Journal of Indonesian Legal Studies
Vol. 11 Issue 1 (2026) 257-298
ISSN: 2548-1584 (Print) 2548-1592 (Online)
DOI: https://doi.org/10.15294/jils.v11i1.35378
Online since: June 13, 2026

Journal of INDONESIAN LEGAL STUDIES
https://journal.unnes.ac.id/journals/jils

Digital Challenge, Analogue Mind-set: Assessing Indonesia's Electronic Criminal Evidence Framework

Anton Hendrik Samudra[1,2] ✉, Subhajit Basu[1], Cristina Saenz Perez[3]

[1] School of Law, University of Leeds, United Kingdom
[2] Faculty of Law, Universitas Surabaya, Indonesia
[3] School of Law, Comillas Pontifical University, Madrid, Spain

✉ Corresponding email: *A.H.Samudra@leeds.ac.uk*

Abstract

This article examines the treatment of electronic evidence in Indonesian criminal proceedings under the EIT Act and the new KUHAP. It argues that the new KUHAP has not succeeded in establishing coherent legal architecture for electronic evidence. Instead, the framework remains fragmented, under-specified, and anchored in an inherited analogue evidentiary mind-set. This is unsatisfactory because it encourages formalistic reliance on printed outputs, leaves the collection, authentication, handling, preservation, and evaluation of electronic evidence inadequately governed, and generates uncertainty for investigators, prosecutors, and judges. The article identifies the principal doctrinal and institutional defects in the current framework and assesses their implications for truth-seeking, procedural fairness, and the

reliability of criminal adjudication. It further evaluates the emerging reliance on open-source electronic evidence and argues that the central weakness of the Indonesian approach lies not merely in legislative incompleteness, but in the absence of a principled evidentiary governance model for digital proof. Its principal contribution is to show that ISO standards can supply that missing framework by structuring the governance, handling, and assessment of electronic evidence and by correcting the mistaken assumption that digital proof can be accommodated within essentially analogue evidentiary categories.

KEYWORDS *Cybercrime, Criminal Investigation, Digital Evidence, Electronic Evidence Framework, Legal Evidence System, Legal Reforms, KUHAP*

Introduction

Indonesia faces the imperative of modernising its criminal justice system (CJS) to accommodate digital nuances adequately. Indonesia has implemented the Electronic Information and Transaction (EIT) Act[1] in response to this evolution, and the new *Kitab Undang-undang Hukum Acara Pidana* (KUHAP, Code of Criminal Procedure) 2025 has very recently been passed. This modernisation should be, one of them, prioritising enhancing the electronic evidence (e-evidence)[2] framework. A contemporary approach to modernising criminal justice would enable a robust system in which e-evidence can be managed efficiently whilst safeguarding the principles of justice. Whilst critically reviewing the current e-criminal evidence framework, focusing on identifying its strengths, weaknesses, and areas requiring urgent attention, this article argues that the new e-evidence framework is still inadequate and further reform of the framework is urgently needed.

---

1 For clarity, this article uses "KUHAP 2025" and occasionally "new KUHAP" to refer to Act No. 20 of 2025 on the Criminal Procedure Code, which was enacted on 17 December 2025 and came into force on 2 January 2026. The "EIT Act" refers to Act No. 11 of 2008 on Electronic Information and Transactions as amended, most recently by Act No. 1 of 2024.

2 Two commonly used terms in the field are "electronic evidence" and "digital evidence." Given the specific context of this research in Indonesia and the prevalent usage of the term "electronic evidence" in relevant statutes, this article will adopt and employ the term "electronic evidence (e-evidence)" throughout its analysis and discussion.

Historically, the former cornerstone of Indonesia's CJS had been the Criminal Procedure Act (CPA) 1981,[3] which delineated the procedural protocols, rights, and obligations inherent in criminal adjudication. Although specialised criminal legislation introduced additional provisions that increased its complexity and flexibility, significant challenges remained: the law was outdated in the modern digital environment, where its architecture had been built around an analogue model of proof;[4] and amendments to the specialised acts had produced a fragmented framework that undermined its coherence.

Lawmakers aimed to address legal challenges arising from electronic transactions, information, and communications, including evidence admissibility and the legality of electronic actions.[5] The EIT Act, supplementing the *Kitab Undang-undang Hukum Pidana* (KUHP, Criminal Code)[6] 2023 and the CPA 1981, marked a significant development in Indonesian Law by formally recognising electronic information and documents as admissible legal evidence.[7]

However, Purwoleksono and Salmah express legitimate concerns about e-evidence's vulnerability to alterations. They advocate for a robust legal framework that ensures the integrity of such evidence whilst addressing its inherent vulnerabilities.[8] Judge Asimah and the Public Prosecutor's Office have both highlighted that, under the old law, a significant practical difficulty in applying the EIT Act lay in the absence of detailed procedural provisions

---

[3] *See* Section I(3) General Elucidation, Indonesia, Act No. 8 of 1981 on Criminal Procedure Act (CPA 1981).

[4] The CPA 1981's evidentiary structure was formulated for an analogue justice system centred on physical documents, direct testimony in court, and conventional forms of proof. As criminal activity and law enforcement increasingly moved into digital spaces—through electronic communications, digital records, CCTV, metadata, platform logs, and cloud-based information—The CPA 1981 no longer provided an adequate procedural foundation. See also Apri Listiyanto, 'Pembaharuan Sistem Hukum Acara Pidana', *Jurnal Rechtsvinding* Rechtsvinding Online (2017): 1–4, 1.

[5] *See* Paragraph 2, General Elucidation of EIT Act.

[6] Indonesia, Act No. 1 of 2023 on Criminal Code (KUHP).

[7] See Article 5(2) and Article 5(1) of the EIT Act (as amended); on the definition of electronic information and documents see Article 1(1) and 1(4) of the EIT Act.

[8] Didik Endro Purwoleksono et al., *Kedudukan Alat Bukti Elektronik Berdasarkan Perundang-Undangan Di Indonesia (Electronic Evidence Position Based on the Laws in Indonesia)*, no. 1962032519860 (2014), 15-17; see also Salmah, 'Ensuring the Admissibility and Credibility of Electronic Evidence in Indonesian Criminal Proceedings', in *Prevention of Crime and Treatment of Offenders*, ed. Morinaga Taro, vol. 113 (The United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders, 2022), 13.

governing the technical assessment of e-evidence.[9] In practice, this gap has encouraged a continued reliance on printed versions of such evidence, particularly within the Prosecutor's Office and in adjudicating cases involving electronic material.[10] This approach has been criticised for overlooking the crucial role that e-evidence can play in a trial.[11] The persistence of this practice illustrates the need for an updated legal framework that specifically regulates the collection, preservation and evaluation of e-evidence and provides for its meaningful integration into criminal proceedings.

Developing a coherent and robust framework for e-evidence, supported by comprehensive implementing regulations, is therefore a precondition for the effective use of such material in criminal trials and for a CJS that can respond to the demands of the digital age. The starting point must be a reassessment of Indonesia's foundational procedural principles from the perspective of e-evidence, to ensure that the emerging framework is consistent with the core values of a fair criminal process and with internationally recognised standards. Only by aligning rules on e-evidence with the transborder and volatile character of digital data, whilst remaining anchored in established legal guarantees, can the law mediate between technological change and traditional legal protections. The article seeks to advance the existing framework on admissibility by offering

---

[9] See Dewi Asimah, 'To Overcome the Constraints of Proof in the Application of Electronic Evidence', *Jurnal Hukum Peratun* 3, no. 2 (2021): 97–110, https://doi.org/10.25216/peratun.322020.97-110, 99; and Research and Development of Indonesia Prosecutor's Office, 'The Strength of the Value of Electronic Evidence in the Handling of Crime', 2016.

[10] *See* Chamdani and Asri Wijayanti, 'Critical Analysis about Legal Evidence in Court in the Justice System in Indonesia', *Journal of Positive School Psychology* 6, no. 2 (2022): 5867–70., p. 5868, *see also* Finna Nazran et al., 'The Legal Paradigm in a Global Context: Judicial of Evidence in Actualization of Electronic in Indonesia', 642 (2021): 154–58, 157 and Insan Pribadi, 'Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana', *Jurnal Lex Renaissance* 3, no. 1 (2018): 109–24, https://doi.org/10.20885/JLR.vol3.iss1.art4, 109; Research and Development of Indonesia Prosecutor's Office, 'The Strength of the Value of Electronic Evidence in the Handling of Crime'.

[11] *See* Elena Alina Ontanu, 'Normalising the Use of Electronic Evidence: Bring Technology Use into a Familiar Normative Path in Civil Procedure', *Oñati Socio-Legal Series* 12, no. 3 (2022): 582–615, https://doi.org/10.35295/osls.iisl/0000-0000-0000-1304; Piotr Lewulis, 'Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law', *Criminal Law Forum* 33, no. 1 (2021): 39–62, https://doi.org/10.1007/s10609-021-09430-4, 61; David S. Wall, 'The Internet as a Conduit for Criminal Activity (Revised October 2015)', in *Information Technology and the Criminal Justice System*, revised, ed. A. Pattavina (Sage, 2005), 11.

a critical and constructive analysis tailored to the particular challenges of Indonesia's multifaceted legal system and by formulating proposals aimed at ensuring rigorous, consistent and just outcomes in an increasingly digital judicial environment.

This article is further justified by the absence of any systematic analysis of the persistence of analogue evidentiary logic within Indonesia's evolving digital procedural framework. Whilst the KUHAP reform has increasingly accommodated e-evidence, scholarship has yet to examine in a sustained way how the new framework continues to inherit assumptions, categories, and methods of proof rooted in an analogue model. By foregrounding that unresolved tension, the article makes an original contribution to the study of criminal procedure in the digital age.

The article is structured in five main parts. Following the introductory discussion, Section 2 examines the challenges and inadequacies of Indonesia's existing legal framework for e-criminal evidence. It begins by assessing whether KUHAP 2025 provides a sufficient procedural foundation, with particular attention to the problem of recognising e-evidence without constructing a coherent legal architecture for its definition, search, and seizure. It then analyses the contribution of the EIT Act, before turning to the changing scope of *Praperadilan* (pre-trial review) and its implications for the admissibility of e-evidence under both the old and new legal regimes. The final sub-section of Section 2 argues that the law must move beyond mere authenticity and legality by embedding reliability as a distinct and essential requirement of e-criminal evidence. Section 3 then focuses on open-source e-criminal evidence, highlighting the legal ambiguities, risks of procedural circumvention, and recurring problems of volatility, integrity, and chain of custody. Section 4 considers SNI ISO/IEC 27037:2014 as an important but underutilised resource for improving Indonesian practice. Building on these analyses, Section 5 sets out proposals for reform, arguing that Indonesia's e-criminal evidence framework must still be fundamentally adapted to the realities and risks of the digital age.

Challenges and Inadequacies in Indonesia's Legal Framework for e-Criminal Evidence

E-evidence has become increasingly relevant in criminal trials due to the rapidly evolving technological landscape and the consequent changes to modern lifestyles; for example, the use of CCTV footage in *Jessica Wongso* ice-cold coffee

murder case.[12] Additionally, prominent digital communication platforms record internet users' digital activities, which could provide essential evidence to solve crimes. Excluding crucial electronic trails, in this sense, could hinder justice. E-evidence—though recognised[13] yet addressed through fragmented provisions—is admissible in criminal trials.[14] Practically, it often serves as indirect evidence, facilitating the inference of disputed facts.[15] The following sub-section turns to assessing the adequacy of the New KUHAP in providing a comprehensive framework for e-evidence.

A. Does KUHAP Provide a Sufficient Framework?

KUHAP 2025 represents an ambitious modernisation. Its predecessor, the CPA 1981, did not have a digital-minded design. Although the previous framework, together with the EIT Act, could be used to support digital investigations, it left significant gaps and did not provide a comprehensive legal framework. Experts like Butt and Lindsey commented that the CPA 1981 was far from comprehensive.[16] Numerous statutes and regulations have been enacted to filled gaps or provide more detail, with the Act patched together by an array of special acts and Constitutional Court case law. Further, Butt and Lindsey have advocated for exhaustive reforms, pointing out the inherent deficiencies and outdated perspectives adopted in the original statute.[17] Although the critique might seem harsh, the CPA 1981 was indeed antiquated and not designed for the recent technological advancements. The framework was designed revolving around traditional means of evidence.

