic evidence under Articles 5 and 44 of the ITE Law. Nonetheless, ambiguity remains regarding whether electronic evidence constitutes a separate evidentiary category or should be subsumed under documentary or indicative evidence. This lack of clarity is further exacerbated by the Constitutional Court's interpretation, which has led to varied understandings of the evidentiary status of digital materials.[4]

In a different context, Pramata examined the use of recordings—such as those obtained from CCTV—as evidence and concluded that while such materials may be admissible, their use must adhere to legal provisions that safeguard the right to privacy. This underscores the critical role of digital forensics in verifying the validity of electronic evidence.[5] Similarly, Pribadi and Ramiyanto emphasized the importance of recognizing electronic evidence, despite its absence as an explicitly defined category within the Indonesian Criminal Procedure Code (KUHAP). In practice, numerous special laws have paved the way for the admissibility of electronic evidence, particularly in cybercrime cases, with its legal foundation grounded in the Electronic Information and Transactions (ITE) Law, which functions as *lex specialis* in the context of cyber law enforcement.[6]

Dewantara and Suartha categorized electronic evidence into two primary forms within the criminal procedure framework: as documents and as indicia (indirect evidence). Printed versions of electronic data may be considered documents due to their tangible form, while their contents may serve as indicia if lawfully obtained.[7] Nafatilopa

---

1 Ali Imron and Muhamad Iqbal, *Hukum Pembuktian* (Tangerang Selatan: Unpam Press, 2019).

2 R. Subekti, *Hukum Pembuktian*, 16th ed. (Jakarta: Pradnya Paramita, 2007).

3 I Made Wirawan, Oheo K. Haris, and Handrawan Handrawan, "Legalitas Perluasan Penggunaan Alat Bukti Elektronik Dalam Penegakan Hukum Pidana Indonesia," *Halu Oleo Legal Research* 2, no. 1 (2020): 75–85, http://dx.doi.org/10.33772/holresch.v2i1.10604.

4 Tri Agus Gunawan and Indira Swasti Gama Bhakti, "Makna Perluasan Alat Bukti Elektronik: Analisis Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016," *Literasi Hukum* 6, no. 2 (2022): 105–16, https://doi.org/10.31002/lh.v6i2.6810.

5 Aldho Galih Pramata, "Analisis Kekuatan Dan Nilai Pembuktian Alat Bukti Elektronik Berwujud CCTV (Closed Circuit Television) Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Dalam Hukum Acara Pidana," *Jurnal Verstek* 8, no. 3 (2020): 392–400, https://doi.org/10.20961/jv.v8i3.47057.

6 Insan Pribadi, "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana," *Lex Renaissance* 3, no. 1 (2019): 109–24, https://doi.org/10.20885/JLR.vol3.iss1.art4; Ramiyanto Ramiyanto, "Bukti Elektronik Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana," *Jurnal Hukum Dan Peradilan* 6, no. 3 (2017): 463–84, https://doi.org/10.25216/jhp.6.3.2017.463-484.

7 Dewa Made Doni Dewantara and I Dewa Made Suartha, "Legalitas Alat Bukti Elektronik Sebagai Alat Bukti Dalam Hukum Acara Pidana," *Kertha Desa* 10, no. 8 (2022): 660–69, https://ojs.unud.ac.id/index.php/kerthadesa/article/view/89360.

and Michael noted that Constitutional Court Decision No. 20/PUU-XIV/2016 significantly influences the treatment of electronic evidence in court, clarifying that such evidence is not inherently autonomous but is typically classified as indicative evidence.[8]

An empirical study by Utami and Lubis explored the use of electronic recordings in money laundering prosecutions. They concluded that for electronic evidence to be deemed legally valid, it must meet both formal and material requirements as outlined in the ITE Law and must be corroborated by at least two pieces of admissible evidence, in accordance with Article 183 of the KUHAP.[9] Astuti highlighted the transformative impact of the technological revolution on evidentiary practices, noting that although the KUHAP does not expressly regulate electronic evidence, it has been acknowledged de facto in cases prosecuted under the ITE Law and anti-terrorism legislation.[10]

