Journal of Strafvordering:
https://nawalaeducation.com/index.php/JOSI/index
Jurnal Hukum Pidana Vol.2 No.6, 2026
E-ISSN : 3046-8620
DOI : https://doi.org/10.62872/0hb7ee97

Screenshots, Chats, and Voice Notes: Rethinking Evidence in Criminal Trials

Pramidazzura Alifa Rifqi[1]✉, Samsidar[2], Harly Clifford Jonas Salmon[3]
Universitas Sebelas Maret[1], Universitas Negeri Sulthan Thaha Saifuddin[2], Universitas Pattimura[3]
e-mail: pramdzzr@gmail.com [1]

ABSTRACT

The increasing reliance on screenshots, chats, and voice notes in Indonesian criminal proceedings reflects a significant shift in evidentiary practices driven by digital communication technologies. However, this development has not been followed by adequate normative adaptation within criminal procedural law. Article 184 of the Criminal Procedure Code does not explicitly accommodate micro-digital evidence, while the Electronic Information and Transactions Law merely provides general recognition without specifying procedural standards for authentication and evidentiary weight. This condition creates normative ambiguity regarding the legal status, admissibility, and probative value of screenshots, chats, and voice notes, resulting in inconsistent judicial practices and potential violations of fair trial principles. This study employs normative legal research using statute, conceptual, and case approaches to analyze the position of micro-digital evidence in Indonesian criminal trials. The findings demonstrate that unverified digital evidence risks eroding the presumption of innocence, shifting the burden of proof to defendants, and undermining legal certainty. This article argues that criminal procedural law must be reformed to explicitly regulate the classification, authentication, and corroboration of micro-digital evidence in order to ensure technological adaptation without compromising due process of law and fair trial guarantees.

Keyword: *criminal evidence, digital evidence, screenshots, fair trial, due process of law.*

INTRODUCTION

The rapid expansion of digital communication technologies has fundamentally transformed evidentiary practices within contemporary criminal justice systems, including Indonesia. Screenshots, instant messaging conversations, and voice notes are increasingly relied upon by investigators, prosecutors, and judges as decisive elements in criminal proceedings. In many cases, such micro-digital evidence determines the direction of investigation, supports indictment strategies, and forms the basis of judicial conviction, despite its inherent technical fragility.[1] This phenomenon reflects a structural shift in social interaction patterns that criminal procedure law has yet to fully accommodate.

Unlike conventional evidence, screenshots, chats, and voice notes are inherently vulnerable to manipulation, selective editing, and contextual distortion. Their probative value cannot be presumed solely from visual or auditory appearance, as digital content

[1] Radina Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence," *Computer Law & Security Review* 42 (2021): 105575

can be altered without leaving obvious traces to non-expert evaluators. [2]Nevertheless, Indonesian criminal practice frequently treats such evidence as self-authenticating, admitting it without comprehensive verification of originality, integrity, or chain of custody. This practice reveals a widening gap between evidentiary reliance and normative safeguards.

The core of this problem lies in the outdated structure of Indonesian criminal procedural law. Article 184 of the Criminal Procedure Code (KUHAP) exhaustively enumerates legally recognized means of proof, namely witness testimony, expert testimony, documents, indications, and the statement of the accused.[3] Drafted long before the digital era, KUHAP does not explicitly recognize electronic or digital evidence, let alone micro-digital forms such as screenshots or voice notes extracted from private communication platforms. This legislative silence creates interpretive uncertainty regarding the admissibility and legal classification of such evidence.

Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016, attempts to bridge this gap by recognizing electronic information and electronic documents as lawful evidence. However, the ITE Law adopts a functional recognition model and does not provide procedural standards governing authentication, integrity verification, or evidentiary weighting within criminal trials.[4] As a result, uncertainty persists as to whether screenshots, chats, and voice notes constitute independent means of proof, extensions of documentary evidence, or merely sources of judicial indications (petunjuk) under KUHAP.[5]

This ambiguity constitutes a clear case of normative vagueness in Indonesian criminal procedural law. The absence of explicit standards governing the legal status and evidentiary force of micro-digital evidence has produced inconsistent practices among law enforcement agencies and courts.[6] Identical forms of digital evidence may be treated as decisive proof in one case and dismissed as insufficient in another, undermining legal certainty and equality before the law. Such inconsistency is not merely technical but strikes at the core of procedural justice.