---

[12] *Jessica K. Wongso*, Putusan Mahkamah Agung RI No. 498 K/PID/2017 (July 21, 2017), https://putusan3.mahkamahagung.go.id/direktori/putusan/0655f7a4b8121a6727ae5c33824a101b.html.

[13] *See* Article 5(2), EIT Act; and Article 235, KUHAP 2025.

[14] See Purwoleksono, Astagiri, and Ristianto, *Kedudukan Alat Bukti Elektronik Berdasarkan Perundang-undangan di Indonesia (Electronic Evidence Position Based on the Laws in Indonesia)*, 16-18 and Pribadi, "Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana.", 117-120; and Mohammad Safrin and Hasnawati Hasnawati, "Kedudukan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana," *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam* 5, no. 2 (2023), https://doi.org/10.37680/almanhaj.v5i2.2878, 1211.

[15] Stephen Mason and Daniel Seng, "The Foundations of Evidence in Electronic Form," in *Electronic Evidence and Electronic Signatures*, ed. Stephen Mason and Daniel Seng (University of London Press, Institute of Advanced Legal Studies, 2021), 51.

[16] Simon Butt and Tim Lindsey, 'The Criminal Procedure Code', in *Crime and Punishment in Indonesia*, 1st edn (Routledge, 2020), 44.

[17] Butt and Lindsey, 'The Criminal Procedure Code', 44.

The new KUHAP, which recently entered into force, moves the procedural landscape towards greater technological integration. However, it is identified, for this article purposes, several areas where the framework remains incomplete or conceptually fragile. Especially regarding e-evidence: the definition of e-evidence, search and seizure, guarantees of authenticity, reliability and integrity, and safeguard.

1. E-evidence: Recognition without architecture

Although KUHAP 2025 recognises e-evidence as a distinct category,[18] the surrounding legal architecture is not fully integrated. The definition of e-evidence is problematic. From the perspective of procedural legality, the scope of e-evidence must be precisely delineated to determine what may be searched, seized, processed, and presented at trial.

a. Criminal Evidence Definition

E-evidence ("*bukti elektronik*") definition further described in Article 242 KUHAP 2025: "... including all forms of electronic information, document, and/ or electronic system which related to criminal offence," and in the elucidation of Article 235(1)f: "...information that is spoken, sent, received, or stored electronically using optical devices or similar means, including any recorded data or information that can be viewed, read, and/or heard, which may be produced with or without the aid of a tool, whether contained on paper, any physical object other than paper, or recorded electronically in the form of writing, images, maps, designs, photographs, letters, symbols, numbers, or perforations that carry meaning."

The definition of "*bukti elektronik*"/e-evidence quoted above is clearly drafted with the intention of being as inclusive as possible, but in doing so it becomes conceptually diffuse and potentially problematic from the standpoint of evidence law and criminal procedure. It amalgamates distinct ideas—communication, data, documents, and physical objects—under a single label, without adequately distinguishing between what counts as "e-evidence" in a technical sense and what counts as an admissible "means of proof" in a procedural sense. In what follows, this paper unpacks these layers and examine the internal coherence of the formulation.

---

[18] See Article 235(1)f, KUHAP 2025.

The KUHAP formulation is weaker than the EIT Act framework as a definition of e-evidence. Although KUHAP 2025 now governs criminal procedure, the conceptual architecture of e-evidence in Indonesia still depends on the EIT Act, which remains the primary source for the categories of *Informasi Elektronik*, *Dokumen Elektronik*, and *Sistem Elektronik*, and continues to recognise electronic information, electronic documents, and their printouts as lawful evidence.[19] This is clearer when KUHAP 2025 is compared with the broader formulation of e-evidence as information that is spoken, sent, received, or stored electronically, including any record of data or information that can be seen, read, or heard, whether embodied on paper, another physical object, or electronic media, in forms such as writing, images, maps, designs, photographs, letters, signs, numbers, or perforations that have meaning. That broader approach is evidentially preferable because it captures electronic material at the threshold level without prematurely imposing legal filters. By contrast, KUHAP 2025's phrase "*data elektronik yang telah diolah dan memiliki arti tertentu sesuai dengan ketentuan peraturan perundang-undangan*" is too restrictive: it suggests that data must already be processed and legally meaningful before it can count as evidence. This is problematic in criminal proof, where probative material often consists of raw logs, metadata, geolocation traces, audit trails, deleted fragments, or machine-generated records whose significance only emerges through forensic interpretation. The KUHAP wording also collapses ontology and admissibility by embedding statutory conformity into the definition itself, even though legality of acquisition, authenticity, integrity, chain of custody, and evidential weight are analytically separate questions. In addition, KUHAP 2025 does little to clarify the distinction between *Informasi Elektronik* as digital content and *Dokumen Elektronik* as a fixed or reproducible record of that content, leaving difficult material such as volatile memory, livestream data, traffic data, ephemeral messages, and changing system states conceptually underdeveloped. The better approach, for now, is therefore to treat the EIT Act as the primary source for the substantive taxonomy of digital material, while KUHAP should regulate its procedural use in criminal proceedings. On that view, EIT Act answers what counts as electronic information or an electronic document, while KUHAP answers how such material is obtained, introduced, tested, and weighed as criminal evidence.

Another difficulty concerns the object of the definition is the definitional overlap with other traditional categories of evidence. The provision explicitly

[19] Articles 1 no. 38 and 39, and Elucidation of 235(1)f, KUHAP 2025.

embraces information that is embodied "on paper, any physical object other than paper, or recorded electronically." This drafting choice threatens to collapse the distinction between e-evidence, on the one hand, and conventional documentary evidence (*surat*) or physical exhibits (*benda*) on the other. In traditional evidence doctrine, documents and physical objects are treated as distinct forms of proof, each with their own rules and conceptual structure.[20] By describing anything written on paper, any physical item, and any electronically recorded content as all falling within the ambit of *bukti elektronik*, the definition invites doctrinal confusion. For example, it becomes uncertain whether a printed email is to be analysed as a document, as e-evidence, or simultaneously as both; likewise, any ordinary physical object with minimal digital features (a product bearing a barcode or QR code, for instance) might be forced under the "e-evidence" rubric. This kind of categorical overlap can disrupt the systematic organisation of evidentiary rules and complicate judicial reasoning about admissibility and weight.

The definition is also unduly medium-centric, rather than conceptually focused on the nature of electronic data. The reference to storage "with optical devices or similar means"[21] foregrounds particular technologies—evoking CDs, DVDs, or optical disks—rather than the underlying characteristic that unifies e-evidence as such: that it consists of data encoded and processed within electronic systems. Contemporary e-evidence encompasses data stored on solid-state drives,[22] in cloud infrastructures,[23] within distributed ledger technologies, or in complex database and logging environments.[24] Anchoring

---

[20] See Adrian Keane and Paul McKeown, *The Modern Law of Evidence*, 9th edn (Oxford University Press, 2012), 9; William Twining, *Rethinking Evidence: Exploratory Essays*, 2nd edn, Law in Context (Cambridge University Press, 2006), Cambridge Core, 193; Jefferson L. Ingram, *Criminal Evidence*, 13th Edition (Routledge, 2018), 512.

[21] Elucidation of Article 235(1)f, KUHAP 2025.

[22] See Albert Antwi-Boasiako and Hein Venter, 'A Model for Digital Evidence Admissibility Assessment', in *IFIP Advances in Information and Communication Technology*, ed. Gilbert Peterson and Sujeet Shenoi, AICT-511, Advances in Digital Forensics XIII (Springer International Publishing, 2017); Salmah, 'Ensuring the Admissibility and Credibility of Electronic Evidence in Indonesian Criminal Proceedings'; Steven J. Murdoch et al., *The Sources and Characteristics of Electronic Evidence and Artificial Intelligence* (Institute of Advanced Legal Studies, 2021), 1; Jan-Jaap Oerlemans and Maša Galič, 'Cybercrime Investigations', in *Essentials in Cybercrime: A Criminological Overview for Education and Practice* (Eleven International Publishing, 2022), 216.

[23] See L. Hongjiao, 'Application of Digital Evidence in Criminal Cases: Dilemma and Optimization', *Contemporary Social Sciences* 9, no. 6 (2024): 115–31, 122.

[24] See Hongjiao, 'Application of Digital Evidence in Criminal Cases: Dilemma and Optimization', 122.

the definition in specific hardware, such as "optical" devices, renders it vulnerable to technological obsolescence and under-inclusiveness.

Moreover, KUHAP 2025 does not provide its own definition of an "electronic system", instead deferring to the EIT Act for this foundational concept.[25] For a newly enacted procedural code, this technique of cross-referencing creates unnecessary fragmentation in the evidentiary framework. From the standpoint of systematic coherence, it would be preferable for the KUHAP itself to articulate the basic conceptual baseline—in this context, a definition of "electronic system" tailored to evidentiary use—rather than relying entirely on external legislation. By failing to do so, the code risks undermining the internal consistency and long-term stability of the notion of *bukti elektronik* (e-evidence). An analytically sound approach would define "electronic system" at the level of electronic encoding and machine processing, rather than by reference to particular technologies, devices, or platforms, thereby reflecting technological neutrality. Framed in this way, the definition would be more resilient to technological change and would provide a stable, general criterion for determining what qualifies as e-evidence over time.

The clause which enumerates various forms of content—"writing, images, maps, designs, photographs, letters, signs, numbers, or perforations that have meaning"—appears to be borrowed from formulations designed for paper-based documents and then transplanted into the electronic realm. Whilst this enumeration does capture some common manifestations of digital content, it does not map comfortably onto many forms of modern e-evidence, such as system log files, metadata, hash values, database records, or audit trails generated by software. These forms can only be forced into the list indirectly, by construing them as "numbers" or "signs," which is both unsatisfactory and potentially contentious. From a conceptual perspective, it would be more precise to define e-evidence in terms of data or information encoded in an electronic system that can be rendered into a human-perceivable form (text, sound, image, or symbolic representation), rather than relying on a historically contingent list derived from the world of physical documents.

In addition, the drafting is linguistically unwieldy and lacks economy. Phrases to the effect that data or information "can be seen, read, and/or heard" and "can be produced with or without the aid of a device" are verbose ways of stating that the information is capable of being made perceptible to human senses, whether directly or via technological mediation. Long, multi-layered sentences of this kind expand the surface area for interpretive disagreement and

[25] See Article 1 number 5, EIT Act (as amended).

increase reliance on judicial construction simply to distil the core meaning of the provision. From an academic standpoint, legal definitions ought, as far as possible, to be both conceptually precise and linguistically economical,[26] especially where they serve as foundational terms for an entire regime of evidentiary rules.

Conceivably the most significant omission, however, is that although it has explained that the EIT Act can taxonomically account for what constitutes e-evidence, it contains no explicit reference to the normative conditions under which electronic data qualifies as evidence in criminal proceedings. In practice, the probative value of electronic material depends crucially on three interrelated aspects: integrity (whether the data remains complete and unaltered since its creation or capture),[27] authenticity (whether it can reliably be attributed to a particular person, system, or source),[28] and the reliability of the electronic system that generated or stored it.[29] It is argued that the current definition is purely descriptive; it tells us what e-evidence may look like, but not what distinguishes it from ordinary electronic data that is too unreliable or untrustworthy to be relied upon in court. Even if these criteria are developed elsewhere in the legislative framework, it would be analytically stronger to signal—at least in broad terms—that *bukti elektronik* refers to electronic data capable of functioning as a means of proof under conditions that allow its integrity and authenticity to be assessed.

