priviet lab.
RESEARCH & PUBLISHING

Priviet Social Sciences Journal

Volume 6
Issue 4 April, 2026

Article 39

22-04-2026

Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity

Litya Surisdani Anggraeniko, Auliah Ambarwati, Feby Reski Utami

To cite this article: Anggraeniko, L. S., Ambarwati, A., & Utami, F. R. (2026). Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity. *Priviet Social Sciences Journal, 6*(4), 483-494.
https://doi.org/10.55942/pssj.v6i4.1566

To link to this article: https://doi.org/10.55942/pssj.v6i4.1566

Private Social Sciences Journal
E-ISSN 2798-6314
P-ISSN 2798-866X
https://doi.org/10.55942/pssj.v6i4.1566

Volume 6
Issue 4
April Edition 2026

Admissibility of digital evidence in Indonesia: Criminal–civil implications for the chain of custody and evidentiary validity

Litya Surisdani Anggraeniko, Auliah Ambarwati*, Feby Reski Utami

Universitas Sultan Ageng Tirtayasa, Jl. Raya Jkt No.3, Sindangsari, Kec. Pabuaran, Kota Serang, Banten 42163, Indonesia
*e-mail: auliah.ambarwati@untirta.ac.id

Received 20 January 2026
Revised 15 March 2026
Accepted 22 April 2026

ABSTRACT

Digital evidence has become a cornerstone of modern litigation in Indonesia; however, its admissibility remains complex because of the varying standards of proof across legal regimes. This study analyzes the construction of digital evidence admissibility following the enactment of Law No. 20 of 2025 (The New Criminal Procedure Code) and its harmonization with Law No. 11 of 2008 (UU ITE). Methodologically, this research employs a doctrinal legal analysis with a conceptual and statutory approach, utilizing court judgments as doctrinal illustrations to identify judicial inconsistencies in handling electronic data. The findings reveal that while Article 177 paragraph (1) letter f of Law No. 20/2025 now explicitly recognizes electronic information as independent evidence, its validity is strictly contingent upon Chain of Custody (CoC) compliance. In criminal proceedings, CoC lapses, such as failure in hashing or unauthorized access, frequently lead to the exclusion of evidence beyond a reasonable doubt. Conversely, in civil cases, procedural defects typically result in a reduction in probative value rather than total inadmissibility, governed by the principle of functional equivalence. To mitigate judicial disparity, this study proposes a Criminal–Civil Admissibility Matrix and a Minimum CoC Checklist comprising five technical indicators: lawful acquisition, hashing, forensic imaging, documented transfer, and expert certification. These frameworks serve as normative guides to ensure the integrity, authenticity, and reliability of digital proof in the Indonesian judiciary.

Keywords: admissibility; chain of custody; digital evidence; evidentiary validity; Indonesia

1. INTRODUCTION

The rapid digitalization of policing, commerce, and court administration has driven a surge in the use of digital evidence in criminal and civil litigation in Indonesia. Statutorily, Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law No. 19 of 2016 and Law No. 1 of 2024, recognizes Electronic Information/Electronic Documents and their printouts as lawful evidence, whereas the earlier KUHAP regime under Article 184 of Law No. 8 of 1981 did not expressly list digital evidence as a standalone category (Indonesia, 1981; Indonesia, 2008; Indonesia, 2016; Indonesia, 2024; Isima, 2022).

In parallel, Supreme Court Regulation No. 1 of 2019, as amended by Supreme Court Regulation No. 7 of 2022, institutionalizes electronic administration and e-litigation, increasing the volume and centrality of digital exhibits in courtrooms (Jayani et al., 2020; Mahkamah Agung Republik Indonesia, 2019; Mahkamah Agung Republik Indonesia, 2022). However, practice remains uneven: judges and litigants have long had to reconcile general procedural rules with special legislation, which creates an urgency to harmonize technical-procedural baselines, especially the chain of custody (CoC), which safeguards authenticity, integrity, and reliability from acquisition to presentation (Ilyas, 2021).

Scholarship and case discussions generally support the acceptance of e-evidence where authenticity and integrity are verifiable through hashing, forensic imaging, access logs, and expert testimony, and forensic best practice is guided by SNI ISO/IEC 27037:2014, together with broader digital-forensic guidance such as NIST SP 800-86 and governance requirements in Government Regulation No. 71 of 2019 on Electronic Systems and Transactions (Badan Standardisasi Nasional, 2014; Indonesia, 2019; Kent et al., 2006). Simultaneously, constitutional jurisprudence underscores that unlawfully obtained evidence may be disqualified or discounted, reinforcing the CoC's centrality (Mahkamah Konstitusi Republik Indonesia, 2016; Ratnasari, 2018).