Lakada addressed inconsistencies in regulatory approaches to electronic evidence, observing that while some frameworks treat it as a form of indicative evidence, others recognize it as standalone evidence. This regulatory disharmony reveals underlying tensions within the Indonesian legal system.[11] Manurung and Krisnawati analyzed the limited normative legitimacy of electronic evidence under the KUHAP, despite its widespread use in practice. They stressed the necessity of digital forensic validation to ensure admissibility in court.[12] Similarly, Pratiwi and Yulianti warned that electronic documents are highly susceptible to manipulation, thereby necessitating rigorous authentication processes involving digital forensics to establish their credibility.[13]

While most previous studies have concentrated on the normative legality and classification of electronic evidence, they have yet to comprehensively examine its evidentiary validity, probative value, and practical application within the criminal justice system following the Constitutional Court's Decision No. 20/PUU-XIV/2016. This study seeks to fill that gap by offering an integrative analysis of the interplay between the Criminal Procedure Code, the ITE Law, and the function of digital forensics in ensuring the authenticity and admissibility of electronic evidence.

---

8 Princes Elsa Nafatilopa and Tomy Michael, "Legalitas Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Umum Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016," *Jurnal Sosial Humaniora Sigli* 5, no. 2 (2022): 342–51, https://doi.org/10.47647/jsh.v5i2.1018.

9 Dinda Puspita Tri Utami and Muhammad Ridwan Lubis, "Legalitas Rekaman Elektronik Sebagai Alat Bukti Dalam Tindak Pidana Pencucian Uang Studi Di Pengadilan Negeri Medan," *Kalam Keadilan* 10, no. 2 (2022): 334–42, http://siakad.univamedan.ac.id/ojs/index.php/kalam-keadilan/article/view/365.

10 Sri Ayu Astuti, "Perluasan Penggunaan Bukti Elektronik (Evidence of Electronic) Terkait Ketentuan Alat Bukti Sah Atas Perbuatan Pidana Di Ruang Mayantara (Cyberspace)," *Pagaruyuang Law Journal* 1, no. 1 (2017): 44–57, https://doi.org/10.31869/plj.v1i1.269.

11 Daniel David Julio Lakada, "Perkembangan Pengaturan Alat Bukti Elektronik Dalam Hukum Acara Pidana: Kajian Hukum Tentang Cyber Crime," *Lex Crimen* 12, no. 5 (2024): 1–11, https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/59171.

12 Theresia Octaviani Manurung and I Gusti Ayu Agung Ari Krisnawati, "Kedudukan Alat Bukti Elektronik Dalam Sistem Pembuktian Perkara Pidana Di Indonesia," *Kertha Desa* 10, no. 5 (2022): 371–81, https://ojs.unud.ac.id/index.php/kerthadesa/article/view/79114.

13 Feroca Mevihanna Noor Pratiwi and Sri Wahyuningsih Yulianti, "Penilaian Kekuatan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Penyebarluasan Konten Pornografi Melalui Media Sosial," *Jurnal Verstek* 10, no. 1 (2022): 59–67, https://doi.org/10.20961/jv.v10i1.63940.

Accordingly, this study aims to provide an in-depth analysis of the legality and evidentiary weight of electronic evidence in Indonesia's criminal justice system. The specific objectives are as follows:

1) To identify the legal status of electronic evidence within Indonesia's criminal procedure framework;
2) To analyze the evolution and impact of Constitutional Court Decision No. 20/PUU-XIV/2016 on the classification and use of electronic evidence; and
3) To examine the validity and authenticity of electronic evidence through the lens of evidentiary principles, with particular emphasis on the role of digital forensics in supporting its admissibility.

2. RESEARCH METHODOLOGY

This study employs a normative legal approach, which centers on the analysis of written legal norms contained in statutory regulations, court decisions, and legal doctrines. This method is selected to examine the legality, legal standing, and evidentiary value of electronic evidence within Indonesia's criminal procedural law framework. The primary focus lies in the normative disharmony between the Criminal Procedure Code (KUHAP), as the general criminal procedural law, and the Electronic Information and Transactions (ITE) Law, as a special procedural law. Within this context, law is viewed as a system of prescriptive norms that must be analyzed systematically and coherently.