For these reasons, the existing formulation can be characterised as over-inclusive, technologically dated, and doctrinally entangled with other evidentiary categories. A more robust approach would be to define *bukti elektronik* in data-centric and function-oriented terms, for example: as any data or information that is encoded, transmitted, received or stored by means of an electronic system, that can be rendered into a perceivable form (such as text,

---

[26] See Niklas Luhmann, *Law as A Social System* (Oxford University Press, 2004), https://doi.org/10.1093/oso/9780198262381.001.0001, 340; Sanne Taekema et al., *Facts and Norms in Law: Interdisciplinary Reflections on Legal Method* (Edward Elgar Publishing, 2016), https://doi.org/10.4337/9781785361098, 136.

[27] See Hongjiao, 'Application of Digital Evidence in Criminal Cases: Dilemma and Optimization', 127.

[28] See A. Yeboah-Ofori and A. D. Brown, 'Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence', *Journal of Forensic, Legal & Investigative Sciences* 6, no. 1 (2020): 1–8, https://doi.org/10.24966/flis-733x/100045.

[29] See Edmon Makarim, 'Electronic Evidence and Electronic Signatures in Indonesia: The Probative Value of Digital Evidence', *Digital Evidence and Electronic Signature Law Review* 10 (2013): 136–43. 143; Lewulis, 'Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law'. 45.

sound, images, or other meaningful symbols), and that is capable of being used as a means of proof in legal proceedings, provided that its integrity and authenticity can be examined and accounted for. Such a definition preserves breadth whilst achieving greater conceptual clarity, aligns with contemporary understandings of e-evidence, and situates the concept squarely within the normative framework of criminal proof.

b. E-Criminal Evidence Search and Seizure Framework

KUHAP 2025 regulates search and seizure and allows the search of electronic information and documents, but its procedural norms still treat e-evidence as peripheral, reflecting an essentially analogue mind-set. Recognising e-evidence in name only, without embedding it in a coherent framework of powers, procedures, and safeguards, produces uncertainty about investigative authority and invites challenges to the authenticity, integrity, and reliability of e-evidence.

The KUHAP outlines search and seizure procedures, and categorises searches into two types: physical location searches and body searches. Although it mentioned electronic information and document as search objects, the provisions do not explicitly and comprehensively cover virtual location.[30]

A house search, defined as an investigator's entry into a residence or enclosed space for examination, seizure, or arrest, requires the presence of a local neighbourhood coordinator (*Rukun Tetangga/Rukun Warga - RT/RW*) or village chief (*Lurah*) and two witnesses unless the homeowner consents.[31] This requirement, however, introduces procedural complexities and raises concerns about both timely investigations and the impartiality of local officials as witnesses. Additionally, the Act fails to address scenarios where these officials are unavailable, creating ambiguity regarding the legality of investigations under such circumstances. On the other hand, a body search involves an investigator examining a suspect's body and/or clothing to locate and seize objects strongly suspected to be concealed therein.[32] The relevant provisions do not extend to virtual or digital locations, such as data stored on cloud servers.

Regarding seizure—Article 1 number 35 KUHAP 2025, which defines objects liable to seizure as tangible or intangible, movable or immovable things for evidentiary purposes, still reflects a pre-digital conception of offending that

[30] See Articles 112-117, KUHAP 2025.

[31] See Article 114, KUHAP 2025.

[32] See Article 117, KUHAP 2025.

does not fully accommodate the realities of data-driven crime.[33] The only clear point of entry for e-evidence into this fragmented seizure framework is Article 113(3), which permits the seizure of e-evidence on the basis that it constitutes a statutory means of proof—referring to Article 235(1). Yet this sits uneasily alongside Article 123, which enumerates objects that may be seized and appears to limit them to *benda*. This, in turn, raises the question whether e-evidence can be subsumed under the notion of *benda*. Conceptually, the definition of *benda* in Article 1 number 35—covering tangible and intangible, movable and immovable objects—could be read broadly enough to encompass electronic data, but the absence of explicit clarification means that this result depends on interpretive reconstruction rather than clear legislative design, in tension with the principle of legal certainty.

Compounding this, KUHAP 2025 still does not lay down concrete, operational rules on the handling, preservation, and documentation of electronic material, even though such rules are critical to establishing forensic reliability. It is true that Articles 55–57 introduce a general framework for "technical assistance" in investigations (*bantuan teknis penyidikan*), including the use of digital forensics (Pasal 56(1)e) for the specialised examination and testing of e-evidence, to be carried out by the police and further regulated by Government Regulation (*Peraturan Pemerintah*). However, these provisions are primarily institutional and organisational: they identify categories of expertise (laboratory, identification, medical, psychological, and digital forensics) and allocate responsibility for providing such assistance, but they do not specify the procedural standards governing how electronic data must be seized, preserved, logged, and presented in court in order to satisfy requirements of integrity and authenticity. The framework is thus pragmatic in that it formally recognises the admissibility of e-evidence and the need for digital forensic support, yet it still fails to provide a comprehensive legal basis for assessing admissibility in practice. This gap is particularly problematic given that, unlike its predecessor, KUHAP 2025 introduces an exclusionary rule,[34] requiring judges to exclude evidence that is not properly authenticated or that has been obtained unlawfully; in the absence of clear criteria for the lawful search and seizure of e-evidence and for its proper forensic treatment, the application of this rule to digital investigations remains uncertain.

---

[33] See also Article 46, KUHAP 2025.

[34] See Article 235(5), KUHAP 2025.

Some legal systems consider digital information a form of "intangible property" that can be subject to seizure.[35] Courts could adopt a similar interpretation to include data within the existing framework. However, in accordance with the principle of legality, criminal laws should be unambiguous.[36] Expanding the definition could create uncertainty and potential violations of due process if the scope of what can be seized is not explicitly defined. Additionally, as data can be easily copied or altered, judges should be concerned about the potential for seizing irrelevant information or compromising the integrity of e-evidence.

The KUHAP designs the evidence seizure framework around '*benda*'.[37] This creates a significant shortcoming, as the Act lacks provisions specifically addressing the distinct characteristics and handling requirements of e-evidence in search and seizure. Firstly, e-evidence is volatile and can be easily modified, overwritten, or deleted, intentionally or unintentionally.[38] This fragility demands strict chain-of-custody procedures and preservation techniques that cannot be explicitly outlined in a framework designed for '*benda*'. Secondly, e-evidence can be easily altered, which refers to the ability to manipulate e-evidence without leaving obvious traces, which poses challenges for authentication and integrity verification. Specialised forensic tools and procedures are needed, which traditional laws might not account for.

Thirdly, the sheer amount of potential e-evidence and the complexity of file formats require advanced technical expertise. The law focused on '*benda*' and did not provide for such specialised needs during seizure and analysis. Fourthly, e-evidence raises jurisdictional and territorial issues, as it often transcends geographic boundaries, especially with cloud storage and data

---

[35] For example, the Netherlands (see Articles 125i-125o, Dutch Criminal Procedure Code; and Bart Custers and Lonneke Stevens, 'Data as Evidence in Criminal Courts: Comparing Legal Frameworks and Actual Practices', in *Human-Robot Interaction in Law and Its Narratives: Legal Blame, Procedure, and Criminal Law* (Cambridge University Press, 2024); and England and Wales (see Theft Act 1968, and particularly Section 69 Police and Criminal Evidence Act 1984 as repealed (14.4.2000) by 1999 c. 23, ss. 60, 67(3), Sch. 6; S.I. 2000/1034, Art. 2(c), Sch.) have expansive and modern definitions of property that encompass data as evidence.

[36] See Jonathan Herring, *Criminal Law: Text, Cases, and Materials* (Oxford University Press, 2022), 9-10.

[37] See Articles 1 number 35 and 123, KUHAP 2025.

[38] See Purwoleksono et al., *Kedudukan Alat Bukti Elektronik Berdasarkan Perundang-Undangan Di Indonesia (Electronic Evidence Position Based on the Laws in Indonesia)*, 15-17; also Salmah, 'Ensuring the Admissibility and Credibility of Electronic Evidence in Indonesian Criminal Proceedings', 13.

transfers. Frameworks focused on '*benda*' might lack the adaptability to address the extraterritorial nature of e-evidence. KUHAP 2025 remains silent on the collection and handling of cross-border e-evidence, particularly regarding its integration within mutual legal assistance (MLA) mechanisms.

Finally, in a modern system, the object of search should be the location—physical (buildings, houses, land, vehicles) and digital or virtual (networks, servers, cloud infrastructures). The purpose of the search is then to seize evidential objects, analogue or digital. Although KUHAP 2025 acknowledges electronic information and documents as search objects, it still confines seizure to *benda*,[39] leaving the treatment of e-evidence to uncertain judicial interpretation. The incomplete and imprecise search and seizure framework should be revised.

The absence of clear guidelines encompassing e-evidence handling can potentially jeopardise the integrity of investigations and compromise the admissibility of crucial evidence in court. Consequently, ensuring the originality, authenticity, and reliability of e-evidence becomes challenging. Moreover, the framework does not account for searches conducted without consent, which means that the legal provisions are inadequate if the accused refuses to provide access to their electronic systems, such as passwords or passkeys.

The practical significance of these deficiencies is not merely theoretical. Concrete illustrations show how these gaps can obstruct real digital investigations. In *Pengadilan Tinggi* Medan No. 1379/Pid.Sus/2020/PT MDN decision, the appellate court overturned the conviction and acquitted the defendant in an EIT case; the *Mahkamah Agung* (Indonesia Supreme Court) database record notes that the relevant Facebook accounts had already been deleted and could not be reactivated in the ordinary way,[40] whilst one of the judges of the District Court identifies the absence of digital-forensic examination as central to the failure to prove account ownership and authorship.

Likewise, in *Pengadilan Tinggi* Pekanbaru No. 274/PID.SUS/2017/PT PBR decision, although the prosecutor secured the conviction, the *Mahkamah Agung* database records the defence position that the prosecutor had failed to

---

[39] See Articles 45-47, KUHAP 2025.

[40] *Imran Haryono Simamora*, Putusan Pengadilan Tinggi Medan No. 1379/Pid.Sus/2020/PT MDN (September 30, 2020) Accessed April 14, 2026. https://putusan3.mahkamahagung.go.id/direktori/putusan/eb831d3462aae96d2a9496899d648c40.html.

prove the e-evidence "..*secara hukum yang benar*.." (lawful)[41] under the EIT framework, illustrating how electronic material may lose decisive evidential force when its acquisition or validation is procedurally weak. Similar problems can easily arise in practice: for example, where investigators seize a powered-on phone but, absent a clear statutory preservation protocol, allow remote wiping, auto-sync, or overwriting to alter the data; where a warrant to search a house is treated as authority to inspect all cloud accounts linked to a seized device, prompting a challenge that the digital search exceeded the warrant's scope; or where a suspect refuses to provide a password or passkey and the law contains no sufficiently clear mechanism for compelled access or alternative lawful extraction. In each scenario, the investigation is not merely made more difficult; the legality, integrity, and admissibility of the resulting e-evidence become vulnerable to challenge.

This difficulty is compounded by the fact that, although KUHAP 2025 expressly recognises e-evidence and expressly permits searches directed at *Informasi Elektronik* and *Dokumen Elektronik*, the new code still identifies unresolved questions about the scope of digital search authority, including whether authority to search a physical location automatically extends to the contents of devices and accounts discovered there, and what procedural limits govern such access.

Regulation (EU) 2023/1543 provides a useful reference point from which Indonesia may draw regulatory insights.[42] It creates an EU-wide mechanism for the cross-border collection of stored e-evidence directly from service providers through a European Production Order and a European Preservation Order, reducing reliance on slower MLA channels. Its core innovation is procedural: it combines direct provider access with differentiated safeguards based on the type of data sought, including subscriber data, user-identification data, traffic data, and content data. It also limits its own reach. The Regulation applies to stored data already existing when the order is received, and does not create a general data-retention duty, authorise interception of future data, or require providers to decrypt data. Its significance lies in the balance it attempts to strike between

---

[41] *Deni Ramdan*, Putusan Pengadilan Tinggi Pekanbaru No. 274/PID.SUS/2017/PT PBR (January 16, 2018) Accessed April 14, 2026. https://putusan3.mahkamahagung.go.id/direktori/putusan/zaec2283d64934e0aa5f313335303137.html.