Against this backdrop, the literature still reveals gaps in how courts consistently link CoC compliance to admissibility (entry into evidence) and weight (probative value), especially across different standards of proof in criminal and civil proceedings (Efendi, 2020). Accordingly, this study asks: (1) How is the admissibility of digital evidence constructed and applied in criminal and civil cases under KUHAP, UU ITE, and e-court regulations?; (2) To what extent does CoC compliance, including early hashing, forensic imaging, write-blockers, CoC forms, and access logs, shape validity (authenticity, integrity, reliability) and evidentiary weight?; and (3) What minimum CoC indicators should be adopted to harmonize technical and procedural practices to ensure that judicial assessments are more consistent?.

2. METHOD

This study employs a non-empirical desk-based doctrinal legal research design. A non-empirical approach is justified because the central problem, the normative disharmony between general procedural law and specialized digital regulations, requires a conceptual and statutory synthesis rather than empirical data collection. This analysis primarily focuses on Law No. 20/2025 and UU ITE. Court judgments are used as doctrinal illustrations to highlight judicial interpretation and identify real-world inconsistencies rather than as a statistical dataset. The analytical procedure follows a qualitative-normative logic by systematizing formal requirements and synthesizing forensic standards within the legal framework.

2.1. Sources and Corpus

First, the primary sources are Indonesian positive laws relevant to digital evidence: Law No. 20 of 2025, Law No. 11 of 2008 as amended by Law No. 19 of 2016 and Law No. 1 of 2024, Government Regulation No. 71 of 2019, Supreme Court Regulation No. 1 of 2019 as amended by Supreme Court Regulation No. 7 of 2022, Constitutional Court Decision No. 20/PUU-XIV/2016, and SNI ISO/IEC 27037:2014 (Badan Standardisasi Nasional, 2014; Indonesia, 2008; Indonesia, 2016; Indonesia, 2019; Indonesia, 2024; Indonesia, 2025; Mahkamah Agung Republik Indonesia, 2019; Mahkamah Agung Republik Indonesia, 2022; Mahkamah Konstitusi Republik Indonesia, 2016). Second, secondary sources

are scholarly articles, commentaries, and practice notes on electronic evidence, authenticity, integrity, reliability, and chain of custody (CoC). Third, illustrative materials are a small number of publicly available judgments cited narratively to exemplify doctrinal points and not as a systematic dataset.

2.2. Analytical Procedure

First, concept framing: clarify admissibility vs. evidentiary weight and the validity triad (authenticity, integrity, reliability), locating CoC as the procedural safeguard. Second, normative synthesis: reading KUHAP, UU ITE, Perma, and PP together (*lex specialis* and e-litigation context) and aligning them with SNI 27037 for the technical baseline of CoC (identification, collection, acquisition, and preservation). Third, comparative reasoning (criminal vs. civil): explain how different standards of proof shape the consequences of weak/strong CoC (e.g., exclusion or sharp downgrading in criminal; weight reduction more common in civil). Fourth, deriving practice tools: translating the synthesis into two outputs promised in the abstract: a Criminal–Civil Admissibility Matrix (linking CoC compliance to admissibility/weight) and a Minimum CoC Checklist (hashing at acquisition, forensic imaging, write blocker, CoC/transfer log, access log, expert testimony).

2.3. Quality & Ethical Considerations

Triangulate statements across statutes, court policies, and reputable scholarship; cross-check technical terms against SNI 27037. All sources are publicly available, and no personal data were collected.

2.4. Limitations

As a desk study, the analysis is argumentative rather than empirical; it does not quantify courtroom practice and depends on the completeness and clarity of the written sources. Therefore, the outputs are guidance-oriented and not statistical claims.

3. RESULTS AND DISCUSSION

3.1. The Admissibility of Digital Evidence Constructed and Applied Across Criminal and Civil Cases Under KUHAP, UU ITE, and E-Court Regulations

The admissibility of digital evidence in Indonesian courts presents a dynamic and intricate legal challenge (Cahyani et al., 2016). It is characterized by the tension between the conventional procedural laws (KUHAP) and the special legislation that explicitly recognizes digital evidence, primarily Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended, which is further supported by the electronic judicial administration system (E-Court).

3.1.1. Legal Foundation and Status: The Role of UU ITE

The UU ITE (Article 5, paragraphs 1 and 2) serves as the primary legal umbrella, explicitly recognizing Electronic Information and/or Electronic Documents and/or their printed results as valid legal evidence. The statute positions electronic evidence as an extension of evidence recognized by prevailing procedural laws, thereby addressing the earlier vacuum in both criminal and civil procedures and granting electronic documents equivalent legal force as long as formal and material requirements are met (Indonesia, 2008; Indonesia, 2016; Indonesia, 2024; Mulyana, 2021).