The constitutional dimension of this issue cannot be ignored. Article 28D paragraph (1) of the 1945 Constitution guarantees the right to fair legal certainty and equal treatment before the law. The uncritical acceptance of digital evidence without adequate verification mechanisms risks shifting the burden of proof onto the accused and eroding the presumption of innocence. Moreover, Law No. 1 of 2023 on the National Criminal Code reaffirms the centrality of legality and proportionality principles in criminal justice, which cannot be meaningfully upheld without coherent evidentiary standards.[7]

---

[2] Jakub Matis, "Digital Evidence and Its Use for Criminal Proceedings," *Analytical and Comparative Jurisprudence* (2025).
[3] Law No. 8 of 1981 on Criminal Procedure (KUHAP), art. 184.
[4] Osco Escobedo Miguel Angel et al., "Digital Evidence as a Means of Proof in Criminal Proceedings," *Russian Law Journal* (2023).
[5] Jakub Matis, "Digital Evidence," (2025).
[6] L. V. Milimko and Y. V. Zhydovtsev, "Electronic Evidence in Criminal Proceedings of Ukraine," *Uzhhorod National University Herald: Series Law* (2025).
[7] Law No. 1 of 2023 on the Criminal Code, arts. 1–2.

From an academic standpoint, existing Indonesian scholarship on criminal evidence remains largely centered on conventional evidentiary instruments or discusses electronic evidence in broad, generalized terms.[8] Comparative studies have extensively examined digital evidence in relation to forensic reliability and human rights protection, yet normative legal analysis focusing specifically on screenshots, chats, and voice notes within the Indonesian procedural framework remains scarce. This research gap necessitates a doctrinal reassessment of evidentiary concepts to ensure technological adaptation does not come at the expense of fair trial guarantees. Accordingly, this article aims to analyze the legal position of non-formal digital evidence in Indonesian criminal proceedings and to reconceptualize the evidentiary framework in a manner that reconciles technological realities with due process and fair trial principles.[9]

METHOD

This study employs normative legal research with a prescriptive-critical character.[10] Normative research is essential for identifying doctrinal inconsistencies, normative gaps, and interpretive ambiguities within criminal procedural law governing digital evidence. Rather than documenting empirical practices, this research evaluates legal norms against constitutional principles and fair trial standards.

The statute approach is applied to analyze the relationship between KUHAP, the ITE Law, and the National Criminal Code.[11] This approach exposes the lack of systemic integration between criminal procedural norms and statutory recognition of electronic evidence, particularly concerning micro-digital forms such as screenshots and voice notes. The conceptual approach is used to examine foundational evidentiary concepts, including means of proof, authenticity, integrity of evidence, and due process of law. Conceptual clarification is necessary to assess whether existing doctrinal categories can accommodate digital evidence or require reformulation to maintain procedural fairness.

The case approach complements statutory and conceptual analysis by examining judicial decisions involving screenshots, chat records, and voice notes. This approach reveals inconsistent judicial reasoning caused by normative ambiguity and highlights the practical consequences of evidentiary uncertainty.[12] Legal materials consist of primary (statutes and court decisions), secondary sources (textbooks and peer-reviewed journals), and tertiary sources (legal dictionaries). Normative-systematic analysis is conducted using grammatical, systematic, and teleological interpretation to formulate prescriptive recommendations for evidentiary reform.