[42] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings, OJ L 191, July 28, 2023, 118.

investigative efficiency and procedural protection. More intrusive requests, particularly for traffic and content data, are subject to stricter judicial control. Seizure must also follow clear principles—relevance, data minimisation, reliability, and integrity—under a judicial warrant, with a documented chain of custody from seizure to return or destruction.

Whilst judicial interpretation might offer temporary solutions, the new KUHAP needs further overhaul. The existing rules of criminal procedure fail to align with the unique demands of digital investigations, further underscoring the legal deficiencies. Stretching the interpretation of analogue provisions to fit digital contexts could undermine the rule of law and result in inconsistencies in its application.

Given these limitations, it is essential to examine more closely the mechanisms within the Indonesian CJS that could address the gaps in the current framework. The following discussion will therefore evaluate the existing e-evidence framework, with particular attention to the extent to which the EIT Act contributes to clarifying it.

B. How Does the EIT Act (as amended) Contribute to the e-Criminal Evidence Framework?

Before KUHAP 2025 came into force, Indonesian law did not contain a single, comprehensive procedural code governing e-evidence. In that vacuum, the EIT Act functioned as the principal general statutory basis for recognising and using electronic material in criminal proceedings, supplemented in particular areas by sector-specific regimes such as anti-corruption and anti-money-laundering legislation.[43]

The EIT Act's first and most important contribution was recognition. Article 5 affirms that Electronic Information, Electronic Documents, and their printouts are lawful evidence, and further states that they constitute an expansion of the legally valid means of proof under Indonesian procedural law. That formulation was doctrinally significant because it provided the bridge by

[43] Other e-evidence provisions including Article 27 of the Emergency Interim Act No. 1 of 2002, as stipulated in Terrorism Eradication Act; Article 29 of Human Trafficking Eradication Act; Article 86(2) of Narcotics Act; Article 38b of Terrorism Financing Prevention and Eradication Act; and Article 37 of Forest Destruction Prevention and Eradication Act.

which courts could receive electronic material even though the older CPA 1981 was drafted on largely analogue assumptions. At the same time, the wording of Article 5 was never entirely self-sufficient. By framing e-evidence as an "extension"[44] of valid evidence under the applicable law of procedure, the EIT Act acknowledged electronic proof without fully specifying its procedural status, classification, or mode of treatment across all criminal cases.[45] In practice, courts and practitioners moved toward broad acceptance, but the statutory technique remained indirect rather than comprehensive.

A second, and continuing, contribution of the EIT Act lies in Article 6. That provision states in substance that electronic information may satisfy a legal requirement of written form so long as the information can be accessed, displayed, its integrity is assured, and it can be accounted for so as to explain a situation. Article 6 is important because it supplies an admissibility-oriented benchmark centred on accessibility, displayability, integrity, and accountability. Yet it also reveals the limits of the pre-KUHAP framework. The EIT Act did not build from those criteria a full procedural architecture governing collection, preservation, chain of custody, forensic examination, and courtroom authentication.[46] Nor did it expressly articulate a distinct requirement of probative value. As a result, the Act recognised e-evidence at the level of principle, but left many operational questions to interpretation and practice.

The EIT Act additionally contributed investigative powers and digital-procedure safeguards, but again only in a partial and sectorally framed manner. Article 43 requires investigators to take account of privacy, confidentiality, continuity of public services, and data integrity; it regulates searches and seizures of electronic systems in accordance with criminal procedure; it enumerates specific powers of specially authorised civil-servant investigators (PPNS), including preserving data by rendering it inaccessible, requesting information from electronic-system providers, and ordering temporary access suspension for accounts and digital assets; and it provides the

---

[44] Article 5(2)'s broad wording, stating "...an extension of valid evidence according to applicable procedural law..." (translation of "..*perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku*...,").

[45] See Salmah, 'Ensuring the Admissibility and Credibility of Electronic Evidence in Indonesian Criminal Proceedings', 12; Chamdani and Asri Wijayanti, 'Critical Analysis about Legal Evidence in Court in the Justice System in Indonesia', 5868; and Edmon Makarim, 'Electronic Evidence and Electronic Signatures in Indonesia: The Probative Value of Digital Evidence', 139.

[46] See Salmah, 'Ensuring the Admissibility and Credibility of Electronic Evidence in Indonesian Criminal Proceedings', 13.

only express statutory basis for cooperation with foreign investigators to share information and evidence.[47] Even so, this regime was incomplete. Its core operative powers were framed through PPNS authority rather than as a general code for all criminal investigators, and the Act still referred crucially back to the general law of criminal procedure instead of supplying a self-contained digital search-and-seizure regime.

KUHAP 2025 substantially changes that landscape. It expressly lists *bukti elektronik* as a statutory means of proof and by defining it to include Electronic Information, Electronic Documents, and electronic systems connected to the offence. More importantly, KUHAP 2025 now requires that evidence be authentic and lawfully obtained, empowers judges to assess both authenticity and legality, and provides that evidence declared unauthentic or unlawfully obtained cannot be used and has no evidentiary force.[48] In addition, the new Code expressly contemplates searches of Electronic Information and Electronic Documents and subjects searches to prior judicial authorisation from the *Ketua Pengadilan Negeri* (Chief of the District Court), with exceptions for urgent situations.[49] In those respects, KUHAP 2025 addresses two of the central weaknesses of the earlier regime: the uncertain procedural status of e-evidence and the absence of an express exclusionary consequence for unlawfully obtained or unauthenticated material.

Even after that reform, however, the EIT Act has not become irrelevant. Its role has shifted from being the principal foundation of admissibility to being a supplementary digital-law statute that continues to inform the treatment of e-evidence where KUHAP 2025 is silent or underdeveloped. The clearest example is Article 6. KUHAP 2025 now speaks in terms of authenticity and lawful acquisition, but it does not reproduce the more specific Article 6 criteria of accessibility, displayability, integrity, and accountability. A strong interpretive argument therefore remains that Article 6 should continue to guide courts when assessing whether a piece of electronic material is sufficiently reliable to be received and weighed, so long as that use is consistent with the new KUHAP framework. Likewise, Article 43 of the EIT Act still matters because KUHAP 2025 does not appear to supply an equally explicit rule on transnational information-sharing and evidence cooperation in the electronic sphere.

The resulting relationship between the two statutes is therefore best understood as complementary, but not entirely free from tension. Both are

---

[47] See Article 43(8), EIT Act.

[48] Articles 235(3), (4), and (5), KUHAP 2025.

[49] Article 113, KUHAP 2025.

statutes of the same formal rank. KUHAP 2025 should now be treated as the primary source for general criminal procedure, including the classification of evidence, judicial screening of authenticity and legality, and the basic rules on search and seizure. The EIT Act, however, still supplies digital-specific norms that KUHAP 2025 either generalises or leaves underspecified. That does not eliminate fragmentation; it manages it. The price of that solution is that courts will still need to engage in coordinated interpretation to determine when the EIT Act supplements KUHAP 2025 and when it must yield to the newer procedural code.

Accordingly, the contribution of the EIT Act (as amended) to Indonesia's contemporary e-criminal-evidence framework is now narrower but more precise. It no longer bears the full weight of recognising e-evidence in criminal proceedings, because KUHAP 2025 has now performed that general procedural function. Its continuing significance lies instead in three areas: first, as the historical foundation on which e-evidence was first normalised in Indonesian law; second, as a supplementary source of admissibility-oriented criteria, especially through Article 6; and third, as a residual source of digital-investigative and cross-border cooperation norms, especially through Article 43. In short, KUHAP 2025 has displaced the EIT Act from the centre of the evidentiary system, but it has not displaced it from the architecture of digital criminal procedure.

The Shift on *Praperadilan* and Its Impact to the e-Criminal Evidence Admissibility

This section examines the shift in the role of *Praperadilan* (pre-trial) in relation to the admissibility of e-evidence, tracing its departure from the previous legal framework and advancing a critique of the new KUHAP. The *Praperadilan* mechanism is conceived as a vital procedural safeguard that institutionalises judicial oversight of law-enforcement conduct. However, as will be shown, the current Indonesian framework relies predominantly on ex post review rather than ex ante control, thereby weakening the preventive function that *Praperadilan* is intended to serve.

A. The Old Law and e-Evidence Admissibility

Under the previous law, the absence of clear regulations and standards for the presentation and adjudication of e-evidence significantly hampered the judicial process. This gap became particularly evident when judges confronted

e-evidence without established guidelines or consistent precedents. The problem was starkly illustrated in the *Wisni Yetti case*, where the court accepted evidence obtained through illegal access by a witness.[50] We argue that the case generated divergent outcomes at different judicial levels, revealing the inconsistent treatment of e-evidence within the system. When the case was reopened for reconsideration (*Peninjauan Kembali*) in 2018, an eyewitness admitted that the evidence relied upon had been produced through unlawful access to Yetti's social media account, from which screenshots and copies had been made. Despite this admission, the *Pengadilan Negeri* (District Court) continued to treat the evidence as admissible.

During the *Peninjauan Kembali* process, the importance of validating the printouts against their original digital versions was repeatedly emphasised. Nonetheless, the court did not require the public prosecutor to produce these original digital files for verification, reflecting a persistent preference for "conventional" forms of evidence over electronic counterparts. Even if the court's approach arguably satisfied a minimal evidentiary threshold, it raised serious concerns about the thoroughness of fact-finding, particularly in relation to establishing *actus reus* and *mens rea*. The lack of rigorous validation and verification of e-evidence in this and other cases highlighted the systemic weaknesses of the earlier framework.

The old system therefore risked inadvertently endorsing illegal investigatory practices and undermining the integrity of the legal process. In the absence of a clear regulatory framework and sustained judicial vigilance, unlawfully obtained electronic material could readily penetrate the evidentiary record. Addressing this would have required courts to prioritise a rigorous examination of the authenticity and legality of e-evidence, and legislators to develop specific procedural guidelines for its collection, preservation, and use. The repeated failure to subject e-evidence to robust scrutiny underscored the need for comprehensive reform.

Within Indonesian legal scholarship, Atmasasmita argued that the illegal acquisition of evidence did not necessarily render it inadmissible but instead reduced its "degree" of probative value.[51] However, what a diminished probative

---

[50] *Wisni Yetti,* Putusan Mahkamah Agung RI No. 324 PK/PID.SUS/2018 (January 17, 2019), https://putusan3.mahkamahagung.go.id/direktori/index/kategori/ite-1/amar/KABUL.html.

[51] See R. Atmasasmita, *Bunga Rampai Hukum Acara Pidana* (Binacipta, 1983); and Adam Ilyas, 'Praktik Penerapan Exclusionary Rules Di Indonesia', *Masalah-Masalah Hukum* 50, no. 1 (2021): 49–59, https://doi.org/10.14710/mmh.50.1.2021.49-59, 52.

value entailed in practice remained ambiguous; a plausible interpretation is that unlawfully obtained evidence would require additional corroboration to establish a legal fact. By contrast, the late Supreme Court judge Alkostar maintained that the rule of law required that evidence obtained in violation of constitutional rights or through illegal procedures should not be used in court, embracing what is commonly known as the exclusionary rule, even though Indonesia did not formally recognise it.[52] He illustrated this by describing a nocturnal police search conducted without proper notification to local authorities (*RT/RW* or *Lurah*), during which narcotics were allegedly found in the homeowner's kitchen without lawful procedural safeguards—conduct that violated Articles 125, 126, and 129 of the CPA 1981. Subsequent developments, including Constitutional Court Decision No. 21/PUU-XII/2014, expanded the scope of pre-trial review beyond Article 77 CPA 1981 to include the designation of suspects and the legality of searches and seizures.[53] At the same time, the legal validity of the Investigation Report (*Berita Acara Pemeriksaan*, BAP) remained central to the legitimacy of the indictment, whose adequacy was assessed against the formal and material requirements in Article 143(2)a–b CPA 1981.[54] Taken together, these elements demonstrated how fragmented and convoluted the framework for assessing the admissibility of e-evidence had become under the old regime.