However, limitations on admissibility remain important. Under Article 5, paragraph (4) of the UU ITE, digital evidence is not admissible where the relevant information or document must, by law, exist in conventional written form or must be executed as a notarial deed or a deed made by an authorized official (Indonesia, 2008; Indonesia, 2016; Indonesia, 2024).

3.1.2. Admissibility in Criminal Cases (KUHAP and UU ITE)

Under the earlier KUHAP regime, Article 184 (1) of Law No. 8 of 1981 strictly defined five valid types of evidence: witness testimony, expert testimony, letters, clues (*petunjuk*), and defendant testimony, while digital evidence was not expressly listed (Indonesia, 1981; Ipakit, 2015). By contrast, Law No. 20 of

2025 recognizes electronic information/documents as independent evidence under Article 177 paragraph (1) letter f (Indonesia, 2025).

3.1.2.1. Conflict Resolution: The Lex Specialis Principle

To integrate digital evidence into the criminal justice system, the principle of *lex specialis derogat legi generali* (special law supersedes general law) has been applied. The UU ITE functioned as a *lex specialis* affirming the validity of electronic evidence, even when the earlier KUHAP framework did not expressly enumerate it. In practice, under the prior regime, digital evidence was often treated as a letter (if printed) or as a clue/*petunjuk*, provided that its veracity was corroborated by other evidence, especially expert testimony in digital forensics (Indonesia, 1981; Indonesia, 2008; Indonesia, 2016; Indonesia, 2024; Isima, 2022).

3.1.2.2. Formal and Material Requirements (Constitutional Court Decision)

The admissibility of digital evidence in criminal cases hinges critically on satisfying both formal (procedural) and material (content) requirements, which are heavily influenced by Constitutional Court Decision No. 20/PUU-XIV/2016 and the statutory framework of the UU ITE (Indonesia, 2008; Indonesia, 2016; Indonesia, 2024; Mahkamah Konstitusi Republik Indonesia, 2016).

First, there are formal requirements (lawful acquisition). These requirements focus on the legal process of obtaining evidence, emphasizing the exclusionary rule: evidence obtained unlawfully is vulnerable to exclusion or serious discounting. This stage, therefore, requires clear documentation of seizures, interceptions, or other investigative acts, supported by procedurally valid records that can later be presented in court (Mahkamah Konstitusi Republik Indonesia, 2016; Mualfah & Ramadhan, 2020) (see Table 1).

Table 1. Methods and Requirements for Obtaining Evidence

Requirement	Description	Legal Basis
Search and Seizure	Must adhere to the KUHAP procedure, requiring a Warrant/Permit from the Head of the District Court for the seizure of electronic systems or data.	Article 43 UU ITE and Articles 77-82 KUHAP
Interception	This must be carried out upon the request of investigators and with a Warrant from the Head of the District Court, based on explicit law (not general crimes).	Article 31 and Article 42 of the UU ITE
Voluntary Submission	For evidence that is not the direct output of the suspect/defendant (e.g., from a third-party server), the decision mandates that it must be obtained through a legal investigative procedure (i.e., seizure with a warrant).	MK Decision No. 20/PUU-XIV/2016

Source: Mahkamah Konstitusi Republik Indonesia (2016)

Second, material requirements (authenticity and integrity) must be met. These requirements focus on the quality and reliability of the data itself: (1) integrity, meaning the data must be demonstrably intact and free from alteration or manipulation since its creation or recording; (2) authenticity, meaning the data must be provably genuine and verifiable as what it purports to be; and (3) accessibility, meaning the information must be capable of being accessed, displayed, and accounted for in explaining a specific condition or event (Indonesia, 2008; Indonesia, 2016; Indonesia, 2019; Indonesia, 2024).

Third, the indispensable role of digital forensics must be emphasized. Digital forensics is not merely an additional tool but a practical requirement for proving the admissibility of digital evidence in criminal trials. Forensic experts are expected to maintain the Chain of Custody, apply forensically sound handling procedures, and provide expert testimony certifying integrity and authenticity, thereby supporting the use of digital material as valid evidence (Badan Standardisasi Nasional, 2014; Kent et al., 2006).

3.1.3. Admissibility in Civil Cases (HAP, UU ITE, and E-Court)

Similar to the criminal sphere, conventional civil procedure law did not originally enumerate electronic evidence as a discrete category, instead recognizing written evidence, witness testimony, presumptions, confessions, and oaths. The legal gateway is provided by the UU ITE through the principle of functional equivalence, while the practical facilitator is the e-Court framework under Supreme Court Regulation No. 1 of 2019 and its amendment in Supreme Court Regulation No. 7 of 2022, which enables electronic filing and hearings (Indonesia, 2008; Indonesia, 2016; Indonesia, 2024; Mahkamah Agung Republik Indonesia, 2019; Mahkamah Agung Republik Indonesia, 2022) (see Table 2).

Table 2. Implementation of the e-Court System

Aspect	E-Court Regulation & Practice	Implication for Admissibility
Submission	Electronic documents (emails, PDFs, digital recordings, and screenshots) can be uploaded and registered as evidence in the e-Court system.	Streamlines the administrative process for introducing digital evidence.
Evidentiary Weight	Digital evidence submitted is generally treated as **Written Evidence** (*Bukti Surat*).	Its probative value is assessed under conventional rules for written evidence (i.e., it must be genuine and relate to the facts).
Verification Challenge	If the opposing party **denies the authenticity** of the digital evidence (e.g., a WhatsApp chat screenshot), the burden shifts to the party submitting the evidence to prove its authenticity.	The court may require **expert testimony** (Digital Forensics) or other corroborating evidence to establish the integrity of the digital file.

Source: Mahkamah Agung Republik Indonesia (2019) and Mahkamah Agung Republik Indonesia (2022)

The challenge in civil cases lies less in formal prohibition and more in authenticity verification when they are challenged. If digital evidence is easily manipulable (like simple screenshots without metadata), judges may accord it only weak probative value, treating it merely as an Initial Clue (preliminary evidence) unless strongly corroborated.

3.1.4. Key Legal Instruments and Data

For more details, see Table 3.

Table 3. Legal Instruments

Regulation/Document	Subject Area	Relevance to Admissibility
Law No. 11/2008 (as amended by No. 19/2016) on ITE	Primary legal basis for digital evidence	**Article 5 (1) and (2):** Establishes validity of the study. **Article 44:** Enforces the Exclusionary Rule (lawful acquisition)
KUHAP (No. 20/2025)	Criminal Procedural Law	**Article 177 (1) f**: Establishes digital evidence as an independent and valid legal evidence
Constitutional Court Decision No. 20/PUU-XIV/2016	Formal requirements for digital evidence in criminal cases.	**Mandates lawful interception/seizure procedures (warrant)** for digital evidence obtained from third parties to be admissible.
Peraturan Mahkamah Agung (Perma) No. 1 of 2019	E-Court administration.	Facilitates the electronic submission of digital evidence in civil cases, treating it as equivalent to written evidence for procedural purposes.
Hukum Acara Perdata	Civil Procedural Law.	Conventional law: digital evidence accommodated as an extension of **Written Evidence**.

Source: Compiled from Indonesia (2008), Indonesia (2016), Indonesia (2019), Indonesia (2024), Indonesia (2025), Mahkamah Agung Republik Indonesia (2019), Mahkamah Agung Republik Indonesia (2022), and Mahkamah Konstitusi Republik Indonesia (2016)

3.2. The Role of Chain of Custody (CoC) in Determining the Validity and Evidentiary Weight of Digital Evidencez

The extent to which Chain of Custody (CoC) compliance shapes the validity (authenticity, integrity, and reliability) and evidentiary weight of digital evidence is fundamental. Because electronic information is inherently fragile and susceptible to modification, the CoC bridges the gap between raw data collection and legal admissibility requirements. Compliance with CoC protocols transforms raw digital data into legally defensible evidence by establishing forensic soundness, whereas a complete custody record documents every stage of handling from the first discovery to courtroom presentation (Badan Standardisasi Nasional, 2014; Cantika et al., 2025; Kent et al., 2006).

3.2.1. CoC and the Three Pillars of Validity (Authenticity, Integrity, and Reliability)

CoC compliance directly addresses the legal requirements for admissibility by systematically proving that the evidence presented in court is the same as that initially collected.

3.2.1.1. Integrity (The Core Function of CoC)

Integrity is the most direct legal requirement addressed by the CoC. In practice, integrity means that the evidence must not have been altered, damaged, or corrupted since collection, which is why forensic standards emphasize hashing, preservation of the original media, and controlled acquisition procedures (Badan Standardisasi Nasional, 2014; Kent et al., 2006) (see Table 4).

Table 4. Integrity Impact of CoC

CoC Technique	Impact on Integrity
Early Hashing	**Crucial.** Generating a mathematical fingerprint (hash value, e.g., SHA-256 or MD5) of the data *immediately* after collection. Any change to a single bit of the data will result in a different hash value, mathematically proving whether the integrity is maintained throughout the CoC.
Forensic Imaging (Bit-Stream Copying)	Creating an exact, sector-by-sector replica of the original storage medium. This preserves the original state of the device, ensuring that the investigation and analysis are performed on a copy, thus protecting the integrity of the primary source.
Write Blockers	**Essential.** Hardware or software tools that physically or logically prevent writing commands from reaching the original media. This guarantees that the process of viewing or copying data does not inadvertently modify any files or metadata on the source device.

Source: Adapted from Badan Standardisasi Nasional (2014) and Kent et al. (2006)

3.2.1.2. Authenticity (Proving the Source)

Authenticity relates to proving that the evidence is genuine and originates from a claimed source (see Table 5).

Table 5. Authenticity impact of CoC

CoC Technique	Impact on Authenticity
CoC Forms and Access Logs	It is important to document who had possession of the evidence, where it was stored, and the exact time and date of any access or transfer. This continuous record links the evidence directly to the original source and collection time, establishing a clear provenance.
Metadata Preservation	Forensic imaging and write blockers ensure that critical system metadata (such as timestamps, access times, and file creation dates) remain unchanged. This metadata is key to proving when and where the evidence was created, directly supporting its authenticity.

Source: Adapted from Badan Standardisasi Nasional (2014) and Kent et al. (2006)

3.2.1.3. Reliability (Proving the Process)

Reliability pertains to the trustworthiness of the process used to acquire and handle evidence (see Table 6).

Table 6. Reliability Impact of CoC

CoC Technique	Impact on Reliability
Standardized Procedures (SOP)	The CoC requires adherence to internationally accepted digital forensic standards (e.g., ISO/IEC 27037). Documenting compliance with these standards proves that the methodology used was scientifically sound and reliable.
Expert Testimony	The forensic examiner's ability to demonstrate a perfect CoC record, supported by logs and hash verification, lends professional credibility to their findings, thus confirming the reliability of the evidence.

Source: Adapted from Badan Standardisasi Nasional (2014) and Kent et al. (2006)

3.2.2. CoC and Evidentiary Weight

In court, evidentiary weight (*bobot pembuktian*) is the degree of influence that evidence has on the judge's conviction. In Indonesia's criminal system, this remains tied to the requirement of legally valid evidence accompanied by a judicial conviction, now restated in Article 183 of Law No. 20 of 2025 (Indonesia, 2025; Mualfah & Ramadhan, 2020).

3.2.2.1. Criminal Cases (KUHAP)

Under the Indonesian criminal system, particularly where evidence is categorized as an indication (*petunjuk*) (as digital evidence often is), a robust CoC is critical to ensure its admissibility. Eliminating Doubt: A perfect CoC record, verified by matching hash values, eliminates reasonable doubt that the evidence was manipulated. This high level of certainty dramatically increases the persuasive value of the evidence, making the judge more confident in its use for conviction.

3.2.2.1. Corroboration

When expert testimony confirms integrity based on a documented CoC, digital evidence can function as independent proof under Article 177, paragraph (1), letter f of Law No. 20 of 2025. This directly supports the minimum-evidence requirement under Article 183 of the same law, so that digital evidence with verified forensic integrity carries far greater probative weight than unverified electronic material under the previous regime (Indonesia, 2025).

3.2.2.1. Civil Cases (UU ITE and E-Court)

One of the duties of a judge in a civil court proceeding in Indonesia is to examine whether the legal relationship forming the basis of a lawsuit exists. If the plaintiff seeks to win the case, the existence of a legal relationship underlying the claim must be proven. This necessity to substantiate the alleged facts makes the evidentiary stage crucial to the judicial process (Soroinda & Nasution, 2022).

In civil law, where the evidentiary burden rests on the party submitting the document, the CoC directly affects the ability to overcome a denial (*penyangkalan*) by the opposing party. If authenticity is challenged, the submitting party must prove its validity through metadata, forensic handling, or expert testimony. Without proper CoC documentation, judges are more likely to treat the material as weak preliminary evidence rather than strong documentary evidence. Conversely, strong CoC compliance allows electronic documents to better satisfy the principle of functional equivalence in e-court practice (Mahkamah Agung Republik Indonesia, 2019; Mahkamah Agung Republik Indonesia, 2022; Soroinda & Nasution, 2022).

3.2.3. Summary of CoC Compliance Requirements

For more details, see Table 7.

Table 7. CoC Admissibility Impact

CoC Component	Purpose	Admissibility Impact
Early Hashing	Proves the integrity of the collected data.	**Essential:** Provides irrefutable mathematical proof against tampering
Write Blockers	Prevents accidental alteration of the original source media	**Essential:** Proves that the acquisition process was non-destructive and legal.
Forensic Imaging	An identical working copy was created for analysis.	**Critical:** It protects the original evidence from further handling and establishes the "what" of the evidence.
CoC Forms & Access Logs	Document transfer, storage, and access history.	**Formal Requirement:** Proven documented and accountable sequence of events (*provenance*) for the evidence.

Source: adapted from Badan Standardisasi Nasional (2014), Indonesia (2025), and Kent et al. (2006)

In conclusion, CoC compliance is the lifeblood of digital evidence collection. Any break in the chain, missing hash values, or undocumented transfer renders the evidence vulnerable to challenge on the grounds of integrity and authenticity, potentially causing a judge to exclude the evidence (in criminal law) or assign it a negligible evidentiary weight (in civil law).

3.3. CoC Indicators should be Adopted to Harmonize Technical–Procedural Practice so that Judicial Assessment is More Consistent

3.3.1. Documented Legal Authority for Collection (The Formal Indicator)

This indicator satisfies the fundamental procedural requirement under the KUHAP and the Constitutional Court Decision No. 20/PUU-XIV/2016. First, the indicator requires a mandatory record attached to the evidence detailing the specific legal basis used to authorize the collection or seizure of the electronic device/data, such as an investigation order or search-and-seizure warrant. Second, its harmonization impact is that it ensures judicial consistency by demonstrating that lawful acquisition was satisfied ab initio; without this, exclusion becomes more likely (Ginting & Joesoef, 2025; Indonesia, 2025; Mahkamah Konstitusi Republik Indonesia, 2016).

3.3.2. Immediate Hashing and Hash Verification (The Integrity Indicator)

This is the single most important technical step for proving integrity, as required by the UU ITE and reinforced by the forensic standards. The hash value (e.g., SHA-256) of the original evidence or forensic image should be calculated immediately upon collection, recorded on the CoC form and/or evidence tags, and re-verified against the working copy during analysis and prior to submission in court. This provides judges with an objective and technically reproducible metric to verify that the digital data have not been altered (Badan Standardisasi Nasional, 2014; Indonesia, 2008; Indonesia, 2016; Indonesia, 2024).

3.3.3. Use of Write-Blocking Technology (The Protection Indicator)

This indicator confirms that the original evidence was protected from accidental alteration during the acquisition process. The use of a hardware or software write-blocker should be declared in the CoC record when accessing and imaging the original media, because this demonstrates non-destructive handling and strengthens claims of integrity and reliability (Badan Standardisasi Nasional, 2014; Kent et al., 2006).

3.3.4. Itemized and Time-Stamped Transfer Log (The Accountability Indicator)

A simplified, standardized record of all transfers is essential to ensure accountability and continuity. At a minimum, the CoC form should identify the item, record the releasing and receiving custodians, describe the action taken (e.g., transfer, storage, or analysis), and include exact timestamps for every change in custody. Such provenance-based documentation allows judges to trace the continuity of possession and assess reliability more consistently (Badan Standardisasi Nasional, 2014).

3.3.5. Signed Expert Certification of Forensic Soundness (The Reliability Indicator)

This final step connects the technical process to the legal finding, transforming the digital data into reliable expert evidence. A signed certification by a qualified digital forensic expert should attest that the acquisition and analysis followed recognized forensic principles, that the hash values were successfully verified across the evidence life cycle, and that the findings were reproducible. This substantially increases probative weight and supports the recognition of digital evidence under Article 177, Paragraph (1), Letter f of Law No. 20 of 2025 (Badan Standardisasi Nasional, 2014; Indonesia, 2025; Kent et al., 2006).

4. CONCLUSION

The transition from the earlier procedural framework to Law No. 20 of 2025 marks a pivotal evolution in Indonesia's evidentiary law, providing much-needed statutory clarity regarding digital evidence. This study concludes that admissibility is not merely a matter of formal legal recognition but is fundamentally rooted in the technical integrity of the Chain of Custody (CoC). The explicit inclusion of electronic documents as independent evidence under Article 177 of the new KUHAP reduces the earlier 'extension' or 'analogy' debate while simultaneously heightening the demand for forensic precision (Indonesia, 2025).

Our analysis demonstrates a clear divergence in judicial treatment: criminal courts apply a stricter exclusionary approach toward CoC failures to protect the rights of the accused, whereas civil courts are more likely to respond through probative weight reduction. Because this divergence can generate uncertainty, implementing a standardized minimum CoC checklist that integrates forensic standards such as SNI ISO/IEC 27037:2014 into procedural practice is no longer optional but necessary. The proposed criminal–Civil Admissibility Matrix offers a structured mechanism for a more consistent judicial assessment. Ultimately, safeguarding the life cycle of digital data through hashing, forensic imaging, and transfer logging is central to fair trial guarantees and legal certainty, and future implementing regulations under Law No. 20 of 2025 should provide a tighter bridge between forensic science and courtroom practice (Badan Standardisasi Nasional, 2014; Indonesia, 2025; Mahkamah Konstitusi Republik Indonesia, 2016).

Ethical Approval

Not Applicable

Informed Consent Statement

Not Applicable

Authors' Contributions

LSA, ARA, and FRU contributed to all aspects of this study. LSA conceptualized and formulated the problem, particularly the development of the three core research questions, and prepared the initial draft, including the proposed Admissibility Matrix model. ARA was responsible for the normative legal analysis and primary data curation, including KUHAP, the ITE Law, and Supreme Court Regulations, and conducted a comparative analysis across criminal and civil law regimes. FRU designed the overall

methodology and analytical procedure, verified the technical findings against the SNI ISO/IEC 27037 standards, and carried out the final substantive review and editing, including the development of the harmonizing Minimum CoC Checklist. All the authors have read and approved the final version of the manuscript.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

Data Availability Statement

The data supporting the findings of this study are not primary data but are sourced entirely from publicly available Indonesian statutes and regulations (Law No. 20 of 2025, Law No. 11 of 2008 as amended by Law No. 19 of 2016 and Law No. 1 of 2024, Government Regulation No. 71 of 2019, and Supreme Court Regulation No. 1 of 2019 as amended by Supreme Court Regulation No. 7 of 2022), the Constitutional Court Decision No. 20/PUU-XIV/2016, SNI ISO/IEC 27037:2014, and published scholarly literature. All sources are referenced in the bibliography.

Funding

This study did not receive any external funding.

Notes on Contributors

Litya Surisdani Anggraeniko
https://orcid.org/0000-0002-6177-0565
Litya Surisdani Anggraeniko is a law lecturer and legal researcher with international experience in humanitarian and human rights projects. Skilled in teaching, legal analysis, and strategic social media communication. Passionate about mentoring students, advancing legal scholarship, and driving positive societal impact.

Auliah Ambarwati
https://orcid.org/0000-0003-0628-6866
Auliah Ambarwati is a lecturer at the Faculty of Law, Sultan Ageng Tirtayasa University, Banten, Indonesia. As a lecturer, she is actively engaged in the Tri Dharma of Higher Education activities, which include teaching, research, and community service. Her academic interests focus on civil law, with much of her research and publications discussing contract and business law.

Feby Reski Utami
Feby Reski Utami is a lecturer at the Faculty of Law, Sultan Ageng Tirtayasa University, Banten, Indonesia. As a lecturer, she is actively engaged in the Tri Dharma of Higher Education activities, including teaching, research, and community service. Her academic interests focus on criminal law, with most of her research and publications discussing criminal acts, sexual violence, and proof of criminal offenses in criminal procedure law.

REFERENCES

Badan Standardisasi Nasional. (2014). *SNI ISO/IEC 27037:2014 teknologi informasi—teknik keamanan—pedoman identifikasi, pengumpulan, akuisisi dan preservasi bukti digital (ISO/IEC 27037:2012, IDT) [SNI ISO/IEC 27037:2014 information technology—security techniques—guidelines for identification, collection,*

acquisition, and preservation of digital evidence]. https://pesta.bsn.go.id/produk/detail/9830-sniisoiec270372014

Cahyani, N. D. W., Martini, B., & Choo, K.-K. R. (2016). Using multimedia presentations to enhance the judiciary's technical understanding of digital forensic concepts: An Indonesian case study. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5617–5626). IEEE. https://doi.org/10.1109/HICSS.2016.695

Cantika, G., Yunara, E., & Trisna, W. (2025). Kebijakan hukum pidana terhadap bukti elektronik: Antara eksistensi, hambatan penggunaan, dan urgensi pengaturannya dalam Kitab Undang-Undang Hukum Acara Pidana. *Acta Law Journal*, *3*(2), 103–125. https://talenta.usu.ac.id/ALJ/article/view/21464

Efendi, T. F. (2020). *Manajemen barang bukti fisik dan chain of custody (CoC) pada penyimpananan laboratorium forensika digital [Management of physical evidence and chain of custody (CoC) in digital forensic laboratory storage]* (Master's thesis, Universitas Islam Indonesia). https://dspace.uii.ac.id/123456789/28744

Ginting, Y. P., & Joesoef, P. G. (2025). Sistem pembuktian pada tindak pidana korupsi: Pembalikan beban, aset recovery, dan standar pembuktian. *IKRA-ITH Humaniora: Jurnal Sosial dan Humaniora*, *9*(3), 73–82. https://journals.upi-yai.ac.id/index.php/ikraith-humaniora/article/view/5267

Ilyas, A. (2021). Praktik penerapan exclusionary rules di Indonesia. *Masalah-Masalah Hukum*, *50*(1), 49–59. https://doi.org/10.14710/mmh.50.1.2021.49-59

Indonesia. (1981). *Undang-Undang Nomor 8 Tahun 1981 tentang hukum acara pidana [Law No. 8 of 1981 concerning criminal procedure]*. https://peraturan.bpk.go.id/Details/47041/uu-no-8-tahun-1981

Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik [Law No. 11 of 2008 concerning electronic information and transactions]*. https://peraturan.bpk.go.id/details/37589/uu-no-11-tahun-2008

Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik [Law No. 19 of 2016 amending Law No. 11 of 2008 concerning electronic information and transactions]*. https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016

Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang penyelenggaraan sistem dan transaksi elektronik [Government Regulation No. 71 of 2019 concerning electronic systems and transactions]*. https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan transaksi elektronik [Law No. 1 of 2024 on the second amendment to Law No. 11 of 2008 concerning electronic information and transactions]*. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

Indonesia. (2025). *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana [Law No. 20 of 2025 concerning the Criminal Procedure Code]*. https://peraturan.bpk.go.id/Download/400351/UU%20Nomor%2020%20Tahun%202025.pdf

Isima, N. (2022). Kedudukan alat bukti elektronik dalam pembuktian perkara pidana. *Gorontalo Law Review*, *5*(1), 179–189. https://doi.org/10.32662/golrev.v5i1.1999

Ipakit, R. (2015). Urgensi pembuktian alat bukti dalam praktek peradilan pidana. *Lex Crimen*, *4*(2), 88–94. https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/7789

Jayani, D. I., Elfitaningsih, V. Y., Agustin, D. A., & Raditya, R. (2020). Urgensi pembentukan e-court sebagai wujud peradilan yang berkembang. *Lontar Merah*, *3*(1), 281–290. https://doi.org/10.31002/lm.v3i1.940

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). *Guide to integrating forensic techniques into incident response (NIST Special Publication 800-86)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-86

Mahkamah Agung Republik Indonesia. (2019). *Peraturan Mahkamah Agung Republik Indonesia Nomor 1 Tahun 2019 tentang administrasi perkara dan persidangan di pengadilan secara elektronik [Supreme Court Regulation No. 1 of 2019 concerning electronic case administration and hearings]*. https://jdih.mahkamahagung.go.id/legal-product/perma-nomor-1-tahun-2019/detail

Mahkamah Agung Republik Indonesia. (2022). *Peraturan Mahkamah Agung Republik Indonesia Nomor 7 Tahun 2022 tentang perubahan atas Peraturan Mahkamah Agung Nomor 1 Tahun 2019 tentang administrasi perkara dan persidangan di pengadilan secara elektronik [Supreme Court Regulation No. 7 of 2022 amending Supreme Court Regulation No. 1 of 2019 concerning electronic case administration and hearings]*. https://jdih.mahkamahagung.go.id/legal-product/perma-nomor-7-tahun-2022/detail

Mahkamah Konstitusi Republik Indonesia. (2016). *Putusan Nomor 20/PUU-XIV/2016 [Decision No. 20/PUU-XIV/2016]*. https://mkri.id/public/content/persidangan/putusan/20_PUU-XIV_2016.pdf

Mualfah, D., & Ramadhan, R. A. (2020). Analisis forensik metadata kamera CCTV sebagai alat bukti digital. *Digital Zone: Jurnal Teknologi Informasi dan Komunikasi*, *11*(2), 257–267. https://doi.org/10.31849/digitalzone.v11i2.5174

Mulyana, Y. (2021). Cultural developments in electronic law enforcement in criminal acts of theory in Indonesia. *Journal Sampurasun: Interdisciplinary Studies for Cultural Heritage*, *7*(1), 17–27. https://doi.org/10.23969/sampurasun.v7i1.4149

Ratnasari, D. (2018). *Membangun model informasi metadata untuk mendukung chain of custody bukti digital [Building a metadata information model to support digital evidence chain of custody]* (Master's thesis, Universitas Islam Indonesia). http://hdl.handle.net/123456789/7590

Soroinda, D. L., & Nasution, A. A. R. S. (2022). Kekuatan pembuktian alat bukti elektronik dalam hukum acara perdata. *Jurnal Hukum & Pembangunan*, *52*(2), 384–405. https://doi.org/10.21143/jhp.vol52.no2.3344