RESULT AND DISCUSSION

Normative Ambiguity of the Legal Status of Digital Evidence in the Indonesian Criminal Evidence System

[8] Peter Mahmud Marzuki, *Legal Research* (Jakarta: Kencana, 2017).
[9] Hafiz Omer Abdullah et al., "Digital Evidence in Criminal Proceedings," (2025)
[10] Peter Mahmud Marzuki, *Legal Research* (Jakarta: Kencana, 2017).
[11] V. Petryk, "The Use of Electronic Evidence in Criminal Proceedings: Issues of Collection, Verification, and Evaluation," *Uzhhorod National University Herald: Series Law* (2025).
[12] Lishchak, "Problems and Challenges in the Collection of Evidence," (2025).

The Indonesian criminal evidence system remains structurally anchored to a closed evidentiary model that reflects pre-digital assumptions about proof. Article 184 of the Criminal Procedure Code (KUHAP) enumerates five lawful means of evidence and does not explicitly accommodate digital evidence, particularly micro-digital forms such as screenshots, chat logs, and voice notes. This exhaustive formulation has produced a rigid doctrinal framework in which any evidentiary innovation must be forcibly subsumed under existing categories, often without adequate conceptual justification.[13]

The enactment of the Electronic Information and Transactions Law (ITE Law) attempted to modernize evidentiary recognition by declaring electronic information and electronic documents as lawful evidence. However, this recognition operates at a declarative level and does not integrate electronic evidence into the systematic structure of criminal procedural law. The ITE Law fails to clarify whether electronic evidence constitutes an independent means of proof or merely supplements existing categories under Article 184 KUHAP.[14] This lack of integration generates normative ambiguity rather than normative harmonization.

As a consequence, screenshots, chats, and voice notes are inconsistently classified in practice. In some cases, courts treat them as documentary evidence; in others, they are reduced to circumstantial indications derived from other lawful evidence. This inconsistency is not merely technical but reflects a deeper conceptual confusion regarding the evidentiary nature of micro-digital artifacts, which differ fundamentally from traditional documents in terms of mutability, reproducibility, and dependency on technological systems.[15]

The ambiguity is exacerbated by the absence of statutory standards governing authentication and integrity verification. Neither KUHAP nor the ITE Law provides criteria for determining originality, detecting manipulation, or assessing the reliability of extracted digital content. As a result, evidentiary evaluation is often left to judicial discretion without normative guidance, creating space for subjective assessment and uneven standards across cases.[16] This condition undermines the principle of legal certainty, which requires predictable and uniform application of procedural norms.

From a normative perspective, the failure to clarify the legal status of micro-digital evidence constitutes a form of normative vagueness rather than a mere legislative gap. The law formally recognizes electronic evidence while simultaneously neglecting to define its procedural consequences. This ambiguity allows evidentiary practices to evolve

[13] Law No. 8 of 1981 on Criminal Procedure (KUHAP), art. 18

[14] Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016, art. 5.

[15] Jakub Matis, "Digital Evidence and Its Use for Criminal Proceedings," *Analytical and Comparative Jurisprudence* (2025).

[16] Hafiz Omer Abdullah, Mudassir Maqsood, and Ahmad Nadeem, "Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in the Digital Era," *Research Journal for Social Affairs* (2025).

pragmatically without sufficient doctrinal control, shifting the balance of power toward law enforcement authorities at the expense of procedural safeguards for defendants.[17]

Prescriptively, this condition necessitates a reconceptualization of the evidentiary system. Screenshots, chats, and voice notes should not be treated as self-standing proof equivalent to traditional documents without explicit statutory authorization. Instead, criminal procedural law must clearly define their position, whether as a distinct evidentiary category or as derivative evidence subject to strict corroboration requirements. Without such clarification, the evidentiary system risks normative incoherence and erosion of due process guarantees.[18]

Validity and Probative Value of Screenshots, Chats, and Voice Notes in Judicial Practice

The primary challenge associated with screenshots, chats, and voice notes in criminal proceedings lies in their evidentiary validity. Unlike physical objects or formally issued documents, micro-digital evidence lacks inherent indicators of authenticity. Digital content can be duplicated, altered, or selectively presented without visibly compromising its appearance, rendering traditional methods of evidentiary assessment insufficient.[19] Consequently, the probative value of such evidence cannot be presumed and must be established through verifiable technical processes.

Authenticity and integrity constitute the minimum conditions for admissibility of digital evidence. Authenticity concerns whether the evidence genuinely originates from the claimed source, while integrity relates to whether the content has remained unchanged since its creation. In Indonesian practice, however, screenshots and chat records are frequently admitted without forensic verification, relying solely on visual inspection or contextual testimony. This practice significantly weakens the evidentiary threshold and exposes criminal adjudication to the risk of fabricated or manipulated evidence.

The absence of mandatory supporting evidence further compounds this problem. Ideally, micro-digital evidence should be corroborated by metadata analysis, digital forensic examination, or expert testimony capable of verifying origin, timestamp, and data integrity. Yet, current procedural law does not require such corroboration as a condition of admissibility. As a result, courts may accept screenshots or voice notes as decisive proof even when technical verification is absent or superficial.[20]

This evidentiary laxity creates structural imbalance between the prosecution and the defendant. Defendants often lack the technical capacity or resources to challenge the authenticity of digital evidence presented against them, particularly when such evidence is treated as prima facie reliable. The burden of disproving manipulated digital content

[17] Radina Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence," *Computer Law & Security Review* 42 (2021): 105575.
[18] Osco Escobedo Miguel Angel et al., "Digital Evidence as a Means of Proof in Criminal Proceedings," *Russian Law Journal* (2023).
[19] Christa M. Miller, "A Survey of Prosecutors and Investigators Using Digital Evidence: A Starting Point," *Forensic Science International: Synergy* 6 (2022).
[20] Akmaral Abuova et al., "Prosecutorial Effectiveness in Kazakhstan's Criminal Justice: The Role of Digital Forensics and Online Trial Broadcasting," *Mitteilungen Klosterneuburg* (2025).

effectively shifts to the accused, contradicting the principle that the prosecution bears the burden of proof in criminal cases.[21]

To clarify these distinctions, the following table outlines the normative differences between verified electronic evidence and unverified micro-digital evidence in criminal proceedings.

Table 1. Comparison of Verified Electronic Evidence and Micro-Digital Evidence in Criminal Adjudication

Aspect	Verified Electronic Evidence	Screenshots/Chats/Voice Notes
Legal Recognition	Explicitly recognized under ITE Law	Implicit, derivative recognition
Authentication	Digital forensic verification	Often absent or informal
Integrity Assurance	Metadata and hash validation	High risk of alteration
Evidentiary Weight	High, subject to verification	Should be limited and corroborative
Fair Trial Impact	Procedurally balanced	Risk of burden-shifting

Normatively, screenshots, chats, and voice notes should not possess autonomous probative force unless supported by forensic validation. Prescriptively, criminal procedural reform must establish minimum technical standards for admissibility, including mandatory authentication mechanisms and clear rules on corroboration. Without such standards, the evidentiary system remains vulnerable to abuse and inconsistent judicial outcomes.[22]

Normative Implications of Evidentiary Ambiguity for Fair Trial and Due Process of Law

The normative ambiguity surrounding the admissibility and evidentiary force of screenshots, chats, and voice notes has direct and significant implications for the protection of fair trial and due process of law in criminal proceedings. When procedural law fails to clearly regulate the status and evaluation of micro-digital evidence, judicial practice becomes susceptible to evidentiary shortcuts that prioritize efficiency over procedural safeguards.[23] This condition undermines the foundational principle that criminal adjudication must be conducted through predictable and normatively constrained mechanisms.

One of the most critical implications concerns the erosion of the presumption of innocence. The admission of unverified digital evidence as prima facie proof risks reversing the burden of proof, implicitly requiring defendants to disprove the authenticity or integrity of evidence presented against them.[24] In practice, defendants are often ill-equipped to challenge digital evidence due to technical complexity and resource asymmetry, resulting in structural inequality between prosecution and defense. Such

[21] Radina Stoykova, "Digital Evidence," 105575

[22] Hafiz Omer Abdullah et al., "Digital Evidence in Criminal Proceedings," (2025)

[23] Radina Stoykova, "Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence," *Computer Law & Security Review* 42 (2021): 105575

[24] Hafiz Omer Abdullah, Mudassir Maqsood, and Ahmad Nadeem, "Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in the Digital Era," *Research Journal for Social Affairs* (2025).

imbalance is incompatible with the principle that the prosecution bears the full burden of proving guilt beyond reasonable doubt.