B. The New Law: Risks of Formalistic Ex Ante Control and Burdensome Ex Post Review

The new KUHAP places particular emphasis on the "*penguatan mekanisme praperadilan*" (strengthening of the pre-trial mechanism). It does so by substantially broadening the scope of *Praperadilan* and enhancing the remedies available, thereby promoting accountability and the protection of human rights.[55] Its core function is expressly defined as "*menguji keabsahan tindakan Penyidik dan Penuntut Umum dalam peradilan pidana*" (to test the legality of actions by the investigator and the prosecutor in criminal

---

[52] Artidjo Alkostar, 'Kebutuhan Responsifitas Perlakuan Hukum Acara Pidana Dan Dasar Pertimbangan Pemidanaan Serta Judicial Immunity', Mahkamah Agung Republik Indonesia, 2011, 2.

[53] Anugerah Rizki Akbari et al., *Audit KUHAP: Studi Evaluasi Terhadap Keberlakuan Hukum Acara Pidana Indonesia* (Institute for Criminal Justice Reform, 2022), 33

[54] Artidjo Alkostar, 'Kebutuhan Responsifitas Perlakuan Hukum Acara Pidana Dan Dasar Pertimbangan Pemidanaan Serta Judicial Immunity', 2.

[55] See The General Elucidation, KUHAP 2025.

proceedings). The new KUHAP specifies that a range of procedural decisions and actions may be challenged through this mechanism, including the execution of coercive measures (*upaya paksa*), termination of cases, seizure of items unrelated to the alleged offence, undue delays in case handling, postponement of detention, and claims for compensation and rehabilitation.[56] In addition, Article 163(3)d clearly provides that evidence obtained unlawfully through search, seizure, or interception must be excluded. This development marks a departure from the previous framework and introduces more pronounced adversarial safeguards into Indonesia's hybrid CJS.[57]

However, the new KUHAP also establishes a significant limitation on review. Coercive measures (*upaya paksa*) that have already obtained permission or approval from the Chief of the District Court are not subject to *Praperadilan*.[58] In effect, prior judicial authorisation can immunise the subsequent execution of measures such as search, seizure, and blocking (*blokir*) from later scrutiny by the *Praperadilan* judge, shifting the locus of oversight to the initial granting of the warrant rather than the legality and propriety of its implementation (except for the specific possibility of reviewing the seizure of unrelated items).

The explanatory memorandum to Article 4 notes that Indonesian criminal procedure combines elements of both the continental European and adversarial traditions, with the latter associated with a stronger commitment to procedural justice. That aspiration, however, can only be meaningfully realised if coercive measures are subject to rigorous ex ante safeguards and effective ex post control. Whilst the new KUHAP formally maintains judicial control by requiring that all coercive measures be authorised by the Chief of the District Court, the breadth of the exception from *Praperadilan* review risks transforming warrant authorisation into a routine rubber-stamping formality rather than a substantive safeguard.

Taken together, the shift in *Praperadilan* under the new KUHAP carries important consequences for the admissibility of e-criminal evidence, not least because it reveals both an expansion and a simultaneous containment of judicial oversight. The old regime lacked clear procedural standards for e-evidence, tolerated the admission of unlawfully obtained material, and relied on fragmented doctrines that risked normalising investigative illegality. Under the old law, *Praperadilan* did not function as a mechanism to challenge the

---

[56] See Article 158, KUHAP 2025.

[57] See Elucidation of Article 4 para 3, KUHAP 2025.

[58] See Elucidation of Article 158 letter a, KUHAP 2025.

admissibility of evidence, leaving questions about the legality of evidentiary acquisition largely outside meaningful pre-trial scrutiny. The new KUHAP appears to respond to that deficiency through the stated objective of "*penguatan mekanisme praperadilan*," broadening the scope of *Praperadilan* and strengthening available remedies in the name of accountability and human rights protection. Yet this reform is internally compromised by a major limitation: coercive measures (*upaya paksa*) that have already received permission or approval from the Chief of the District Court are excluded from *Praperadilan* review. That restriction is difficult to reconcile with the claimed strengthening of pre-trial safeguards, because it risks converting judicial authorisation into a shield against subsequent scrutiny rather than a trigger for deeper accountability.

Additionally, the gains were undercut by the heavy reliance on ex post review and by the broad immunity granted to coercive measures once authorised ex ante by the Chief of the District Court, which threatened to turn warrant authorisation into a largely formalistic exercise. In the context of e-criminal evidence, this is particularly problematic, since digital searches, seizures, interceptions, and extractions often involve intrusive and technically opaque methods that demand rigorous review. By insulating court-approved coercive measures from challenge, the new KUHAP risks fostering judicial passivity, where courts defer to prior formal authorisation instead of substantively examining whether rights were infringed in the collection of evidence. The result is a troubling institutional imbalance in rights protection: investigators and prosecutors retain broad practical control over the production and use of e-evidence, whilst the judiciary's supervisory role is weakened precisely where constitutional vigilance should be strongest. Rather than fully strengthening *Praperadilan*, the reform may therefore entrench a model of oversight that is broader in form but narrower in effect.

Overall, whilst the legislative reform moved Indonesian criminal procedure closer to a model of procedural justice, it did not fully resolve the tension between effective law enforcement and the protection of fair-trial rights, and it underscored the continuing need for stricter standards, clearer evidentiary rules, and more substantive judicial scrutiny of both the authorisation and execution of coercive measures, particularly in cases involving e-evidence.

C. Beyond Authenticity and Legality: Embedding Reliability in the Law of e-Criminal Evidence

The reliability of e-evidence is a precondition for both its admissibility and its probative value in criminal proceedings, and safeguarding this reliability demands the coherent integration of technical and legal requirements across the entire evidential lifecycle.[59] The core objective is to ensure that e-evidence is authentic, accurate, complete, and trustworthy.[60] Because e-evidence is highly volatile (easy to change, damage, or lose) and susceptible to being falsified, intercepted, removed, or engineered, rigorous processes are mandatory.[61] For judicial fact-finding, reliability thus stands alongside authenticity and legality as a distinct and indispensable criterion for establishing legal truth.[62] Yet, standards governing the authentication of e-evidence remain underdeveloped, typically lacking robust requirements for a documented chain of custody or forensically sound handling of data. Notably, both the previous and the new legislative frameworks fail to provide an explicit chain of custody regime for e-evidence, thereby perpetuating a structural weakness in the protection of its integrity and, ultimately, in the credibility of criminal adjudication that relies upon it.

Under the previous framework, Indonesian criminal procedure was highly fragmented, particularly in relation to e-evidence. Multiple investigatory bodies operated under a dispersed set of norms, including Government Regulation No. 27 of 1983 on the Implementation of the Criminal Procedure Act (as amended)[63] and Government Regulation No. 43 of 2012 on coordination,

---

[59] Albert Antwi-Boasiako and Hein Venter, 'A Model for Digital Evidence Admissibility Assessment'; Radina Stoykova and Katrin Franke, 'Reliability Validation Enabling Framework (RVEF) for Digital Forensics in Criminal Investigations', *Forensic Science International: Digital Investigation* 45, no. 301554 (2023): 1, https://doi.org/10.1016/j.fsidi.2023.301554.

[60] A. Yeboah-Ofori and A. D. Brown, 'Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence'.; Hongjiao, 'Application of Digital Evidence in Criminal Cases: Dilemma and Optimization'.

[61] Albert Antwi-Boasiako and Hein Venter, 'A Model for Digital Evidence Admissibility Assessment'; Salmah, 'Ensuring the Admissibility and Credibility of Electronic Evidence in Indonesian Criminal Proceedings'; Ahmad Fekry Moussa, 'Electronic Evidence and Its Authenticity in Forensic Evidence', *Egyptian Journal of Forensic Sciences* 11, no. 1 (2021), https://doi.org/10.1186/s41935-021-00234-6; Olivier Leroux, 'Legal Admissibility of Electronic Evidence', *International Review of Law, Computers & Technology* 18, no. 2 (2004): 193–220, https://doi.org/10.1080/1360086042000223508.

[62] See Alvin I Goldman, 'Legal Evidence', *The Blackwell Guide to the Philosophy of Law and Legal Theory*, Wiley Online Library, 2005, 163–75, 170; also *Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 589 (1993)*; Susan Haack, *Evidence Matters: Science, Proof, and Truth in the Law*, Law in Context (Cambridge University Press, 2014), Cambridge Core, https://doi.org/10.1017/CBO9781139626866, 201.

[63] See Government Regulation No. 58 of 2010 and Government Regulation No. 92 of 2015.

supervision, and technical guidance for special police and civil servant investigators, alongside the CPA 1981. At the investigative level, the Police Chief Regulation No. 6 of 2019—adopted in response to Constitutional Court Decision No. 130/PUU-XIII/2015 and replacing Regulation No. 14 of 2012—sought to systematise investigative procedures, whilst Regulation No. 10 of 2009 provided technical guidelines for crime scene examination and laboratory analysis. Yet these instruments largely presuppose traditional, physical forms of evidence and remain ill-adapted to the identification, collection, acquisition, and preservation of e-evidence. The same structural weakness is evident in Minister of Law and Human Rights Regulation No. 16 of 2014 on seized-goods storage, which designates *Rupbasan* as the repository for seized items but fails to address the specific requirements of secure digital storage, and in Attorney General and Police regulations that focus primarily on tangible property in the context of asset recovery. Although Attorney General Guideline 24/2021 acknowledges that physical seizure of entire systems is unnecessary where complete forensic copies can be made,[64] it also exposes deeper conceptual and technical ambiguities, such as the fact that duplicating a computer file does not "seize" the data in a legally meaningful sense, but only the medium that contains it. Most of these implementing regulations post-date the EIT Act, yet the overall framework for evidence collection, processing, and preservation still marginalises e-evidence, and the EIT Act itself declines to mandate any detailed procedural regulations, thereby entrenching normative and practical gaps in the treatment of e-evidence.

The new KUHAP, as earlier explained, introduces provisions on *Bantuan Teknis Penyidikan* (Technical Assistance for Investigation)[65] intended to support law enforcement in dealing with scientific and specialised forms of proof, including digital forensics. In principle, this mechanism is designed to ensure that investigators are assisted by appropriate technical expertise in producing scientifically grounded evidence (*pembuktian secara ilmiah*). However, the detailed outlines of this regime are deferred to a future Government Regulation (*Peraturan Pemerintah*), which, at the time of writing, has not yet been enacted. This legislative choice weakens the immediate normative impact of the reform: without clear secondary rules on methods, standards, and institutional responsibilities, "technical assistance" risks

[64] See Attorney General of Republic of Indonesia Guidelines 24/2021 on Handling General Criminal Case, 151.

[65] See Articles 55-57, KUHAP 2025.

remaining a largely aspirational label rather than a concrete guarantee of forensic reliability.

More fundamentally, the Indonesian framework continues to prioritise authenticity and formal legality in determining evidentiary admissibility, whilst largely neglecting the distinct requirement of reliability, particularly for e-evidence. The absence of detailed implementing provisions on core digital forensic practices—such as the forensic imaging of storage media, including requirements on bit-stream copying, order-preserving duplication, and the documentation of all handling[66]—means that the system offers little concrete guidance on how e-evidence should be collected, preserved, and examined in a forensically sound manner. As a result, the new KUHAP, despite its gestures towards scientific proof, does not yet resolve the structural deficiencies that undermine the reliability of e-evidence in practice.