The legal materials utilized in this study include primary sources such as the KUHAP, the ITE Law and its subsequent amendments, Constitutional Court Decision No. 20/PUU-XIV/2016, and related implementing regulations on electronic evidence. Secondary legal materials comprise legal textbooks, scholarly journal articles, academic writings, and previous research addressing electronic evidence and digital forensics. Tertiary legal materials—such as legal dictionaries and legal encyclopedias—are used to support the interpretation of key legal terms and concepts within criminal procedure.

The analysis is conducted qualitatively using systematic and grammatical interpretation of legal norms, along with comparative analysis between the KUHAP and the ITE Law. Additionally, a legal hermeneutic approach is applied to understand the dynamics of judicial practice and evaluate the legal implications of the Constitutional Court's decision. This study aims to answer three key questions: (1) how electronic evidence is legally recognized; (2) how its regulation aligns with the principles of a fair trial; and (3) how normative harmonization is essential to ensure its legal validity and effective probative value.

3. RESEARCH RESULT AND DISCUSSION

3.1. Legal Status of Electronic Evidence in the Criminal Procedure System

The primary objective of this study is to identify and analyze the legal status of electronic evidence within Indonesia's criminal procedure system, particularly in the context of the normative provisions outlined in the Criminal Procedure Code (KUHAP) and various special laws and regulations that explicitly recognize the legality of electronic evidence. This study also seeks to examine the processes by which electronic evidence attains formal legal standing and to explore its integration and challenges within the framework of modern criminal evidentiary practice.

The analysis reveals that the regulation of electronic evidence in Indonesia has evolved incrementally through a range of sector-specific legislative instruments that operate as *lex specialis*. These include, notably, Law No. 8 of 1997 concerning Company Documents, which implicitly acknowledges the legitimacy of electronic data storage media, and the Electronic Information and Transactions (ITE) Law—most recently amended by Law No. 1 of 2024—which explicitly affirms the admissibility of electronic information, electronic documents, and their printouts as legal evidence.

In practice, the Criminal Procedure Code (KUHAP), as the general criminal procedural law (lex generalis), does not expressly regulate electronic evidence. Article 184 of the KUHAP recognizes only five forms of valid evidence: witness testimony, expert opinion, documents, indications, and the defendant's statement. Nevertheless, applying the principle of functional equivalence, electronic evidence—particularly printed forms—may be analogized to written documents or indicia. This interpretation was confirmed by Constitutional Court Decision No. 20/PUU-XIV/2016, which affirmed that electronic evidence may be deemed valid if it meets the criteria of authenticity, system integrity, and legal compliance.

Furthermore, electronic evidence is explicitly recognized under several special criminal laws. These include Article 26A of the Anti-Corruption Law, Article 27 of the Anti-Terrorism Law, Article 73 of the Anti–Money Laundering Law, and provisions in both the Human Trafficking Law and the Narcotics Law. These statutes treat electronic evidence either as a form of stand-alone evidence or as an extension of indicative (indirect) evidence. Based on a comprehensive analysis of legislative texts and judicial practices, this study concludes that the legal status of electronic evidence in Indonesia's criminal procedure system can be classified into five categories:

1) Stand-alone evidence when explicitly recognized in special criminal statutes;
2) An extension of written evidence, under the principle of functional equivalence;
3) A source of indicative evidence, as outlined in Article 188 of the KUHAP, which allows indicia to be derived from documents or the defendant's statements, including verifiable electronic printouts;
4) Legally valid evidence, provided it satisfies both formal and substantive requirements in accordance with the ITE Law and is supported by expert digital forensic analysis;

5) Sufficient preliminary evidence, especially in investigations of cybercrime and corruption, as stipulated in Article 44 of the ITE Law and Article 26A of the Anti-Corruption Law.