The ambiguity also fosters inconsistent judicial reasoning, which further weakens legal certainty. Courts confronted with similar forms of digital evidence may reach divergent conclusions regarding admissibility and probative value, depending on subjective judicial assessment rather than objective normative standards.[25] This inconsistency undermines the uniform application of criminal procedural law and erodes public confidence in the integrity of the justice system. Legal certainty, as a core element of the rule of law, cannot coexist with evidentiary practices governed primarily by discretion rather than normativity.

From a constitutional perspective, this condition poses a direct threat to the right to fair legal process as guaranteed by Article 28D paragraph (1) of the 1945 Constitution. Due process of law requires not only substantive legality but also procedural fairness, including clear rules governing evidence evaluation.[26] The absence of explicit standards for digital evidence verification allows procedural arbitrariness to persist, exposing defendants to the risk of wrongful conviction based on unreliable or manipulated digital content.

Furthermore, the increasing reliance on micro-digital evidence without normative safeguards contributes to the phenomenon of digital-based criminalization. Conduct may be criminally attributed on the basis of fragmented or decontextualized digital communication, detached from its broader situational context.[27] This trend risks expanding criminal liability beyond its normative justification and conflicts with the principle of proportionality embedded in modern criminal law. Without clear evidentiary thresholds, digital traces may be overinterpreted as conclusive proof of criminal intent or conduct.

Prescriptively, addressing these implications requires a fundamental recalibration of criminal procedural law. Screenshots, chats, and voice notes should be expressly regulated as conditional evidence whose admissibility and probative value depend on strict verification and corroboration standards. Procedural reform must ensure that digital evidence serves as a tool for truth-finding without compromising fairness, equality of arms, and the presumption of innocence.[28] Only through normative clarification can technological adaptation be aligned with constitutional guarantees.

CONCLUSION

The increasing reliance on screenshots, chats, and voice notes in Indonesian criminal proceedings reflects an unavoidable transformation in evidentiary practice driven by digital communication technologies. However, this development has not been accompanied by adequate normative adaptation within criminal procedural law. The

[25] Jakub Matis, "Digital Evidence and Its Use for Criminal Proceedings," *Analytical and Comparative Jurisprudence* (2025).
[26] 1945 Constitution of the Republic of Indonesia, art. 28D(1).
[27] Radina Stoykova, "Digital Evidence," 105575.
[28] Osco Escobedo Miguel Angel et al., "Digital Evidence as a Means of Proof in Criminal Proceedings," *Russian Law Journal* (2023).

absence of explicit regulation concerning the legal status, authentication standards, and probative value of micro-digital evidence has produced normative ambiguity that undermines legal certainty, consistency of judicial reasoning, and procedural fairness.

This study concludes that screenshots, chats, and voice notes cannot be equated with traditional documentary evidence without clear statutory authorization and technical verification requirements. Treating such evidence as autonomous proof in the absence of forensic validation risks eroding the presumption of innocence and shifting the burden of proof onto defendants. Consequently, the current evidentiary framework is incompatible with fair trial and due process principles as constitutionally guaranteed.

Normatively and prescriptively, criminal procedural law must be reformed to explicitly regulate micro-digital evidence. Such reform should include clear classification of screenshots, chats, and voice notes within the evidentiary system, mandatory authentication and integrity verification standards, and strict corroboration requirements. Without these reforms, the use of digital evidence will continue to pose structural risks to justice and undermine the legitimacy of criminal adjudication in the digital era.

REFERENCE

Abdullah, H., Maqsood, M., & Nadeem, A. (2025). Digital Evidence in Criminal Proceedings: Legal Standards, Chain of Custody, and Evidentiary Reliability in The Digital Era. Research Journal for Social Affairs. https://doi.org/10.71317/rjsa.003.05.0375.

Abuova, A., Bakirova, N., Begaliyev, Y., Begaliyev, B., & Malakhov, D. (2025). Prosecutorial Effectiveness in Kazakhstan's Criminal Justice: The Role of Digital Forensics and Online Trial Broadcasting. Mitteilungen Klosterneuburg. https://doi.org/10.61586/fg5be.

Abuova, A., Bakirova, N., Begaliyev, Y., Begaliyev, B., & Malakhov, D. (2025). Prosecutorial Effectiveness in Kazakhstan's Criminal Justice: The Role of Digital Forensics and Online Trial Broadcasting. Mitteilungen Klosterneuburg. https://doi.org/10.61586/fg5be

Al-Billeh, T., Al-Hammouri, A., Khashashneh, T., Makhmari, M., & Kalbani, H. (2024). Digital Evidence in Human Rights Violations and International Criminal Justice. Journal of Human Rights, Culture and Legal System. https://doi.org/10.53955/jhcls.v4i3.446

Angel, O., Mercedes, C., Elisa, Q., Joaquin, D., De Oliveira Diaz Deny Giovanna, C., & Beatriz, G. (2023). DIGITAL EVIDENCE AS A MEANS OF PROOF IN CRIMINAL PROCEEDINGS. Russian Law Journal. https://doi.org/10.52783/rlj.v11i5s.895.

Hoxhaj, A. (2025). The CJEU Ruled that the EncroChat Data can be Admissible Evidence in the EU. European Journal of Risk Regulation. https://doi.org/10.1017/err.2025.10047.

Lishchak, A. (2025). Problems and challenges in the collection of evidence in misdemeanor cases: key issues faced by investigators and prosecutors during evidence gathering. Analytical and Comparative Jurisprudence. https://doi.org/10.24144/2788-6018.2025.05.3.31.

Luhina, N., & Paliukh, O. (2025). PECULIARITIES OF PROOF IN CRIMINAL PROCEEDINGS RELATED TO CYBERCRIME. Social Development: Economic and Legal Issues. https://doi.org/10.70651/3083-6018/2025.4.27.

Marzuki, P. M. (2017). Penelitian hukum (Edisi revisi). Kencana.

Matis, J. (2025). Digital evidence and its use for criminal proceedings. Analytical and Comparative Jurisprudence. https://doi.org/10.24144/2788-6018.2025.03.3.19.

Matis, J. (2025). Digital evidence and its use for criminal proceedings. Analytical and Comparative Jurisprudence. https://doi.org/10.24144/2788-6018.2025.03.3.19.

Milimko, L., & Zhydovtsev, Y. (2025). Electronic evidence in criminal proceedings of Ukraine. Uzhhorod National University Herald. Series: Law. https://doi.org/10.24144/2307-3322.2025.88.3.45.

Miller, C. (2022). A survey of prosecutors and investigators using digital evidence: A starting point. Forensic Science International: Synergy, 6. https://doi.org/10.1016/j.fsisyn.2022.100296.

Petryk, V. (2025). The use of electronic evidence in criminal proceedings: issues of collection, verification, and evaluation. Uzhhorod National University Herald. Series: Law. https://doi.org/10.24144/2307-3322.2025.87.4.17.

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Comput. Law Secur. Rev., 42, 105575. https://doi.org/10.1016/j.clsr.2021.105575.

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Comput. Law Secur. Rev., 42, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Sujatmiko, B., & Soesatyo, B. (2025). The Urgency of Using Electronic Evidence in Trials as an Effort to Answer the Challenges of Law Enforcement in the Digital Era and Social Media Dynamics. Asian Journal of Social and Humanities. https://doi.org/10.59888/ajosh.v3i9.567.

Sujatmiko, B., & Soesatyo, B. (2025). The Urgency of Using Electronic Evidence in Trials as an Effort to Answer the Challenges of Law Enforcement in the Digital Era and Social Media Dynamics. Asian Journal of Social and Humanities. https://doi.org/10.59888/ajosh.v3i9.567.