Reliability in digital forensics is best understood as a property of the investigative process as a whole,[67] expressed in its capacity to yield consistent, reproducible, and scientifically defensible results.[68] This presupposes the standardisation of forensic stages—acquisition, examination, analysis, and reporting—in line with national and international benchmarks such as ISO/IEC 27037:2012,[69] ISO/IEC 17025,[70] and recognised professional guidelines (e.g. the Association of Chief Police Officers Good Practice Guide, ACPO).[71] Within this framework, reliability depends on the technical assurance of integrity and authenticity, safeguarded through measures such as

---

[66] See Orin S. Kerr, 'Search Warrants in An Era of Digital Evidence', *Missisipi Law Journal* 75 (2005): 85, 88 & 95; and Rebecca Mitchell et al., 'The Search and Seizure of Digital Materials Under Warrant and Protecting Privilege: Comparative Analysis and Recommendations for Best Practice', *The Journal of Criminal Law*, ahead of print, 2024, https://doi.org/10.1177/00220183231223592, 16.

[67] Radina Stoykova, 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence', *Computer Law & Security Review* 42, no. 105575 (2021): 1–20, https://doi.org/10.1016/j.clsr.2021.105575.

[68] Radina Stoykova et al., 'Reliability Assessment of Digital Forensic Investigations in the Norwegian Police', *Forensic Science International: Digital Investigation* 40 (March 2022): 301351, https://doi.org/10.1016/j.fsidi.2022.301351, 2.

[69] International Organisation for Standardisation, *ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence* (International Organisation for Standardisation, 2012), 1–38.

[70] International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 17025: General Requirements for the Competence of Testing and Calibration Laboratories (Geneva: ISO, 2017).

[71] Albert Antwi-Boasiako and Hein Venter, 'A Model for Digital Evidence Admissibility Assessment', 26.

cryptographic hashing at the point of acquisition, the use of write-blockers, and the restriction of examinations to forensic copies.[72] These safeguards must be embedded within a continuous preservation regime and supported by a strict, well-documented chain of custody that provides a complete audit trail from initial seizure through to presentation in court; without such documentation, continuity and thus reliability cannot be convincingly demonstrated.

At the same time, technical reliability requires the validation of methods, tools, and personnel. Forensic tools and models must be tested, peer-reviewed where possible, and deployed with known and documented error rates, in accordance with criteria analogous to the *Daubert* standard,[73] whilst examiners must possess demonstrable expertise and be able to justify each step taken in handling and interpreting e-evidence. Yet even the most robust technical practices are insufficient if divorced from legal legitimacy: e-evidence must be obtained under lawful authority and be relevant to the issues in dispute, failing which it may be excluded or accorded limited weight to protect due process and individual rights. Reliability in digital forensics is therefore not merely a technical attribute but the outcome of an integrated architecture that combines standardised processes, technical safeguards, procedural guarantees, scientific validation, and compliance with substantive and procedural law.

Practical implementation necessitates additional regulations to provide law enforcement with a clear operational framework. Although steps have been taken to create thorough guidelines for handling e-evidence, like adopting ISO/IEC 27037:2012 as a national standard without any modification,[74] implementation has been hindered due to the lack of a specific regulatory framework. Further discussion of the ISO is provided in Section 4, which examines the current situation and considers the way forward.

The analysis so far has exposed critical gaps and inadequacies within Indonesia's legal framework for e-evidence. The current laws and regulations evidently struggle to keep pace with the digital age, often lacking clear guidance

---

[72] See also Adi Setya and Abba Suganda, 'Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014', *JUITA: Jurnal Informatika* 10, no. 1 (2022): 127–38, https://doi.org/10.30595/juita.v10i1.13149, 134; Albert Antwi-Boasiako and Hein Venter, 'A Model for Digital Evidence Admissibility Assessment', 30; Orin Kerr, 'Digital Evidence and the New Criminal Procedure', *Columbia Law Review* 105 (2005): 279–318, 288.

[73] *Daubert v. Merrell Dow Pharmaceuticals, Inc.,* 509, U.S. 579 (1993).

[74] Badan Standardisasi Nasional, *SNI ISO/IEC 27037:2014 Teknologi Informasi—Teknik Keamanan—Pedoman Untuk Identifikasi, Pengumpulan, Akuisisi Dan Pelestarian Bukti Digital*, 2014.

for law enforcement and the judiciary, raising questions about the accuracy of adjudication. Whilst the challenges of securing and analysing e-evidence obtained through traditional investigative methods are significant, publicly available online information, whilst easily obtained and potentially valuable for investigations, introduces unique considerations regarding authentication, relevance, and the potential for privacy violations.[75] The following discussion will explore the legal and practical implications of using open-source e-evidence in Indonesian criminal proceedings.

Open-source e-Criminal Evidence and the Challenges

The vast amount of publicly available online information, including social media posts and news reports, may provide valuable leads and corroborative evidence in various cases. Such material may be collected as open-source evidence. Open-source e-evidence presents a significant opportunity to enhance criminal investigations.[76] However, the challenges surrounding the collection, acquisition, and admissibility of open-source e-evidence, often obtained from publicly available websites and social media, in Indonesia are systemic. They stem from a fundamental mismatch between the unique, volatile nature of this digital information and the nation's existing legal and procedural frameworks, which remain heavily rooted in concepts designed for physical, analogue evidence.

A. Legal Ambiguity and Procedural Circumvention

The primary challenge lies in the lack of clear and comprehensive legislation specifically governing the handling and collection of publicly available digital data, forcing law enforcement to employ ad-hoc or circumventing procedures. This article identifies that, in this matter, Indonesia has general law yet specific problem. Although the CJS recognises electronic

---

[75] On the privacy violations in Indonesia context see Rina Shahriyani Shahrullah et al., 'Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment', *Hasanuddin Law Review* 10, no. 1 (2024), http://dx.doi.org/10.20956/halrev.v10i1.5016, 3.

[76] Cecelia Horan and Hossein Saiedian, 'Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions', *Journal of Cybersecurity and Privacy* 1, no. 4 (2021): 580–96, https://doi.org/10.3390/jcp1040029, 580.

information and documents as valid legal evidence,[77] the law does not explain in detail how proper handling of such evidence should proceed.

The new KUHAP stipulates that unlawfully (illegally) obtained electronic information may be excluded from evidence.[78] However, uncertainty arises because the methods used to obtain open-source data may be disregarded in practice. Where evidence is acquired unlawfully, the court may exclude it or find that it has no evidentiary value. In the context of open-source data, this implies that the court must assess whether the method of collection was lawful and appropriate, even in the absence of clear procedural guidelines.

The lack of proper digital forensic procedures for open-source material[79] means that unverifiable documentation, particularly printouts, could potentially be the default method of online content presentation in the courtroom. This undermines the scientific verification required for open source e-evidence.

B. Volatility, Integrity, and Chain of Custody Failures

One major challenge lies in establishing the authenticity[80] and reliability of open-source e-evidence. The nature of online information makes it susceptible to manipulation and fabrication, requiring meticulous efforts to verify its original source and ensure its accuracy.[81] Open-source data, such as content available on social media accounts, is logical information that is on the server and is vulnerable to change at any time, necessitating quick acquisition.[82] Moreover, the EIT Act mandates that e-evidence is only deemed valid if the information contained therein is accessible, displayable, guaranteed for its integrity, and accountable so as to explain a situation.[83] Due to the volatility of

---

[77] See Article 235(1)f, KUHAP 2025.

[78] See Article 235(5), KUHAP 2025.

[79] See Elizabeth White, 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism', *Leiden Journal of International Law* 37, no. 1 (2024): 228–50, Cambridge Core, https://doi.org/10.1017/S0922156523000444.

[80] See Article 235(5), KUHAP 2025.

[81] Lewulis, 'Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law', 40.

[82] Setya and Suganda, 'Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014', 131.

[83] See Article 6, EIT Act (as amended).

open-source content, proving this integrity without scientific documentation is difficult.

The methods used to acquire open-source data, such as Screenshot, Screencast, Save Webpage, Data Export, or Application Programming Interface (API) access, have varying capabilities to prove authenticity and require specialised expertise.[84] For instance, the Data Export technique often relies on trusting the social network to extract a complete history, which itself is cited as a problem impacting reliability.[85] Sampson pointed out that if open-source intelligence (OSINT) is to be relied upon as evidence, the gatherer must ask questions about what processes they used to get it.[86] Additionally, a lack of standardised storage procedures can result in duplication of materials, make subsequent analyses difficult, and may even compromise the evidence itself.[87]

Furthermore, assessing the relevance of such evidence is crucial, as not all publicly available information necessarily possesses probative value for a given case.[88] Determining whether open-source e-evidence directly connects to the alleged crime and understanding its context are essential steps in maintaining the integrity of investigations.[89] Additionally, privacy concerns are paramount when dealing with open-source e-evidence, particularly when it involves personal or sensitive data.[90] Striking a balance between utilising valuable information for investigations and protecting individuals' privacy rights is crucial in upholding the principles of justice and fairness.

---

[84] Damir Kahvedžić, "Internet Searches and Computer Forensics: Using Open-Source Intelligence to Gather Evidence Online" (paper presented at Obtaining E-Evidence When Investigating and Prosecuting Crimes: Focus on the Whole Life Cycle of E-Evidence (Custody Chain, Presentation & Assessment) seminar, Cracow, March 24–25, 2022, event no. 322DT03f/SBa).

[85] Kahvedžić, "Internet Searches and Computer Forensics: Using Open-Source Intelligence to Gather Evidence Online".

[86] Fraser Sampson, 'Intelligent Evidence: Using Open Source Intelligence (OSINT) in Criminal Proceedings', *The Police Journal* 90, no. 1 (2017): 55–69, https://doi.org/10.1177/0032258X16671031.

[87] White, 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism'.

[88] Keith Hiatt, 'Open Source Evidence on Trial', *Yale Law Journal Forum* 125 (2016), 326

[89] See Keith Hiatt, 'Open Source Evidence on Trial', 326 & 328; see also White, 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism', 232.

[90] Keith Hiatt, 'Open Source Evidence on Trial', 324.

The absence of specific provisions in Indonesian law necessitates reliance on general principles of evidence and existing regulations, which may not adequately address the unique characteristics of open-source e-evidence. This legal void, coupled with the increasing ubiquity of online information, emphasises the urgency for a comprehensive legal framework tailored to the use of open-source e-evidence in criminal investigations. Such a framework should address authentication protocols, relevance assessment, and privacy safeguards, ensuring this valuable investigative tool is utilised responsibly and effectively in pursuing justice. However, establishing such a framework requires legal reform and technical guidance. International standards, such as the ISO/IEC 27037:2012, could offer valuable insights into best practices for e-evidence handling. The following section will discuss the challenges encountered in implementing and practically applying the ISO/IEC 27037:2012 standard in Indonesia, highlighting the need for adaptation and integration within the country's legal and investigative procedures.

SNI ISO/IEC 27037:2014—an Untapped Resource

The ISO/IEC 27037:2012 standard, adopted in Indonesia as SNI ISO/IEC 27037:2014,[91] provides a structured methodological framework for the identification, acquisition, handling, and preservation of e-evidence, defined as "digital data that may possess evidential value" in legal proceedings.[92] It sets out internationally recognised good-practice requirements for the initial handling of e-evidence,[93] emphasising the use of appropriate tools and methods, the credibility and competence of Digital Evidence First Responders (DEFRs) and Digital Evidence Specialists (DESs).[94] International scholars such as

[91] Badan Standardisasi Nasional, *SNI ISO/IEC 27037:2014 Teknologi Informasi—Teknik Keamanan—Pedoman Untuk Identifikasi, Pengumpulan, Akuisisi Dan Pelestarian Bukti Digital*.

[92] International Organisation for Standardisation, *ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, 1.

[93] A. Ajijola et al., 'A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012', *World Congress on Internet Security (WorldCIS-2014)*, 8 December 2014, 66–73, https://doi.org/10.1109/WorldCIS.2014.7028169.

[94] International Organisation for Standardisation, *ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*.

Boasiako and Venter,[95] Ajijola et al.,[96] and Stoykova et al.[97] have explicitly advocated the adoption of this standard by law enforcement agencies as a means of aligning investigative practice with forensic best practice, whilst Indonesian digital forensic academics—including Prayudi et al.[98] and Setya and Suganda[99]—have similarly called for the development of a standardised system modelled on SNI ISO/IEC 27037:2014.