These findings align with previous research. Wirawan et al. observed that electronic evidence may serve either as independent proof or as an extension of indicia, depending on the legal context and nature of the case.[14] Gunawan and Bhakti highlighted the continuing ambiguity surrounding the classification of electronic evidence due to its absence from the KUHAP.[15] Lakada and Ramiyanto emphasized the necessity of formally recognizing electronic evidence as an essential element of modern criminal proceedings, given the increasing predominance of digital evidence in contemporary cases.[16] This study builds upon those insights by demonstrating that legal developments have gradually institutionalized the status of electronic evidence and by emphasizing the critical role of judicial interpretation and digital forensics in validating its authenticity and legal reliability.

The legal status of electronic evidence in Indonesia's criminal justice system reflects a legal paradigm in transition. On one hand, the Criminal Procedure Code (KUHAP) continues to uphold classical formalism in evidentiary standards; on the other, the demands of modern legal practice have necessitated the acceptance of digital-based electronic evidence. The attempt to reconcile these two approaches presents structural challenges, particularly given the absence of a comprehensive revision of the KUHAP that can accommodate the realities of legal digitalization. The admissibility of electronic evidence hinges not only on its form and legal source but also on fundamental principles of evidence such as authenticity, integrity, and relevance. Judges are required to evaluate electronic evidence by considering the reliability of the electronic system from which it originated, its relevance to the case at hand, and its probative value in establishing legal facts.[17]

In practice, judges play a pivotal role in determining the admissibility of electronic evidence. For instance, in Decision No. 18/Pdt.G/2023/PN Mgg of the Magelang District Court, the judge accepted a video recording stored on a CD as valid evidence, despite the absence of digital forensic authentication. The court's reasoning was grounded in the principle of relevance and its consistency with other pieces of evidence—demonstrating the judiciary's evolving flexibility in adapting to digital forms of evidence.

---

[14] Wirawan, Haris, and Handrawan, "Legalitas Perluasan Penggunaan Alat Bukti Elektronik Dalam Penegakan Hukum Pidana Indonesia."

[15] Gunawan and Bhakti, "Makna Perluasan Alat Bukti Elektronik: Analisis Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016."

[16] Lakada, "Perkembangan Pengaturan Alat Bukti Elektronik Dalam Hukum Acara Pidana: Kajian Hukum Tentang Cyber Crime"; Ramiyanto, "Bukti Elektronik Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana."

[17] Debra Littlejohn Shinder and Michael Cross, *Scene of the Cybercrime* (Oxford: Syngress, 2008).

This study affirms that electronic evidence has gained substantive legal recognition within Indonesia's criminal procedure framework, despite the normative gap in the KUHAP. Consequently, the current legal standing of electronic evidence relies heavily on cross-legislative integration and progressive interpretation by law enforcement authorities, particularly the judiciary. These findings underscore the urgent need for reform of the Criminal Procedure Code to explicitly regulate electronic evidence as part of the formal evidentiary system—while upholding principles of digital validity, privacy protection, and traceability (audit trails). Moreover, the establishment of operational standards for digital forensics and certification mechanisms for electronic systems is essential to ensure that evidence presented in court is not only legally admissible, but also credible in terms of integrity and authenticity. Thus, electronic evidence can be considered legally binding and enforceable, provided it satisfies formal and material requirements, aligns with prevailing legal norms, and supports the broader pursuit of substantive justice.

3.2. Transformations in Indonesian Evidentiary Law Following Constitutional Court Decision No. 20/PUU-XIV/2016

The primary objective of this study is to critically examine the evolving landscape of evidentiary law in Indonesia following the issuance of Constitutional Court Decision No. 20/PUU-XIV/2016. Specifically, this study explores the decision's impact on the legitimacy and legal status of electronic evidence within the Indonesian criminal procedure system, and how it addresses the normative disjunction between the Criminal Procedure Code (KUHAP) as lex generalis and a range of sectoral laws that govern electronic evidence as *lex specialis*.

Constitutional Court Decision No. 20/PUU-XIV/2016 represents a jurisprudential turning point in the clarification of electronic evidence's legal status. The Court asserted that electronic information, electronic documents, and their printouts—provided they comply with statutory requirements—constitute legally valid evidence and are functionally equivalent to forms of evidence recognized under general procedural law. This clarification resolved longstanding ambiguities surrounding Article 5 paragraphs (1) and (2) of the Electronic Information and Transactions (ITE) Law, which had previously raised interpretive questions as to whether electronic evidence could only be used in cybercrime cases or also in conventional criminal proceedings.

The Court's decision affirmed that electronic evidence is admissible in all types of criminal cases, provided it satisfies both formal and material requirements—such as authenticity, system integrity, and evidentiary relevance. Moreover, the Court emphasized that the use of electronic evidence, including wiretaps, recordings, and digital documents, must respect constitutional rights, particularly the right to privacy as guaranteed under Article 28G of the 1945 Constitution.

In practice, various forms of electronic evidence—including emails, instant messaging records, CCTV footage, and digital financial transactions—have been introduced in cases involving corruption, money laundering, human trafficking, and terrorism. Prior to the Constitutional Court's decision, however, the admissibility of such evidence was frequently contested, due to its absence from the evidentiary categories explicitly enumerated in Article 184 of the KUHAP.

This study finds that Constitutional Court Decision No. 20/PUU-XIV/2016 has significantly strengthened and expanded the legal recognition of electronic evidence in Indonesia's criminal justice system. The ruling not only provides legal certainty but also serves as a binding interpretive framework for judges and law enforcement authorities in evaluating the admissibility and probative value of electronic evidence in judicial proceedings. The study further reveals that, in the wake of this decision, various sectoral laws—such as the Anti-Corruption Law, the Anti-Terrorism Law, the Anti–Money Laundering Law, and the ITE Law—have been more coherently integrated into Indonesia's national evidentiary regime. This development reinforces the principle of *lex specialis derogat legi generali*, whereby specific procedural norms can validly expand evidentiary scope beyond the confines of the general criminal procedure code.

These findings reinforce prior research—such as the study by Nafatilopa and Michael—which interpreted the Constitutional Court's ruling as a form of judicial acknowledgment of electronic evidence as an independent category.[18] However, this study goes further by framing the decision not only as an interpretive act but also as a form of legislative correction that fills a normative gap within the KUHAP. The findings are also in alignment with Gunawan and Bhakti, who observed that the ambiguous legal position of electronic evidence has led to inconsistency in judicial practice. This study builds upon such insights by offering a systemic perspective on the post-decision integration of cross-sectoral evidentiary norms.[19]

The Constitutional Court's Decision No. 20/PUU-XIV/2016 reflects a pivotal development in Indonesia's criminal procedural law, marking a transition from a conventional evidentiary framework to a digitally oriented system of proof. The Court not only affirmed the legality of electronic evidence, but also opened a new legal paradigm in which the digitalization of information serves as a critical instrument for enhancing the effectiveness and efficiency of judicial proceedings. This decision signifies a paradigm shift from formalistic evidentiary law to a more substantive approach, wherein the pursuit of material truth is prioritized over rigid adherence to evidentiary form.[20] Through this progressive interpretation, the Court urges the judiciary to move

---

[18] Nafatilopa and Michael, "Legalitas Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Umum Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016."

[19] Gunawan and Bhakti, "Makna Perluasan Alat Bukti Elektronik: Analisis Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016."

[20] Alfitra Alfitra, *Hukum Pembuktian Dalam Beracara Pidana, Perdata Dan Korupsi Di Indonesia* (Jakarta: Asser, 2014).

beyond legalistic formalism and to remain adaptive to emerging forms of evidence shaped by technological advancement.

However, this progressive legal development presents significant challenges. Chief among them is the necessity for a reliable and standardized digital forensic framework that ensures the authenticity and integrity of electronic evidence. Additionally, clear protocols for the collection, processing, and storage of digital evidence are essential to maintain its admissibility and probative value in court. These requirements align with the internationally recognized principles of audit trail and chain of custody. This study confirms that Constitutional Court Decision No. 20/PUU-XIV/2016 has had a transformative impact on the evidentiary regime within Indonesian criminal law. Several key affirmations may be drawn from this decision:

1) Electronic evidence is constitutionally recognized as valid legal proof—whether classified as documentary evidence, indicative evidence, or independent evidence in criminal proceedings.
2) The Constitutional Court's decision serves as a foundational legal instrument for reconciling normative fragmentation between the Criminal Procedure Code (KUHAP) and sectoral regulations governing electronic evidence.
3) Judges are granted legal discretion to assess the validity of electronic evidence, guided by both formal and material evidentiary principles as outlined in the Court's ruling.
4) The admissibility of electronic evidence must be balanced with the protection of fundamental rights, particularly in matters involving surveillance, wiretapping, and personal data.
5) Comprehensive regulatory reform is still needed, particularly in the form of KUHAP revision, the establishment of national digital forensic standards, and capacity-building initiatives to enhance law enforcement's technical and legal understanding of electronic evidence.

The legal status of electronic evidence has shifted from the periphery to a central component of Indonesia's evidentiary system. Constitutional Court Decision No. 20/PUU-XIV/2016 stands as the legal milestone that underpins this transformation. Nonetheless, the effectiveness of its implementation remains contingent upon legislative responsiveness, institutional preparedness, and the digital competency of law enforcement authorities.

3.3. The Validity and Authenticity of Electronic Evidence in Indonesia's Criminal Procedure System

This study aims to comprehensively examine the validity and authenticity of electronic evidence in Indonesia's criminal procedure system, with particular emphasis on the

application of evidentiary principles and the role of digital forensics in ensuring evidentiary integrity. The increasing reliance on digital documents, electronic communications, and transaction records as primary forms of evidence has generated an urgent need for both legal and technical clarity regarding their admissibility in court. The analysis reveals that the legality of electronic evidence has been progressively recognized through various legislative instruments. Since its initial acknowledgment in Law No. 8 of 1997 on Company Documents, the recognition of electronic data as valid evidence has steadily evolved. This development is reinforced by provisions in the following laws:

1) Law No. 20 of 2001 on the Eradication of Corruption, which broadens the scope of indicative evidence to include electronic documents;
2) Law No. 15 of 2003 on Terrorism and Law No. 8 of 2010 on Money Laundering (TPPU), both of which permit the use of digital data as direct evidence;
3) and especially Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), particularly Articles 5 and 44, which affirm that electronic information and electronic documents constitute legitimate extensions of evidence within the justice system.

Nevertheless, while the normative foundation for electronic evidence is well established, its factual validity—namely whether the submitted digital files are genuine, unaltered, and relevant—remains subject to scrutiny. Here, digital forensics plays a crucial role. The findings of this study indicate that courts assess the admissibility of electronic evidence based on two primary dimensions:

1) Authenticity – the ability to demonstrate that the evidence originates from a verifiable source and has not been tampered with from the time it was collected to its presentation in court;
2) Integrity – assurance that the content of the evidence remains complete and unaltered, verified through forensic methods such as audit trails, checksums, metadata analysis, and a clearly documented chain of custody.

Judges must evaluate both aspects when determining whether electronic evidence may be classified as documentary evidence, indicative (indirect) evidence, or sufficient preliminary evidence. This study concludes that electronic evidence can be considered valid and legally admissible only if it satisfies both formal and material requirements, including:

1) Retrieval through an electronic system that meets information security standards;
2) Assurance of no data modification post-acquisition (maintained integrity);
3) Verifiability through a digital audit trail;

4) Collection and presentation in accordance with lawful procedures;
5) Accompaniment by a digital forensic expert report providing technical and scientific validation.

The role of digital forensics is not merely complementary but constitutes an integral and indispensable component of the evidentiary process involving electronic evidence. This study reinforces and further refines the conclusions of earlier research. Ramiyanto and Pratiwi and Yulianti argue that digital evidence is inherently vulnerable to manipulation and cannot rely solely on normative legal recognition. They emphasize the critical need for technical authentication and scientific verification procedures.[21] This study builds upon those insights by concretely mapping the conditions under which electronic evidence may be deemed valid, grounded in the principles of evidentiary law: competence, relevance, and materiality.

Moreover, the study introduces a practical dimension, asserting that digital forensics is the most objective and reliable method for assessing the authenticity and integrity of electronic evidence—whether in hardcopy or softcopy format—and across a range of criminal cases, from corruption to money laundering. The findings reveal that although electronic evidence is normatively acknowledged within Indonesia's legal system, judicial practices remain inconsistent due to the absence of uniform technical and legal standards. In the absence of digital forensic analysis, electronic evidence remains a digital file susceptible to denial or challenge by opposing parties. Consequently, judges and law enforcement officers bear the responsibility to ensure that electronic evidence is obtained lawfully (e.g., wiretaps must be authorized by a court), is not manipulated or edited (e.g., WhatsApp messages must include metadata), is retrieved by authorized parties, and is tested using scientific methods by qualified forensic experts.

This interpretation aligns with the view expressed by Shinder and Cross, who stated that evidence must meet the standards of competence, relevance, and materiality to be admissible in court.[22] This study emphasizes that legal recognition of electronic evidence must be supported by robust technical mechanisms to ensure its reliability and probative value. Based on field observations and normative analysis, this study arrives at the following key conclusions:

1) Valid electronic evidence must be authenticated and verified—both through digital forensic analysis and secure information systems.
2) The role of digital forensics is foundational, not merely supplementary, especially in verifying the integrity and validity of evidence in legal proceedings.

---

21 Ramiyanto, "Bukti Elektronik Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana"; Pratiwi and Yulianti, "Penilaian Kekuatan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Penyebarluasan Konten Pornografi Melalui Media Sosial."

22 Shinder and Cross, *Scene of the Cybercrime*.

3) Judges must assess electronic evidence in relation to its consistency with other admissible evidence, as required under the Criminal Procedure Code and the ITE Law.
4) The minimum standard for the admissibility of electronic evidence should include: a documented audit trail, a preserved chain of custody, lawful acquisition, and forensic validation by certified experts.
5) The decision of the Magelang District Court in Case No. 18/Pdt.G/2023/PN Mgg serves as a practical example that, even in the absence of digital forensics, judges may admit electronic evidence based on cautious evaluation, considering its relevance and coherence with other evidence.

Therefore, the current legal framework on the admissibility of electronic evidence must be urgently supplemented by binding technical regulations and standardized operational procedures for digital forensics. Without such measures, the validity of electronic evidence will remain subjective, thereby jeopardizing the pursuit of material truth and legal certainty in criminal adjudication.

4. CONCLUSION

This study aims to analyze the legal standing, validity, and evidentiary strength of electronic evidence within the Indonesian criminal procedure system. Employing a normative legal approach, it conducts a comprehensive analysis of the Criminal Procedure Code (KUHAP), the Electronic Information and Transactions (ITE) Law, and Constitutional Court Decision No. 20/PUU-XIV/2016. The findings indicate that electronic evidence has attained normative legitimacy as admissible legal proof. Substantively, such evidence may be classified as documentary evidence, indicative evidence, or even stand-alone evidence, provided it meets formal and material requirements—including the principles of authenticity, integrity, and relevance.

The Constitutional Court's decision represents a pivotal moment in bridging regulatory fragmentation and affirms that electronic evidence is admissible not only in cybercrime cases but in all types of criminal proceedings. The study underscores the essential role of digital forensics in validating the authenticity and reliability of electronic evidence in court. The admissibility of such evidence depends not only on normative legality but also on technical verification—such as audit trails, metadata analysis, a verifiable chain of custody, and certification of electronic systems.

The significance of this research lies in its contribution to the development of scholarly discourse on digital criminal procedure and the urgent need to reform the KUHAP to accommodate technological advancements. A key limitation of this study is its normative focus, which does not incorporate empirical data from broader judicial practice. Therefore, regulatory harmonization between the KUHAP and the ITE Law,

along with the establishment of national digital forensic standards, is necessary to enhance evidentiary quality. Future research should explore empirical analyses of the application of electronic evidence in courtrooms, including comparative studies of jurisdictions with more advanced digital evidence frameworks.

REFERENCES

Journals

Astuti, Sri Ayu. "Perluasan Penggunaan Bukti Elektronik (Evidence of Electronic) Terkait Ketentuan Alat Bukti Sah Atas Perbuatan Pidana Di Ruang Mayantara (Cyberspace)." *Pagaruyuang Law Journal* 1, no. 1 (2017): 44–57. https://doi.org/10.31869/plj.v1i1.269.

Dewantara, Dewa Made Doni, and I Dewa Made Suartha. "Legalitas Alat Bukti Elektronik Sebagai Alat Bukti Dalam Hukum Acara Pidana." *Kertha Desa* 10, no. 8 (2022): 660–69. https://ojs.unud.ac.id/index.php/kerthadesa/article/view/89360.

Gunawan, Tri Agus, and Indira Swasti Gama Bhakti. "Makna Perluasan Alat Bukti Elektronik: Analisis Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016." *Literasi Hukum* 6, no. 2 (2022): 105–16. https://doi.org/10.31002/lh.v6i2.6810.

Lakada, Daniel David Julio. "Perkembangan Pengaturan Alat Bukti Elektronik Dalam Hukum Acara Pidana: Kajian Hukum Tentang Cyber Crime." *Lex Crimen* 12, no. 5 (2024): 1–11. https://ejournal.unsrat.ac.id/v3/index.php/lexcrimen/article/view/59171.

Manurung, Theresia Octaviani, and I Gusti Ayu Agung Ari Krisnawati. "Kedudukan Alat Bukti Elektronik Dalam Sistem Pembuktian Perkara Pidana Di Indonesia." *Kertha Desa* 10, no. 5 (2022): 371–81. https://ojs.unud.ac.id/index.php/kerthadesa/article/view/79114.

Nafatilopa, Princes Elsa, and Tomy Michael. "Legalitas Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Umum Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016." *Jurnal Sosial Humaniora Sigli* 5, no. 2 (2022): 342–51. https://doi.org/10.47647/jsh.v5i2.1018.

Pramata, Aldho Galih. "Analisis Kekuatan Dan Nilai Pembuktian Alat Bukti Elektronik Berwujud CCTV (Closed Circuit Television) Pasca Putusan Mahkamah Konstitusi Nomor 20/PUU-XIV/2016 Dalam Hukum Acara Pidana." *Jurnal Verstek* 8, no. 3 (2020): 392–400. https://doi.org/10.20961/jv.v8i3.47057.

Pratiwi, Feroca Mevihanna Noor, and Sri Wahyuningsih Yulianti. "Penilaian Kekuatan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Penyebarluasan Konten Pornografi Melalui Media Sosial." *Jurnal Verstek* 10,

no. 1 (2022): 59–67. https://doi.org/10.20961/jv.v10i1.63940.

Pribadi, Insan. "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana." *Lex Renaissance* 3, no. 1 (2019): 109–24. https://doi.org/10.20885/JLR.vol3.iss1.art4.

Ramiyanto, Ramiyanto. "Bukti Elektronik Sebagai Alat Bukti Yang Sah Dalam Hukum Acara Pidana." *Jurnal Hukum Dan Peradilan* 6, no. 3 (2017): 463–84. https://doi.org/10.25216/jhp.6.3.2017.463-484.

Utami, Dinda Puspita Tri, and Muhammad Ridwan Lubis. "Legalitas Rekaman Elektronik Sebagai Alat Bukti Dalam Tindak Pidana Pencucian Uang Studi Di Pengadilan Negeri Medan." *Kalam Keadilan* 10, no. 2 (2022): 334–42. http://siakad.univamedan.ac.id/ojs/index.php/kalam-keadilan/article/view/365.

Wirawan, I Made, Oheo K. Haris, and Handrawan Handrawan. "Legalitas Perluasan Penggunaan Alat Bukti Elektronik Dalam Penegakan Hukum Pidana Indonesia." *Halu Oleo Legal Research* 2, no. 1 (2020): 75–85. http://dx.doi.org/10.33772/holresch.v2i1.10604.

Books

Alfitra, Alfitra. *Hukum Pembuktian Dalam Beracara Pidana, Perdata Dan Korupsi Di Indonesia*. Jakarta: Asser, 2014.

Imron, Ali, and Muhamad Iqbal. *Hukum Pembuktian*. Tangerang Selatan: Unpam Press, 2019.

Shinder, Debra Littlejohn, and Michael Cross. *Scene of the Cybercrime*. Oxford: Syngress, 2008.

Subekti, R. *Hukum Pembuktian*. 16th ed. Jakarta: Pradnya Paramita, 2007.