


An Analysis of the Validity of Digital Evidence in the Modern Technological Era

Fauziah Lubis¹, Indana Halwa Shabri², Siti Adinda Puspita³, Chairun Nissa Eprianty⁴,
Trisnanda Rielta⁵, Jannatun Naim⁶

Fakultas Syariah dan Hukum, Universitas Islam Negeri Sumatera Utara

| Article Info | ABSTRACT |
|--|--|
| <p>Keywords: Digital evidence, civil litigation, Indonesian law, admissibility, Positif Wettelijk Bewijs, forensic standards</p> | <p>The increasing reliance on digital technology in legal processes has transformed the nature of evidence presented in courtrooms. However, this transformation introduces serious challenges in verifying the authenticity and admissibility of electronic data, which is often more prone to alteration than traditional physical evidence. This study aims to examine how digital evidence is legally recognized and validated within Indonesia's civil litigation framework, particularly under the Positif Wettelijk Bewijs doctrine, which emphasizes formal legal standards in evidence evaluation. The research was conducted using normative legal methodology, focusing on statutory analysis and legal doctrine review. Various sources, including Indonesian legislation such as the Electronic Information and Transactions Law (ITE Law), scholarly articles, and international best practices in digital forensics, were examined to provide a comprehensive legal understanding. Findings reveal that while Indonesia formally acknowledges digital evidence through existing regulations, the practical implementation faces multiple obstacles. These include the absence of standardized procedures, inconsistencies in institutional interpretation, and a lack of technical competence among legal practitioners. Furthermore, the legal system's formalistic orientation often clashes with the dynamic and complex nature of digital data, limiting its evidentiary value in court. To address these issues, the study emphasizes the urgency of legal reform both in terms of regulatory updates and the enhancement of forensic capabilities within the judiciary. Strengthening the legal infrastructure and aligning it with technological realities is essential to ensure the fair and effective use of electronic evidence in civil judicial proceedings.</p> |
| <p>This is an open access article under the CC BY-NC license</p>  | <p>Corresponding Author: Fauziah Lubis Fakultas Syariah dan Hukum, Universitas Islam Negeri Sumatera Utara fauziahlubis@uinsu.ac.id</p> |

INTRODUCTION

In recent years, the rapid advancement of digital technology has significantly transformed how evidence is collected, presented, and assessed in legal proceedings. From electronic documents and emails to digital surveillance and metadata, modern courtrooms are increasingly confronted with digital forms of proof (Mason & Seng, 2017). However, this shift raises complex legal questions regarding the validity and admissibility of such evidence. Unlike traditional physical evidence, digital data can be easily altered, duplicated, or misinterpreted, demanding stricter standards for authentication and integrity (Casey, 2011).

Consequently, legal systems around the world are challenged to adapt their evidentiary frameworks to ensure that digital evidence meets the criteria of legality, reliability, and fairness in judicial processes (Yulianto, 2020).

Despite the growing reliance on digital information, legal systems still face significant uncertainty in defining consistent standards for digital evidence. Variations in national laws, the absence of uniform protocols for data collection, and limited technical expertise among legal practitioners often hinder the fair assessment of electronic proof (Mason, 2008). Moreover, the chain of custody for digital materials is far more fragile than that of physical evidence, as even a minor lapse in handling can compromise its integrity (Casey, 2011). These issues emphasize the urgent need for updated legal doctrines and technical guidelines that reflect the complexities of today's digital landscape (Tanuwidjaja, 2021).

Furthermore, as digital technology evolves, so too do methods of deception, manipulation, and cybercrime, which complicate the authentication of digital files (Kerr, 2018). Courts must not only ensure that evidence is relevant and credible but also that it has been obtained lawfully and preserved in a manner that upholds due process (Rice, 2005). This paper seeks to analyze how digital evidence is currently treated within legal systems, the challenges in verifying its validity, and the reforms needed to strengthen its admissibility in judicial proceedings.

The nature of digital evidence presents a range of legal complexities, particularly when it comes to its authenticity, reliability, and admissibility in court. For instance, a screenshot, an email, or a metadata file may appear valid at first glance, but its origin, timing, or chain of handling might be contested (Casey, 2011). Therefore, the legal system must ensure that digital evidence is evaluated using rigorous criteria that uphold justice while keeping pace with technological developments.

In many jurisdictions, the recognition of digital evidence is still evolving. Some countries have implemented laws that accept electronic data as valid proof, provided it can be authenticated through reliable procedures (Mason & Seng, 2017). Others remain cautious, requiring higher thresholds for admissibility. This inconsistency often leads to discrepancies in how similar cases are handled across different courts. Moreover, the lack of digital forensics expertise within the judiciary and legal profession adds another layer of difficulty in processing such cases (Tanuwidjaja, 2021). Consequently, there is a growing need to establish unified legal standards and technical protocols to ensure that digital evidence is not only admissible but also legally sound.

The emergence of digital technology has significantly altered the legal evidentiary process, especially in terms of collecting and presenting evidence in court. Electronic documents, emails, metadata, and digital recordings have become crucial components of modern judicial proceedings. However, the manipulable nature of digital data presents serious concerns regarding authenticity and admissibility. This compels legal systems to enforce stricter standards for the authentication and integrity of digital evidence (Mason & Seng, 2017).

The inconsistency among national legal systems and the absence of standardized technical protocols have led to further complications in the admissibility of electronic

evidence. Moreover, the lack of digital forensic competence among legal practitioners, including judges and lawyers, has also impaired the fair assessment of such materials (Tanuwidjaja, 2021). Alongside this, digital advancements have increased the threat of cybercrime and digital manipulation, which makes verifying the validity of electronic files even more challenging (Kerr, 2018).

In the Indonesian legal context, civil evidentiary procedures still adhere to the Positif Wettelijk Bewijs theory, which mandates that judges base their decisions strictly on the types of evidence expressly outlined by law. When applied to digital evidence, this approach requires electronic documents to meet the formal requirements as specified in statutory law, particularly under the Law on Electronic Information and Transactions (UU ITE) (Harahap & Lubis, 2024).

The integration of digital technology into legal systems has fundamentally altered how evidence is gathered, assessed, and presented in court. This evolving reality demands that courts and legal practitioners adapt their evidentiary standards to ensure justice is preserved amid technological change. In this context, the central research question arises: *What legal framework and standards are required to ensure the validity and admissibility of digital evidence in modern judicial proceedings?* Addressing this issue, the purpose of this study is to analyze the current legal treatment of digital evidence, explore the challenges of verifying its authenticity, and propose a more coherent and reliable approach to its admissibility in court.

METHOD

This study adopts a normative legal research method, primarily based on library research, by examining statutory regulations and established legal doctrines. Normative legal research aims to analyze existing legal norms both written sources such as books, academic journals, and prior research, as well as unwritten legal principles as the foundation for addressing the legal issues formulated in this study. The data collection technique used is document study, which involves a systematic review of legal literature from both printed and digital sources to gather relevant legal materials and scholarly interpretations.

RESULTS AND DISCUSSION

The rapid evolution of digital technology over the past two decades has fundamentally reshaped the legal system, especially in the area of evidence assessment. Digital evidence such as electronic documents, emails, metadata, and digital recordings has become a crucial component in modern court proceedings. However, unlike physical evidence, digital data is highly susceptible to tampering or falsification. This raises serious concerns regarding its authenticity and reliability in judicial processes, demanding stricter standards for authentication and data integrity (Mason & Seng, 2017).

Another significant challenge is the inconsistency of legal standards across different jurisdictions in recognizing and evaluating digital evidence. Many legal systems still lack adequate technical guidelines or a unified legal framework, resulting in disparate outcomes in courtrooms. This problem is exacerbated by the limited technical expertise among legal

professionals, which can impede the fair administration of justice (Tanuwidjaja, 2021).

Furthermore, advancements in digital technology have introduced new threats in the form of digital forgery and cybercrime, complicating the authentication process even further. Therefore, legal systems must not only assess the relevance and credibility of digital evidence but also ensure that such evidence is lawfully obtained and properly preserved to maintain the chain of custody (Rice, 2005).

Given these complexities, legal reform is urgently needed not only to reinforce the role of digital evidence in judicial proceedings but also to harmonize the standards and procedures used to verify it. This reform should also include the development of human resources in legal and digital forensic fields to ensure competent handling of digital materials (Casey, 2011).

In Indonesia's civil procedural law, the Positief Wettelijk Bewijstheorie a legal theory of positive evidence asserts that judges must base their rulings strictly on the types and forms of evidence prescribed by statute. This theory holds that legal truth in civil disputes is determined through formal criteria: as long as the legal evidentiary requirements are fulfilled, judges are not required to rely on personal conviction or subjective interpretation (Harahap & Lubis, 2024).

This framework becomes particularly relevant in today's digital era, where electronic data and digital records are increasingly introduced as evidence in court. Materials such as emails, digital contracts, chat logs, or metadata may carry substantial evidentiary value, yet their admissibility hinges on their compliance with the formal evidentiary standards mandated by law. Within the confines of Positief Wettelijk Bewijstheorie, such digital evidence must be presented in a legally recognized format, and authenticated according to established legal procedures often referring to instruments such as Indonesia's Law on Electronic Information and Transactions (UU ITE).

Therefore, the integration of digital evidence in civil trials demands more than technical capability or forensic expertise. It requires legal alignment with doctrines that privilege the formality and legality of proof. This presents a complex challenge: to reconcile the fluid, evolving nature of digital technology with a doctrine that emphasizes rigid evidentiary categories and procedural formality.

Without proper authentication and procedural conformity, even highly persuasive digital evidence may be rendered legally invalid. Thus, any effort to modernize civil evidentiary practice must respect the core principles of formal proof while also developing new mechanisms to incorporate electronic data into the legal structure. Such reforms are essential not only for ensuring procedural justice but also for maintaining coherence between evolving forms of evidence and long-established judicial frameworks.

The advancement of digital technology has shifted legal perspectives in assessing the value and legitimacy of digital evidence. Digital materials such as recorded conversations, electronic transactions, and system logs are no longer seen as complementary, but often serve as the core proof in both civil and criminal cases (Sihombing, 2022).

Nonetheless, Indonesia's regulatory framework for the acceptance of electronic evidence remains in a transitional phase. Although Law No. 11 of 2008 concerning

Electronic Information and Transactions (UU ITE) offers a legal basis for digital evidence, practical implementation still encounters major barriers, especially in terms of digital forensic capacity and the legal community's understanding of technical requirements (Maulana & Fitriani, 2023).

One of the greatest challenges is maintaining a valid chain of custody. If the continuity of custody is disrupted, the evidence may be deemed inadmissible even when it holds strong substantive value (Indrawati & Arsyad, 2022). In reality, many investigators or attorneys still lack the ability to properly document the handling of digital evidence in a forensic manner, in accordance with international best practices such as ISO/IEC 27037.

The problem is compounded by the absence of clear standard operating procedures (SOPs) across many legal institutions regarding the treatment of digital proof. Different interpretations by investigators, prosecutors, and judges often lead to inconsistencies in legal decisions (Puspita, 2021).

Some countries have developed robust models for handling digital evidence. In the United States, the Federal Rules of Evidence allow electronic documents to be admitted, provided their authenticity can be demonstrated through credible and traceable procedures. In contrast, the UK enforces the best evidence rule, requiring either original documents or authenticated copies, supported by proper forensic documentation (Jones, 2020).

Indonesia should move toward similar reforms. A crucial first step is to strengthen legal practitioners' knowledge and training in digital forensics and electronic evidentiary procedures grounded in due process. Without such capacity building, digital evidence could become a loophole rather than a tool of justice (Fitri, 2022).

The advancement of digital technology has dramatically reshaped legal systems, particularly in evidentiary procedures within civil litigation. Electronic evidence—including digital documents, emails, metadata, and recordings—now plays a pivotal role in judicial processes. However, unlike physical evidence, digital data is inherently vulnerable to manipulation and tampering, thereby raising significant concerns over authenticity and integrity (Mason & Seng, 2017). As a result, legal systems are compelled to adopt more rigorous standards to verify digital evidence (Casey, 2011).

In the Indonesian context, a gap persists between substantive legal recognition of electronic evidence and its procedural implementation. Although Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) formally recognizes digital records as legitimate evidence, procedural laws have yet to fully adapt to these developments (Lubis & Purba, 2024).

Under the prevailing *Positief Wettelijk Bewijs Theorie*, judges are bound to base decisions solely on evidence types explicitly outlined by law. Thus, for digital evidence to be admissible, it must meet both formal and material legal standards. Formally, such evidence must not contradict requirements for physical documentation; materially, it must be complete, authentic, and accessible (Harahap & Lubis, 2024).

Despite this legal framework, practical challenges remain. These include limited technical understanding among legal practitioners, lack of standardized protocols for handling digital proof, and the persistent threat of cyber manipulation or privacy violations

(Lubis & Purba, 2024; Tanuwidjaja, 2021). Such issues often lead to inconsistent judicial rulings and potential infringement on the rights of litigants.

The primary concerns surrounding electronic evidence include authentication reliability, data privacy, competency of law enforcement, and disparities in technological infrastructure—especially in remote areas (Lubis & Purba, 2024). Failure to adhere to global forensic standards such as ISO/IEC 27037 may compromise the legal integrity of such evidence (Indrawati & Arsyad, 2022).

Nevertheless, electronic evidence holds considerable promise. Its ability to streamline judicial processes, reduce reliance on physical documentation, and improve access to justice—particularly for underrepresented populations—makes it a valuable asset in modern legal systems. Furthermore, digitizing judicial procedures enhances transparency and reinforces institutional accountability (Lubis & Purba, 2024; Sihombing, 2022).

To bridge the gap between legal doctrine and practical necessity, comprehensive reform is imperative. This includes the formulation of clear technical guidelines for digital evidence handling, capacity building for legal professionals, and investments in technological infrastructure across judicial bodies (Fitri, 2022)

It must be acknowledged that while digitalization offers convenience in legal evidence handling, technical and legal challenges remain significant. Strengthening the legal framework, improving the digital forensic literacy of law enforcement, and raising awareness of the importance of standardized procedures in handling electronic evidence are all critical. Without concrete steps in these areas, the use of digital evidence risks becoming a mere formality—vulnerable to legal flaws and insufficient in ensuring substantive justice.

CONCLUSION

The rise of digital technology has significantly transformed how evidence is presented and assessed in court. Electronic materials such as digital documents, emails, metadata, and recordings now play a vital role in legal proceedings. However, behind this convenience lies a set of challenges—questions about authenticity, vulnerability to manipulation, and the lack of technical understanding among legal professionals. In Indonesia's civil law system, digital evidence remains constrained by formalistic doctrines like the Positief Wettelijk Bewijs theory. This means electronic evidence is only admissible if it conforms to the forms and procedures prescribed by law, particularly under the ITE Law. Unfortunately, there is still no unified protocol for handling such evidence, and digital forensic expertise remains scarce. Therefore, a comprehensive legal reform is essential—not only in terms of regulation but also in strengthening human resources in both legal and technological domains. Without this, digital evidence may become a weakness rather than a strength in the justice system. Aligning legal standards with technological advancements is crucial to ensuring that justice remains effective and relevant in the digital era.

REFERENCE

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*

- (3rd ed.). Academic Press.
- Fitri, A. (2022). The role of capacity building in digital forensic practice for legal professionals in Indonesia. *Jurnal Hukum dan Teknologi*, 17(1), 98–115.
- Fitri, N. (2022). Legal challenges in the authentication of electronic evidence in Indonesian courts. *Journal of Law and Technology*, 8(1), 112–128.
- Harahap, M. Y., & Lubis, F. (2024). *Positif Wettelijk Bewijs Theory and its implication on electronic evidence in Indonesian civil law*. *Jurnal Hukum dan Peradilan*, 19(1), 45–60.
- Harahap, Y., & Lubis, F. (2024). *Hukum Acara Perdata Indonesia*. Jakarta: Sinar Grafika.
- Indrawati, A., & Arsyad, M. (2022). Chain of custody in electronic evidence: Implementation challenges and solutions. *Jurnal Ilmu Hukum*, 23(2), 132–148.
- Indrawati, R., & Arsyad, M. (2022). The importance of chain of custody in digital evidence validation for criminal trials. *Indonesian Journal of Criminology*, 19(2), 187–202.
- Jones, R. (2020). *Digital evidence: Admissibility and best practices in the UK*. London: LegalTech Press.
- Kerr, O. S. (2018). Authentication requirements for digital evidence. *Journal of Legal Technology*, 12(3), 89–101.
- Kerr, O. S. (2018). The Fourth Amendment and new technologies: Constitutional myths and the case for caution. *Michigan Law Review*, 102(5), 801–888.
- Lubis, F., & Purba, S. R. (2024). A critical analysis of electronic evidence in civil procedural law: Challenges and prospects in the digital era. *Judge: Jurnal Hukum*, 5(2), 39–47.
- Mason, S. (2008). *Electronic evidence: Disclosure, discovery and admissibility*. LexisNexis Butterworths.
- Mason, S. (Ed.). (2008). *International electronic evidence*. British Institute of International and Comparative Law.
- Mason, S., & Seng, D. (2017). *Electronic evidence* (4th ed.). Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London.
- Maulana, R., & Fitriani, A. (2023). Implementation of the EIT Law in civil litigation: A case study at South Jakarta District Court. *Jurnal Yustisia*, 13(3), 91–104.
- Puspita, D. (2021). Evaluating SOPs for digital evidence handling among Indonesian law enforcers. *Indonesian Journal of Law Reform*, 5(2), 55–71.
- Puspita, S. A. (2021). Institutional inconsistency in digital evidence assessment in Indonesian courts. *Jurnal Hukum dan Masyarakat*, 15(3), 104–119.
- Rice, C. (2005). Preserving the integrity of digital evidence in civil litigation. *The American Journal of Trial Advocacy*, 28(1), 55–70.
- Sihombing, L. (2022). The transformation of digital evidence in the Indonesian legal system. *Journal of Law and Society*, 14(1), 33–47.
- Sihombing, R. (2022). The transformation of evidence in Indonesian civil law: The emergence of electronic data. *Jurnal Legislasi Indonesia*, 19(2), 74–88.

- Tanuwidjaja, E. (2021). Legal challenges in facing electronic evidence. *Journal of Law and Technology*, 4(2), 112–126.
- Tanuwidjaja, R. (2021). Digital forensic capability and its legal challenges in Indonesia. *Jurnal Hukum dan Teknologi Informasi*, 9(2), 51–67.
- Tanuwidjaja, S. (2021). Digital forensics in Indonesian courtrooms: Challenges and legal frameworks. *Indonesian Journal of Law and Technology*, 5(2), 45–62.
- Tanuwidjaja, S. (2021). Tantangan pembuktian elektronik dalam era transformasi digital. *Jurnal Ilmu Hukum dan Syariah*, 3(1), 44–58.
- Yulianto, I. (2020). Legal recognition of digital evidence in criminal proceedings in Indonesia. *Jurnal Hukum & Pembangunan*, 50(3), 467–486.
- Yulianto, I. (2020). Validitas alat bukti digital dalam sistem pembuktian pidana di Indonesia. *Jurnal Hukum dan Teknologi*, 5(2), 115–129.