The standard provides detailed guidance on recognising potential e-evidence, documenting crime scenes, collecting and preserving electronic data,[100] and ensuring secure packaging and transportation across a wide range of devices and environments, including computers, mobile phones, PDAs/PEDs, memory cards, navigation systems, digital cameras, and TCP/IP-based networks (the list being indicative rather than exhaustive).[101] Its core purpose is to ensure that e-evidence is relevant, reliable, and sufficient for judicial scrutiny. Reliability is strengthened by requiring DEFRs and DESs to verify that potential e-evidence accurately corresponds to its original source;[102] integrity is protected by mandating that examination and analysis are carried out on forensic copies rather than on original media; and sufficiency is supported by meticulous documentation and quality control.[103] In particular, the standard embeds the principles of auditability, repeatability, reproducibility, and justifiability in all stages of evidence handling, and requires a rigorous, logically coherent chain of custody that records the chronological history of all transfers and interventions. As Stoykova notes, such a chain of custody not only supports technical assessment of the probative value of evidence but also ensures that legal

---

[95] Albert Antwi-Boasiako and Hein Venter, 'A Model for Digital Evidence Admissibility Assessment'.

[96] A. Ajijola et al., 'A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012'.

[97] Radina (Adi) Stoykova, 'A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings', *Computer Law & Security Review* 55 (November 2024): 106040, https://doi.org/10.1016/j.clsr.2024.106040.

[98] Yudi Prayudi et al., 'A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia', *I. J. Computer Network and Information Security* 11 (2015): 1–8.

[99] Setya and Suganda, 'Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014'.

[100] International Organisation for Standardisation, *ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, 6-7.

[101] International Organisation for Standardisation, 1.

[102] International Organisation for Standardisation.

[103] International Organisation for Standardisation, 6.

challenges focus on valid grounds and that bias or parallel construction can be exposed.[104]

In the Indonesian context, however, the practical integration of SNI ISO/IEC 27037:2014 into the procedures of law enforcement agencies—especially the Indonesian National Police (Polri)—remains limited. The standard is non-compulsory, has not been translated into Bahasa Indonesia, and has been adopted by the National Standard Agency rather than directly by law enforcement bodies, which significantly restricts its operational uptake. These institutional and linguistic barriers are compounded by procedural gaps in existing Indonesian legislation, including the absence of detailed cybercrime handling guidelines that systematically incorporate digital forensic methods. As a result, the potential of SNI ISO/IEC 27037:2014 as a reference model for Indonesian practice is largely unrealised.

For Indonesia, the key insight is that the existence of a high-quality technical standard is necessary but not sufficient: it must be made accessible, formally recognised, and legally binding. A holistic reform strategy would therefore require, at minimum, (i) translating the standard into Bahasa Indonesia, (ii) formally integrating its core provisions—competent and authorised DEFRs, mandatory use of forensic copies, comprehensive and auditable chains of custody,[105] and processes that are demonstrably repeatable, reproducible, and justifiable—into binding procedural rules, and (iii) embedding these rules either through targeted amendments to the new KUHAP and its implementing regulations, or through law enforcement agencies' regulations that are more coherently tailored to the realities of e-evidence. The essential requirement for Indonesia is to align its procedural law with the substantive guarantees embodied in SNI ISO/IEC 27037:2014, thereby securing the integrity, reliability, and admissibility of e-evidence in its CJS.

A further consequence of making SNI ISO/IEC 27037:2014 mandatory would be a significant restructuring of institutional practice across the CJS. For the police, it would require the formal revision of standard operating procedures for search, seizure, imaging, storage, and transfer of digital devices; the designation, training, certification, and periodic evaluation of authorised DEFRs and DESs; investment in forensic laboratories, validated tools, secure

---

[104] Radina Stoykova, 'Encrochat: The Hacker with a Warrant and Fair Trials?', *Forensic Science International: Digital Investigation* 46 (2023), https://doi.org/10.1016/j.fsidi.2023.301602, 6.

[105] International Organisation for Standardisation, *ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*.

evidence storage, and audit systems; and the creation of internal supervision and accountability mechanisms for breaches of chain of custody or other forensic requirements. For public prosecutors, mandatory adoption would shift their role from merely receiving e-evidence to actively scrutinising whether it was identified, acquired, preserved, and documented in compliance with the standard before relying on it in indictments and at trial, thereby increasing the need for prosecutorial guidelines, specialised expertise, and closer coordination with investigators. For courts, it would provide a clearer benchmark for assessing authenticity, integrity, reliability, and probative value of e-evidence, whilst also requiring judges to develop greater technical literacy in digital forensic processes and to treat non-compliance with mandatory safeguards as a factor affecting admissibility or evidential weight. In practical terms, therefore, mandatory incorporation of the standard would not only improve evidential quality but would also institutionalise forensic discipline, redistribute professional responsibilities, and create a more transparent and reviewable framework for handling e-evidence across police, prosecutorial, and judicial institutions.

Indonesia's e-Criminal Evidence Framework Reform: (Still) Adapting to the Digital Age

Indonesia must modernise its framework on e-evidence if the CJS is to produce accurate and defensible outcomes. The existing regime remains fragmented and dominated by an analogue mindset, insufficiently attuned to the technical characteristics and vulnerabilities of e-evidence. As a result, it struggles to capture the nuances of digital data, risks hindering effective investigation, and creates gaps in the protection of human rights. A comprehensive and forward-looking reform is therefore required. This paper recommends such reforms into legislative, institutional, and technical forensic reform.

At the legislative level, the proper legislative reform is to make KUHAP the complete procedural code for the criminal use of digital material, while aligning its definitions with the broader EIT taxonomy and expressly codifying the admissibility conditions that are currently missing or underdeveloped. First, it should adopt a technology-neutral threshold definition of e-evidence that captures electronically encoded, transmitted, received, processed, or stored data before admissibility filters are applied. Second, it should separate ontology from admissibility: the statute should distinguish what counts as digital material from the separate questions of legality of acquisition, authenticity, integrity, reliability, chain of custody, and evidential weight. Third, it should preserve

clear doctrinal boundaries between *Informasi Elektronik*, *Dokumen Elektronik*, printouts, *surat*, and physical exhibits, so that the categories do not collapse into each other. Fourth, KUHAP should contain its own general definition of "electronic system", rather than leaving that foundation to be supplied externally. Fifth, KUHAP should state—at least at framework level—the minimum normative conditions under which electronic material can function as criminal evidence. The present KUHAP text recognises e-evidence and describes its scope, but it does not itself provide that fuller criminal-evidence architecture.

On that foundation, detailed rules are needed for the entire lifecycle of e-evidence: identification, collection, acquisition, preservation, chain of custody, storage, analysis, and verification. These rules must be structured not only around authenticity and legality, but also around reliability, understood as the capacity of evidence to withstand scrutiny regarding its integrity, completeness, and resistance to manipulation. This entails, inter alia, mandatory preservation of original data and metadata, explicit requirements to compare any printout or derivative format with its electronic source, and the use of validated forensic tools and methods.

The legislative framework must further address digital search and seizure by providing explicit rules on lawful access to e-evidence where consent is withheld, including data production orders, evidence isolation, and limits on investigators' powers to copy, filter, and segregate data. It must also incorporate safeguards consistent with due process and human rights, since concentrating warrant-issuing authority in the Chief of the District Court without substantive criteria or meaningful review risks reducing judicial authorisation to a formalistic ex ante ritual rather than a genuine rights-protective filter. Finally, legislation should expressly regulate open-source e-evidence and cross-border data access, recognising the former's potential probative value whilst imposing strict safeguards concerning authenticity, reliability, privacy, and proportionality, and clarifying jurisdictional limits to prevent conflicts of law, forum shopping, and rights-violating extraterritorial practices.

At the institutional level, legislative revision must be supported by operationally realistic implementing measures across the CJS. Law enforcement agencies should be placed under a clear statutory duty to employ standardised validation and verification mechanisms rather than relying on ad hoc practices, whilst police, prosecutors, and courts should each be assigned defined responsibilities in relation to the handling and assessment of e-evidence. For investigators, this requires institutional procedures governing lawful collection, preservation, documentation, and transfer; for prosecutors, it requires

systematic scrutiny of whether e-evidence has been obtained and handled in accordance with legal and forensic requirements before it is relied upon in charging and trial; and for courts, it requires a structured framework for assessing the authenticity, integrity, reliability, and probative value of digital material. Institutional reform also entails specialised training, accreditation, and oversight mechanisms for those involved in e-evidence handling, together with clearer inter-agency coordination and internal accountability for breaches of chain of custody or other evidential safeguards. In this sense, institutional reform translates legislative norms into enforceable professional practice.

At the technical forensic level, the reformed framework must be supported by detailed forensic protocols that render legal standards operational in practice. Technical guidance should regulate the handling, storage, preservation, and verification of digital material in ways that are both scientifically sound and legally intelligible. This includes rigorous chain-of-custody procedures, documentation of collection methods, preservation of metadata, forensic imaging, verification of forensic copies against original sources, and the use of validated tools and reproducible methods. In this respect, the translated and operationalised SNI ISO/IEC 27037:2014 standard could serve as a foundational reference for Indonesian practice, particularly in relation to the identification, acquisition, handling, and preservation of e-evidence. The same approach should apply to open-source e-evidence, where technical procedures must govern the capture and preservation of publicly accessible data, including documentation of screenshots, web-crawling, or API extraction, whilst ensuring that intrusive surveillance is not disguised as open-source collection. Taken together, these three levels of reform would create a coherent framework in which legislative norms, institutional responsibilities, and forensic methods mutually reinforce one another, thereby improving the integrity, reliability, and admissibility of e-evidence in Indonesia's CJS.

6. Conclusion

Indonesia's legal framework for e-evidence is at a critical juncture. Despite the significant progress marked by the introduction of the new KUHAP and its pragmatic operability of the previous system, it does not adequately confront the distinctive legal and technical problems posed by e-evidence. The result is a framework that remains fragmented, under-specified, and overly dependent on judicial interpretation, thereby weakening legal certainty in an area where precision is indispensable. The absence of comprehensive rules on search and seizure, authentication, preservation, chain of custody, and forensic verification creates serious risks not only for effective law enforcement, but also for the

protection of individual rights. Without urgent reform, these deficiencies may become systemic: unreliable or improperly obtained e-evidence may be admitted without adequate scrutiny, coercive investigative powers may expand without corresponding safeguards, and fair trial guarantees may be progressively eroded in practice rather than denied in principle.

Moving forward, Indonesia should treat the regulation of e-evidence not as a peripheral technical matter, but as a central question for the future of criminal justice in the digital age. The recent reform of the Code—KUHAP—represents a missed opportunity. Rather than meaningfully addressing the challenges of digital investigation and embedding safeguards for coercive measures involving electronic data, the new KUHAP is perpetuating and even extending the existing patchwork of norms. A more coherent approach is therefore required. Instead of continuing to rely on fragmented *lex specialis* legislation, such as the EIT Act, Indonesia should insert and integrate a detailed and internally consistent regime for e-evidence directly into the new KUHAP and its implementing regulations. At the same time, clear operational guidelines must be developed for investigators, prosecutors, and judges. Only through such a holistic framework—one that combines doctrinal clarity, institutional responsibility, and technically sound forensic practice—can Indonesia build a system for handling e-evidence that is reliable, rights-compliant, and capable of strengthening both fair trial guarantees and the rule of law in an increasingly digital society.

References

Ajijola, A., P. Zavarsky, and R. Ruhl. 'A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012'. *World Congress on Internet Security (WorldCIS-2014)*, 8 December 2014, 66–73. https://doi.org/10.1109/WorldCIS.2014.7028169.

Antwi-Boasiako, Albert, and Hein Venter. 'A Model for Digital Evidence Admissibility Assessment'. In *IFIP Advances in Information and Communication Technology*, edited by Gilbert Peterson and Sujeet Shenoi, AICT-511. Advances in Digital Forensics XIII. Springer International Publishing, 2017.

Asimah, Dewi. 'To Overcome the Constraints of Proof in the Application of Electronic Evidence'. *Jurnal Hukum Peratun* 3, no. 2 (2021): 97–110. https://doi.org/10.25216/peratun.322020.97-110.

Badan Standardisasi Nasional. *SNI ISO/IEC 27037:2014 Teknologi Informasi—Teknik Keamanan—Pedoman Untuk Identifikasi, Pengumpulan, Akuisisi Dan Pelestarian Bukti Digital*. 2014.

Butt, Simon, and Tim Lindsey. 'The Criminal Procedure Code'. In *Crime and Punishment in Indonesia*, 1st edn. Routledge, 2020.

Biasiotti, Maria Angela, Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, and Fabrizio Turchi. 'Introduction: Opportunities and Challenges for Electronic Evidence'. In *Handling and Exchanging Electronic Evidence Across Europe*, edited by Maria Angela Biasiotti, Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, and Fabrizio Turchi. Springer, 2018.

Chamdani, and Asri Wijayanti. 'Critical Analysis about Legal Evidence in Court in the Justice System in Indonesia'. *Journal of Positive School Psychology* 6, no. 2 (2022): 5867–70.

Custers, Bart, and Lonneke Stevens. 'Data as Evidence in Criminal Courts: Comparing Legal Frameworks and Actual Practices'. In *Human-Robot Interaction in Law and Its Narratives: Legal Blame, Procedure, and Criminal Law*. Cambridge University Press, 2024.

Giri Santosa, Dewa Gede, and Karell Mawla Ibnu Kamali. 'Acquisition and Presentation of Digital Evidence in Criminal Trial in Indonesia'. *Jurnal Hukum Dan Peradilan* 11, no. 2 (2022): 195. https://doi.org/10.25216/jhp.11.2.2022.195-218.

Goldman, Alvin I. 'Legal Evidence'. *The Blackwell Guide to the Philosophy of Law and Legal Theory*, Wiley Online Library, 2005, 163–75.

Haack, Susan. *Evidence Matters: Science, Proof, and Truth in the Law*. Law in Context. Cambridge University Press, 2014. Cambridge Core. https://doi.org/10.1017/CBO9781139626866.

Herring, Jonathan. *Criminal Law: Text, Cases, and Materials*. Oxford University Press, 2022.

Hiatt, Keith. 'Open Source Evidence on Trial'. *Yale Law Journal Forum* 125 (2016).

Hongjiao, L. 'Application of Digital Evidence in Criminal Cases: Dilemma and Optimization'. *Contemporary Social Sciences* 9, no. 6 (2024): 115–31. Scopus.

Horan, Cecelia, and Hossein Saiedian. 'Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions'. *Journal of Cybersecurity and Privacy* 1, no. 4 (2021): 580–96. https://doi.org/10.3390/jcp1040029.

Ingram, Jefferson L. *Criminal Evidence*. 13th Edition. Routledge, 2018.

International Organisation for Standardisation. *ISO/IEC 27037:2012 - Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*. International Organisation for Standardisation, 2012.

Keane, Adrian, and Paul McKeown. *The Modern Law of Evidence*. 9th edn. Oxford University Press, 2012.

Kerr, Orin. 'Digital Evidence and the New Criminal Procedure'. *Columbia Law Review* 105 (2005): 279–318.

Kerr, Orin. 'Search Warrants in An Era of Digital Evidence'. *Missisipi Law Journal* 75 (2005): 85.

Leroux, Olivier. 'Legal Admissibility of Electronic Evidence'. *International Review of Law, Computers & Technology* 18, no. 2 (2004): 193–220. https://doi.org/10.1080/1360086042000223508.

Lewulis, Piotr. 'Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law'. *Criminal Law Forum* 33, no. 1 (2021): 39–62. https://doi.org/10.1007/s10609-021-09430-4.

Listiyanto, Apri. 'Pembaharuan Sistem Hukum Acara Pidana'. *Jurnal Rechtsvinding* Rechtsvinding Online (2017): 1–4.

Luhmann, Niklas. *Law As A Social System*. Oxford University Press, 2004. https://doi.org/10.1093/oso/9780198262381.001.0001.

Makarim, Edmon. 'Electronic Evidence and Electronic Signatures in Indonesia: The Probative Value of Digital Evidence'. *Digital Evidence and Electronic Signature Law Review* 10 (2013): 136–43.

Mason, Stephen and Daniel Seng, "The Foundations of Evidence in Electronic Form," in *Electronic Evidence and Electronic Signatures*, , edited by Stephen Mason and Daniel Seng. University of London Press, Institute of Advanced Legal Studies, 2021.

Mitchell, Rebecca, Michael Stockdale, and Francis A. Gilligan. 'The Search and Seizure of Digital Materials Under Warrant and Protecting Privilege: Comparative Analysis and Recommendations for Best Practice'. *The Journal of Criminal Law*, ahead of print, 2024. https://doi.org/10.1177/00220183231223592.

Moussa, Ahmad Fekry. 'Electronic Evidence and Its Authenticity in Forensic Evidence'. *Egyptian Journal of Forensic Sciences* 11, no. 1 (2021). https://doi.org/10.1186/s41935-021-00234-6.

Murdoch, Steven J., Daniel Seng, Burkhard Schafer, and Stephen Mason. *The Sources and Characteristics of Electronic Evidence and Artificial Intelligence*. Institute of Advanced Legal Studies, 2021.

Nazran, Finna, Tan Kamello, Hasim Purba, and Saidin. 'The Legal Paradigm in a Global Context: Judicial of Evidence in Actualization of Electronic in Indonesia'. 642 (2021): 154–58.

Oerlemans, Jan-Jaap, and Maša Galič. 'Cybercrime Investigations'. In *Essentials in Cybercrime: A Criminological Overview for Education and Practice*. Eleven International Publishing, 2022.

Ontanu, Elena Alina. 'Normalising the Use of Electronic Evidence: Bring Technology Use into a Familiar Normative Path in Civil Procedure'. *Oñati Socio-Legal Series* 12, no. 3 (2022): 582–615. https://doi.org/10.35295/osls.iisl/0000-0000-0000-1304.

Pratito, Arief Afdala. 'The Validity of Electronic Evidence in Indonesian Criminal Procedure'. *Ratio Legis Journal* 2, no. 2 (2023): 744. http://dx.doi.org/10.30659/rlj.2.2.%25p.

Prayudi, Yudi, Ahmad Ashari, and Tri K Priyambodo. 'A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia'. *I. J. Computer Network and Information Security* 11 (2015): 1–8.

Pribadi, Insan. 'Legalitas Alat Bukti Elektronik Dalam Sistem Peradilan Pidana'. *Jurnal Lex Renaissance* 3, no. 1 (2018): 109–24. https://doi.org/10.20885/JLR.vol3.iss1.art4.

Purwoleksono, Didik Endro, Brahma Astagiri, and Agus Ristianto. *Kedudukan Alat Bukti Elektronik Berdasarkan Perundang-Undangan Di Indonesia (Electronic Evidence Position Based on the Laws in Indonesia)*. No. 1962032519860. 2014.

European Parliament and Council of the European Union. *Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Proceedings and for the Execution of Custodial Sentences Following Criminal Proceedings*. OJ L 191, July 28, 2023.

Research and Development of Indonesia Prosecutor's Office. 'The Strength of the Value of Electronic Evidence in the Handling of Crime'. 2016.

Safrin, Mohammad and Hasnawati Hasnawati, "Kedudukan Alat Bukti Elektronik dalam Pembuktian Tindak Pidana," *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam* 5, no. 2 (2023). https://doi.org/10.37680/almanhaj.v5i2.2878.

Salmah. 'Ensuring the Admissibility and Credibility of Electronic Evidence in Indonesian Criminal Proceedings'. In *Prevention of Crime and Treatment of Offenders*, edited by Morinaga Taro, vol. 113. The United Nations Asia

and Far East Institute for the Prevention of Crime and the Treatment of Offenders, 2022.

Sampson, Fraser. 'Intelligent Evidence: Using Open Source Intelligence (OSINT) in Criminal Proceedings'. *The Police Journal* 90, no. 1 (2017): 55–69. https://doi.org/10.1177/0032258X16671031.

Setya, Adi, and Abba Suganda. 'Design of Digital Evidence Collection Framework in Social Media Using SNI 27037: 2014'. *JUITA: Jurnal Informatika* 10, no. 1 (2022): 127–38. https://doi.org/10.30595/juita.v10i1.13149.

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah. 'Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment'. *Hasanuddin Law Review* 10, no. 1 (2024). http://dx.doi.org/10.20956/halrev.v10i1.5016.

Sitompul, Josua. *Cyberspace, Cybercrimes, Cyberlaw: Tinjauan Aspek Hukum Pidana*. Tatanusa, 2012.

Stoykova, Radina. 'Encrochat: The Hacker with a Warrant and Fair Trials?' *Forensic Science International: Digital Investigation* 46 (2023). https://doi.org/10.1016/j.fsidi.2023.301602.

Stoykova, Radina, Stig Andersen, Katrin Franke, and Stefan Axelsson. 'Reliability Assessment of Digital Forensic Investigations in the Norwegian Police'. *Forensic Science International: Digital Investigation* 40 (March 2022): 301351. https://doi.org/10.1016/j.fsidi.2022.301351.

Stoykova, Radina, and Katrin Franke. 'Reliability Validation Enabling Framework (RVEF) for Digital Forensics in Criminal Investigations'. *Forensic Science International: Digital Investigation* 45, no. 301554 (2023): 1. https://doi.org/10.1016/j.fsidi.2023.301554.

Stoykova, Radina (Adi). 'A New Right to Procedural Accuracy: A Governance Model for Digital Evidence in Criminal Proceedings'. *Computer Law & Security Review* 55 (November 2024): 106040. https://doi.org/10.1016/j.clsr.2024.106040.

Stoykova, Radina. 'Digital Evidence: Unaddressed Threats to Fairness and the Presumption of Innocence'. *Computer Law & Security Review* 42, no. 105575 (2021): 1–20. https://doi.org/10.1016/j.clsr.2021.105575.

Taekema, Sanne, Bart van Klink, and Wouter de Been. *Facts and Norms in Law: Interdisciplinary Reflections on Legal Method*. Edward Elgar Publishing, 2016. https://doi.org/10.4337/9781785361098.

Twining, William. *Rethinking Evidence: Exploratory Essays*. 2nd edn. Law in Context. Cambridge University Press, 2006. Cambridge Core.

Wall, David S. 'The Internet as a Conduit for Criminal Activity (Revised October 2015)'. In *Information Technology and the Criminal Justice System*, revised, edited by A. Pattavina. Sage, 2005.

White, Elizabeth. 'Closing Cases with Open-Source: Facilitating the Use of User-Generated Open-Source Evidence in International Criminal Investigations through the Creation of a Standing Investigative Mechanism'. *Leiden Journal of International Law* 37, no. 1 (2024): 228–50. https://doi.org/10.1017/S0922156523000444.

Yeboah-Ofori, A., and A. D. Brown. 'Digital Forensics Investigation Jurisprudence: Issues of Admissibility of Digital Evidence'. *Journal of Forensic, Legal & Investigative Sciences* 6, no. 1 (2020): 1–8. https://doi.org/10.24966/flis-733x/100045.

***

Acknowledgment

The authors gratefully acknowledge the financial support provided by BPI (Indonesian Education Scholarship), PPAPT (Centre for Higher Education Funding and Assessment), Ministry of Education, Culture, Research, and Technology, the Republic of Indonesia and LPDP (Indonesia Endowment Fund for Education), Ministry of Finance of the Republic of Indonesia.

Funding Information

This research was conducted with funding support from the PPAPT–LPDP program.

Conflicting Interest Statement

The authors declare that there are no competing financial or non-financial interests that could have influenced the research, authorship, or publication of this article. Although this research received financial support from the PPAPT-LPDP, the funding bodies had no role in the study design, data collection and analysis, interpretation of the findings, decision to publish, or preparation of the manuscript.

Generative AI Statement

None.

Cite this article as: