

Borobudur Law and Society Journal
ISSN: 2809-9664
Vol. 5 No. 4 (2026)
pp: 55-70
DOI: https://doi.org/10.31603/18090

UNIMMA PRESS
UNIVERSITAS MUHAMMADIYAH MAGELANG

The Influence of a Digital Forensic Framework on the Effectiveness of Proving Cybercrime in Indonesia

Fariz Abdullah Zulkarnain[1*], Anita Dewi[1], Muhammad Dava Wijaya[1], Muhammad Auliya Rahman[1], Muhammad Rusdi Daud[1]

[1] Faculty of Law, Universitas Muhammadiyah Jakarta, Jakarta, Indonesia
[*]Corresponding author email: farizabdullah555@gmail.com

Abstract

Cybercrime cases in Indonesia turn on electronic evidence that is easily copied, altered and deleted, yet the rules on how such evidence must be handled are scattered across statutes, police regulations and technical standards. This normative study asks how a digital forensic framework, a staged process of identification, acquisition, preservation, analysis and reporting, influences the effectiveness of proving cybercrime, and what legal and institutional conditions limit that influence in practice. It applies statutory, conceptual and comparative approaches to the Criminal Procedure Code of 2025 (Law No 20 of 2025), the Electronic Information and Transactions Law as amended in 2024, Constitutional Court Decision No 20/PUU-XIV/2016, police regulations and international standards, read against the forensic literature and international standards on evidence handling. The study finds that each stage of a framework answers a specific evidentiary risk: integrity, authenticity, reliability and lawful acquisition. Indonesian law now recognises electronic evidence but prescribes no technical procedure, custody rule or laboratory accreditation, so the effect of a framework depends on investigators' capacity and judges' understanding. The study therefore recommends a national regulation on digital forensics that adopts ISO/IEC 27037, requires chain-of-custody records and laboratory accreditation, and trains investigators, prosecutors and judges.

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

Keywords

Forensics; Cybercrime; Evidence; Custody; Admissibility; Indonesia

Introduction

Cybercrime, understood as crime committed with a computer or other electronic device, mainly over the internet,[1] leaves its traces in logs, messages, files and metadata. In many cases those traces are all the prosecution has: there is no weapon, no eyewitness and no physical scene. Proof therefore depends on whether digital material can be collected without altering it, kept in a way that can be shown to a court, and explained so that a judge can decide how far to rely on it. A study commissioned by the United States National Institute of Justice found that the main difficulties lay in the inexperience of patrol officers and detectives in preserving and collecting digital evidence, the unfamiliarity of court officials with it, and the volume of work facing examiners, and it stressed that recovery and admissibility must be balanced against privacy.[2]

Digital evidence differs from conventional evidence in ways that matter for proof. It is easily duplicated, can be changed without visible trace, may be stored on servers in another country and requires technical skill to read. A digital forensic framework is the response of the discipline to these properties. McKemmish defined forensic computing as the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable,[3] and a framework turns that definition into an ordered set of stages with documentation at each step. Casey adds that every item of digital evidence carries error, uncertainty and the possibility of loss, which the examiner must identify and explain to the court.[4]

The Indonesian legal setting has just changed. Until 2025 the Criminal Procedure Code of 1981 (*Kitab Undang-Undang Hukum Acara Pidana*, KUHAP) contained a closed list of means of proof in its article 184, which did not name electronic evidence,[5] and the status of electronic information came from the Electronic Information and Transactions Law (ITE Law).[6] Law No 20 of 2025 replaced the 1981 Code and has been in force since 2 January 2026, alongside the new Criminal Code (Law No 1 of 2023).[7][8] The new Code lists electronic evidence among the means of proof, but commentators note that its provisions on the subject are few and still lean

[1] Raj Singh Deora & Dhaval Chudasama, "Brief Study of Cybercrime on an Internet" (2021) 11:1 *Journal of Communication Engineering & Systems* 1.

[2] Sean E Goodison, Robert C Davis & Brian A Jackson, *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence* (Santa Monica, Cal: RAND Corporation, 2015).

[3] Rodney McKemmish, *What is Forensic Computing?, Trends & Issues in Crime and Criminal Justice No 118* (Canberra: Australian Institute of Criminology, 1999).

[4] Eoghan Casey, "Error, Uncertainty, and Loss in Digital Evidence" (2002) 1:2 *International Journal of Digital Evidence* 1.

[5] Law No 8 of 1981 on the Criminal Procedure Code (Indonesia), art 184.

[6] Law No 11 of 2008 on Electronic Information and Transactions (Indonesia), as amended by Law No 19 of 2016 and Law No 1 of 2024, arts 5 and 6.

[7] Law No 20 of 2025 on the Criminal Procedure Code (Indonesia).

[8] Law No 1 of 2023 on the Criminal Code (Indonesia).

on the ITE Law.[9] Neither instrument says how electronic evidence is to be acquired, preserved and analysed. That question is left to police regulations and to the practice of individual units.

Earlier research has approached the subject from several directions. Hakim and Alamsyah proposed a digital forensic framework that adds open-source intelligence to the analysis stage in order to deal with anti-forensic techniques on mobile devices.[10] Arshad, Jantan and Abiodun reviewed the problems of validating digital evidence scientifically, in particular for cloud computing, social media and the internet of things.[11] Prayudi and Azhari reviewed the digital chain of custody and the complications caused by the characteristics of digital evidence.[12] Matijašević, Bingulac and Marinković examined the collection and processing of digital evidence and the conditions for its admissibility before a criminal court.[13] These studies are technical, comparative or concerned with other legal systems. None examines, for Indonesia, how each stage of a framework relates to the legal requirements for proof, and none can take account of Law No 20 of 2025, which is the first Indonesian procedural code to list electronic evidence as a means of proof.

This article fills that gap. It asks: (1) what stages and principles make up a digital forensic framework, and how do they protect the integrity of digital evidence; (2) how does Indonesian law, as it stands after 2 January 2026, treat electronic evidence and its handling; (3) how does the use of a framework influence the accuracy and effectiveness of proving cybercrime; and (4) what regulatory and institutional obstacles limit that influence? Its purpose is to show where the law already supports forensic practice, where it leaves gaps, and what a national regulation on digital forensics should contain.

Research Method

This is normative (doctrinal) legal research. It uses a statutory approach to the legal rules on electronic evidence, a conceptual approach to the notions of integrity, authenticity, reliability and lawful acquisition, and a comparative approach limited

---

[9] "Kritik dan Tantangan Pembuktian Alat Bukti Elektronik di KUHAP Baru", *Hukumonline*, online: <https://www.hukumonline.com/berita/a/kritik-dan-tantangan-pembuktian-alat-bukti-elektronik-di-kuhap-baru-lt69a1432790a2b>.

[10] Muhamad Faishol Hakim & Alamsyah, "Development of Digital Forensic Framework for Anti-Forensic and Profiling Using Open Source Intelligence in Cyber Crime Investigation" (2024) 2:2 *Recursive Journal of Informatics*, DOI: <10.15294/7ytx8194>.

[11] Humaira Arshad, Aman Jantan & Oludare Isaac Abiodun, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence" (2018) 14:2 *Journal of Information Processing Systems* 346, DOI: <10.3745/JIPS.03.0095>.

[12] Yudi Prayudi & Azhari SN, "Digital Chain of Custody: State of the Art" (2015) 114:5 *International Journal of Computer Applications* 1, DOI: <10.5120/19971-1856>.

[13] J Matijašević, N Bingulac & D Marinković, "Digital Evidence in Criminal Proceedings – Challenges and Solutions" (2024) 41:4 *Pravna teorija i praksa* 18, DOI: <10.5937/ptp2404018m>.

to two international instruments: the Convention on Cybercrime (the Budapest Convention) and the standard ISO/IEC 27037:2012 on handling digital evidence. The primary legal materials are Law No 20 of 2025 and the Code it replaced, Law No 1 of 2023, the ITE Law as amended by Law No 19 of 2016 and Law No 1 of 2024, Government Regulation No 71 of 2019, Law No 27 of 2022 on Personal Data Protection, the Corruption Law, Chief of Police Regulation No 10 of 2010 and Constitutional Court Decision No 20/PUU-XIV/2016. The secondary materials are books, reports, journal articles and professional commentary on digital forensics and digital evidence; only works whose bibliographic details could be verified are cited.

The analysis proceeds in two directions. Deductively, the stages and principles of a forensic framework are set against the requirements that the law places on evidence, to identify for each stage the evidentiary risk it addresses and the legal rule that applies. Inductively, the accounts of practice in the literature are used to assess how far the law and the framework work together in Indonesia. The article reports no interviews and does not analyse court files. Statements on the shortage of experts and laboratories therefore rest on the literature and are presented as assessments that require confirmation by official data. For the same reason, 'effectiveness' is assessed by legal criteria (whether the evidence can be shown to be intact, authentic, reliable, lawfully obtained and open to challenge), not measured statistically.

Results and Discussion

The Digital Forensic Framework: Stages and Principles

The Digital Forensic Research Workshop of 2001 described a generic investigation process of identification, preservation, collection, examination, analysis, presentation and decision.[14] Later models have added or merged stages, and no single model has become the accepted guide for all cases. Researchers continue to adapt frameworks to new problems, such as the anti-forensic techniques that suspects use to hide or destroy data on mobile devices.[15] For legal analysis, however, what matters is not the number of stages but the function each one serves. This article uses five: identification, acquisition, preservation, analysis and reporting. Table 1 relates each stage to the evidentiary risk that it controls and to the legal rule that makes the risk relevant in Indonesia.

[14] Gary Palmer, *A Road Map for Digital Forensic Research, Technical Report DTR-T001-01* (Utica, NY: Digital Forensic Research Workshop, 2001).
[15] Hakim & Alamsyah, *supra* note 10.

Table 1. Stages of a digital forensic framework and their evidentiary function

Stage	What the framework requires	Evidentiary risk if omitted	Legal anchor in Indonesia
Identification	Locate and document devices, accounts and data sources within the authorised scope; record volatile data	Seizure beyond the warrant; loss of volatile data; intrusion into the data of third parties	Law No 20 of 2025 (search of electronic information with court permission); Law No 27 of 2022
Acquisition	Forensic imaging with write protection; hash value taken at acquisition	Alteration of the original; successful challenge to authenticity	ITE Law, arts 5–6; Decision No 20/PUU-XIV/2016; ISO/IEC 27037
Preservation	Secure storage; hash verification; chain-of-custody record for every transfer	Break in custody; contamination; doubt about identity of the exhibit	Law No 20 of 2025, art 235 (authentic, lawfully obtained); Chief of Police Regulation No 10 of 2010
Analysis	Validated tools and repeatable methods; examiner records error and uncertainty	Unreliable results; unexplained margin of error	Expert statement as a means of proof (Law No 20 of 2025, art 235(1)); ISO/IEC 27037
Reporting	Clear report and testimony that a judge can assess and the defence can test	Evidence discounted because the court cannot evaluate it	Judge's assessment of means of proof under Law No 20 of 2025

Source: compiled by the authors from the sources cited in this section.

The common principle behind the stages is forensic soundness: the original data must not be altered, every action must be documented, and a third party must be able to repeat the process and reach the same result. ISO/IEC 27037 expresses the same idea as three requirements for digital evidence: relevance, reliability and sufficiency. It sets guidelines for identification, collection, acquisition and preservation of potential digital evidence, and it distinguishes the first responder who handles the evidence at the scene from the specialist who analyses it.[16] The standard is not law, but it supplies the technical content that Indonesian law lacks, and a court that has to decide whether evidence is reliable can use it as a measure.

Two points follow from the table. First, the stages are not equally visible to the law. Acquisition and reporting meet legal rules directly, since the way data is seized is governed by search and seizure provisions and the report is presented as expert evidence. Preservation and analysis are less visible: the law says almost nothing about hashing, imaging or tool validation, and these are exactly the steps that determine whether the evidence is reliable. Second, a framework is cumulative. A flaw at identification (for example, copying data beyond the scope of the warrant) cannot be cured by careful analysis, and a break in preservation cannot be cured by a persuasive report.

Chain of Custody as the Core Safeguard of Integrity

Among the stages, preservation and its documentation, the chain of custody, deserve separate treatment because they carry the most weight in court. A chain of custody is the chronological record of who found, acquired, transferred, analysed

[16] *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*, ISO/IEC 27037:2012 (Geneva: ISO, 2012).

and stored the evidence from discovery until it is produced in court. Prayudi and Azhari describe it as an attempt to preserve the integrity of digital evidence and note that the characteristics of digital evidence, above all that it can be copied and reached remotely, complicate the task.[17] Technical tools respond to these characteristics. A hash value acts as a digital fingerprint that shows whether a file or image has changed; forensic image formats such as EWF and AFF4 store the acquired data with its metadata; and evidence containers keep the collected items together with the record of their handling. The record is both a technical and a legal document, because it is what allows the prosecution to show that the item produced in court is the item that was seized.

Under the new Code the custody record has acquired more importance. Commentary on Law No 20 of 2025 reports that the Code requires evidence to be authentic and lawfully obtained under article 235, and that a judge who finds it inauthentic or unlawfully obtained may not use it.[18] The same commentary advises defence and bench alike to examine the scope of the search permit, the integrity of the seized media, the imaging method and the chain of custody.[19] Authenticity of electronic evidence is thus no longer only a matter of the ITE Law, which requires that electronic information be accessible, displayable, assured of integrity and accountable.[20] It is now also a condition for evidence to be usable at all, and the custody record is the main way of proving it.

Indonesian regulation of this step is thin. Chief of Police Regulation No 10 of 2010, as amended in 2014, governs the management of evidence within the police in general terms.[21] On the authors' reading it does not prescribe procedures specific to digital evidence, such as imaging, hashing, the labelling of media or the recording of transfers between examiners; this reading should be checked against the current text and against any later police regulation. Without such procedures each unit follows its own practice, and the court has no common standard against which to judge a custody record. The Arshad review adds a further difficulty: data held in cloud services, social media and connected devices is not in one physical place, so

[17] Prayudi & Azhari, *supra* note 12.

[18] "Doktrin Buah dari Pohon Beracun di KUHAP 2025: Eksklusi Bukti dan Tantangan Pembuktian Digital", *Dandapala*, online: <https://dandapala.com/article/detail/doktrin-buah-dari-pohon-beracun-di-kuhap-2025-eksklusi-bukti-tantangan-pembuktian-digital>.

[19] *Ibid*.

[20] ITE Law, *supra* note 6, art 6.

[21] Chief of Police Regulation No 10 of 2010 on Procedures for Managing Evidence within the Indonesian National Police, as amended by Regulation No 8 of 2014.

the chain of custody has to cover data obtained from providers, not only from seized devices.[22]

Electronic Evidence under Indonesian Law after 2 January 2026

Before 2026, electronic evidence entered Indonesian criminal procedure by an indirect route. Article 184 of the 1981 Code listed witness statements, expert statements, documents, indications and the statement of the accused. The ITE Law then provided that electronic information, electronic documents and their printouts are valid legal evidence and extend the means of proof recognised by procedural law,[23] subject to conditions on the electronic system that produced them. Government Regulation No 71 of 2019 elaborates the duties of electronic system operators.[24] The Constitutional Court limited this route in Decision No 20/PUU-XIV/2016. It held the phrase 'electronic information and/or electronic documents' in articles 5(1), 5(2) and 44 of the ITE Law conditionally constitutional: such material is valid evidence only if it was obtained for law enforcement at the request of the police, the prosecution or another body authorised by law.[25] The decision matters for forensics because it ties the evidential value of electronic material to the way, and the authority under which, it was acquired.

Law No 20 of 2025 moves the rule into the procedural code. Article 235(1) lists electronic evidence among the means of proof, together with witness statements, expert statements, documents, the statement of the accused, physical evidence and the judge's own observation, and article 242 describes it as covering electronic information, electronic documents and electronic systems related to the offence.[26] Article 1 defines electronic information and electronic documents, in terms that differ slightly from those of the ITE Law, and the Code does not define the electronic system.[27] The Code also provides that a court may review the lawfulness of search and seizure in pretrial proceedings and that evidence obtained through an invalid measure cannot be used, and that a search of electronic information requires the prior permission of the head of the district court.[28] Taken together, these provisions give the framework an anchor it lacked: lawful acquisition, authenticity and judicial control of intrusive measures are now legal requirements, and they correspond to the identification, acquisition and preservation stages of Table 1.

---

[22] Arshad, Jantan & Abiodun, *supra* note 11.
[23] ITE Law, *supra* note 6, art 5.
[24] Government Regulation No 71 of 2019 on the Implementation of Electronic Systems and Transactions (Indonesia).
[25] Constitutional Court of the Republic of Indonesia, Decision No 20/PUU-XIV/2016 (7 September 2016).
[26] Law No 20 of 2025, *supra* note 7, arts 235(1) and 242.
[27] "Kritik dan Tantangan Pembuktian Alat Bukti Elektronik di KUHAP Baru", *supra* note 9.
[28] "Doktrin Buah dari Pohon Beracun di KUHAP 2025: Eksklusi Bukti dan Tantangan Pembuktian Digital", *supra* note 18.

What the Code does not do is equally important. It does not say how electronic data is to be imaged or hashed, who may perform the examination, what qualifications an expert needs, how tools are validated, or how custody is recorded. For these matters the authorities still rely on police regulation and internal practice, and on the ITE Law, whose article 35 punishes the manipulation or creation of electronic information so that it appears authentic.[29] That offence shows the other side of the problem: a forged electronic document can be detected only by examining metadata and hash values, which is forensic work that the law neither requires nor regulates. The Personal Data Protection Law adds a further layer, since seizing a phone or server exposes the data of third parties.[30] How the exceptions for law enforcement in that Law interact with the search of devices under the new Code needs separate study; this article only notes that a framework which limits acquisition to the data within the permit also serves privacy. Finally, the substantive offences of cybercrime are found in the ITE Law and the new Criminal Code; their relationship is outside the scope of this article.

How the Framework Influences the Accuracy and Effectiveness of Proof

The influence of a framework on proof can be analysed through five mechanisms. The first is integrity. Digital data is fragile, and any interaction of an investigator with a device can change its content. A framework that requires write-protected acquisition, verification by hash and work on copies reduces the chance that the defence can credibly allege alteration, and so removes a ground on which evidence is commonly contested. The effect is on the prosecution's ability to meet the burden of showing authenticity that article 235 and the ITE Law impose.

The second mechanism is reliability. Many forensic tools have not been tested empirically for accuracy, and the literature identifies the lack of scientific validation as a central weakness of digital evidence, particularly when the data comes from cloud services, social media or connected devices.[31] A framework that requires validated tools and repeatable methods lets the court ask whether a result comes from the activity of the person concerned or from a fault in the tool, and lets another expert re-test it. This makes the process of finding the truth transparent and open to challenge, which is a condition of fairness to the accused as much as an advantage for the prosecution.

[29] ITE Law, *supra* note 6, art 35.
[30] Law No 27 of 2022 on Personal Data Protection (Indonesia).
[31] Arshad, Jantan & Abiodun, *supra* note 11.

The third mechanism is the treatment of uncertainty. Casey argued that digital evidence always contains error, uncertainty and possible loss, whether in the time stamps, the origin of the data or the possibility that logs have been tampered with, and that the examiner must state these limits so that the court can weigh the evidence.[32] An expert who cannot explain the margin of error of a tool or the limits of a conclusion weakens the evidence before the judge, because reliability is a precondition of its acceptance. Accuracy in this sense is not a technical figure but the investigator's ability to minimise and disclose uncertainty at each stage. The claim that a framework makes evidence 'incontrovertible' should therefore be rejected: a framework does not remove uncertainty, it makes it visible and manageable.

The fourth mechanism is lawful acquisition. Because the Court in Decision No 20/PUU-XIV/2016 and the new Code both make the value of evidence depend on how it was obtained, the identification and acquisition stages have a direct legal effect: a search that exceeds the permit or a seizure of devices without authority can make technically perfect evidence unusable. A framework that begins with a written scope for each operation, and records each access to a device or account, helps to show that the evidence was lawfully obtained and to separate it from data that was not covered.

The fifth mechanism concerns attempts to defeat the proof. Suspects may delete messages, damage hardware or obscure their digital activity, and such acts may themselves constitute obstruction of justice under the Corruption Law where the proceedings concern corruption.[33] Forensic procedures give investigators the means to recover deleted data, to detect fabrication and to show when and how data was removed. Work on anti-forensics shows that frameworks must be adapted continually, for example by adding open-source intelligence to analysis when a device yields too little.[34] In this respect the framework protects the proceedings as well as the evidence: a perpetrator cannot avoid liability simply by erasing digital traces if the traces can be recovered by a sound process.

These five mechanisms support the authors' central proposition, but with a qualification. A framework does not make evidence admissible, and Indonesian law does not prescribe it as a condition of admissibility. Its influence is indirect: it reduces the grounds on which evidence can be successfully challenged, and it gives

[32] Casey, *supra* note 4.
[33] Law No 31 of 1999 on the Eradication of Corruption (Indonesia), as amended by Law No 20 of 2001.
[34] Hakim & Alamsyah, *supra* note 10.

the judge the information needed to assess reliability. That influence is also conditional on the knowledge of those who apply it. In the study of the United States justice system the needs ranked highest were education for judges and prosecutors and training for officers in collection and preservation.[35] The same applies in Indonesia. Where the judge does not understand the characteristics of electronic evidence, it risks being treated as less convincing than conventional evidence, although in cybercrime cases it is often the only evidence available. Training, certification and the inclusion of digital forensics in legal education are therefore part of the framework's effect on proof, not an addition to it.

Applying the Framework: An Illustration and a Checklist for Courts

A hypothetical example shows how the stages work together. Suppose an offence of online fraud is investigated and the prosecution relies on messages stored on the suspect's mobile phone and on records obtained from a messaging provider. At identification the investigator defines, in writing, the device, the accounts and the period covered, and obtains the court permission that the new Code requires for a search of electronic information.[36] At acquisition a forensic image of the phone is taken through a write-protected process and its hash value is recorded, and the provider's records are requested through a documented request. At preservation the image is stored in a controlled location, its hash is re-verified before each examination, and each person who handles it signs the custody record. At analysis a validated tool extracts the messages, the examiner notes which parts of the record are incomplete, for example because messages were deleted, and the report states the limits of what can be concluded. At reporting the examiner explains the process to the court in terms a judge can follow. If the defence alleges that the messages were fabricated, the prosecution can answer with the hash records and the custody log, and the court can test the answer. If any stage is missing, the defence has a specific point of attack, and the court a specific reason to doubt.

The same logic can be turned into questions that a judge or a pretrial court can put to any digital evidence. Was the search or seizure authorised, and did it stay within the authority? Was the original protected from change, and is there a hash value or equivalent record showing that the produced item matches what was acquired? Who handled the evidence between acquisition and trial, and is each transfer recorded? Were the tools and methods validated, and are they described so that another expert could repeat the work? Does the report state the margin of error and

[35] Goodison, Davis & Jackson, *supra* note 2.
[36] "Doktrin Buah dari Pohon Beracun di KUHAP 2025: Eksklusi Bukti dan Tantangan Pembuktian Digital", *supra* note 18.

the limits of its conclusions? Does the examiner have the competence to give an expert statement on the matter? These questions follow from the framework of Table 1, from the requirements of authenticity and lawful acquisition in the Code and the ITE Law, and from the standard of ISO/IEC 27037. They do not add a requirement to Indonesian law; they make the existing requirements usable in practice.[37]

The case for placing such questions in a binding national regulation, and not leaving them to the discretion of units, rests on three reasons. The first is legal certainty: suspects, investigators and judges should know in advance what a proper handling of electronic evidence looks like. The second is equality between the parties: if the standard is unwritten, the party with access to technical expertise has the advantage, and in practice that is usually the investigating authority, whose handling is rarely tested by a defence that lacks an expert of its own. The third is the consistency of decisions: when courts use different tests for the same kind of evidence, similar cases end differently. A written standard serves all three, and it protects investigators who follow it from later accusations of misconduct.

Regulatory and Institutional Obstacles

Three obstacles limit the influence of frameworks in Indonesia. The first is the fragmentation of regulation. The Code recognises electronic evidence and the ITE Law sets conditions for electronic systems, but technical procedures are left to the police regulation on evidence management and to unit practice. The result is that there is no national standard against which a court can judge the handling of a particular item. The Code replaced the 1981 statute without filling this gap, and commentators have already described its treatment of electronic evidence as minimal.[38]

The second obstacle is capacity. The literature on digital forensics in Indonesia, and the international studies cited above, point to the same problems: too few qualified examiners, uneven laboratory infrastructure and limited knowledge of electronic evidence among prosecutors and judges. This article could not verify national figures for examiners or for laboratories with accreditation to ISO/IEC 17025, and the statements here are therefore assessments. Collecting those figures from the police, the prosecution service and the accreditation body is a precondition for any serious reform and a subject for further research.

---

[37] ISO/IEC 27037:2012, *supra* note 16.

[38] "Kritik dan Tantangan Pembuktian Alat Bukti Elektronik di KUHAP Baru", *supra* note 9.

The third obstacle is the absence of an institution responsible for the quality of the forensic process. Laboratories within the police examine evidence for the police, and there is no independent body that audits their methods against a standard. An independent accreditation and audit mechanism, in which the police, the prosecution service, the courts and the universities take part, would make the standards enforceable in practice and not only on paper, and would increase public confidence in the integrity of digital evidence.

Harmonisation with International Standards

Cybercrime crosses borders, and so does its evidence: servers, service providers and suspects are often in different countries. Two instruments are relevant. The first is ISO/IEC 27037, discussed above, which gives a common technical language for evidence handling.[39] Adopting it, or a national standard derived from it, would give Indonesian courts and foreign partners the same benchmark for reliability. The second is the Convention on Cybercrime, which requires its parties to provide for the expedited preservation of stored computer data, for the search and seizure of stored data, and for mutual assistance in obtaining it.[40] To the authors' knowledge Indonesia is not a party to the Convention, and the current position should be checked with the treaty office of the Council of Europe. Whether or not it accedes, the Convention is a useful reference for drafting rules on preservation orders and data requests to providers, which the Code covers only in general terms. A United Nations convention against cybercrime was also concluded in 2024 and opened for signature in 2025; Indonesia's position on it should be confirmed before the regulation recommended below is drafted.

Comparison with Earlier Research

Table 2 compares this article with the studies discussed in the Introduction. Hakim and Alamsyah propose a framework for a technical problem and do not ask how it fits the law;[41] this article takes the framework as given and tests it against the legal requirements. The review by Arshad and colleagues identifies validation as the central weakness of digital evidence;[42] the present analysis agrees, and adds that Indonesian law has no rule on validation at all. Prayudi and Azhari treat the chain of custody as a technical problem;[43] this article shows that after Law No 20 of 2025 it is also the main means of proving that evidence is authentic and lawfully

[39] ISO/IEC 27037:2012, *supra* note 16.
[40] Convention on Cybercrime, 23 November 2001, Eur TS 185 (entered into force 1 July 2004).
[41] Hakim & Alamsyah, *supra* note 10.
[42] Arshad, Jantan & Abiodun, *supra* note 11.
[43] Prayudi & Azhari, *supra* note 12.

obtained. Matijašević and colleagues conclude that the admissibility of digital evidence depends on the legal framework and on methodology;[44] the Indonesian findings are consistent with that conclusion, but they show a different pattern, in which the legal framework recognises the evidence while leaving methodology unregulated. Finally, Goodison, Davis and Jackson found that training of officers, prosecutors and judges is the highest need in the United States;[45] the Indonesian position, as far as the literature allows an assessment, is similar.

Table 2. Comparison of this article with earlier research

Study	Focus	Main contribution	What this article adds
Hakim & Alamsyah (2024)	Framework with open-source intelligence against anti-forensics on mobile devices	Adapts the process to a technical problem	Relates the framework to legal requirements for proof
Arshad, Jantan & Abiodun (2018)	Scientific validation of digital evidence	Identifies validation as a central weakness	Shows that Indonesian law has no rule on validation
Prayudi & Azhari (2015)	Digital chain of custody	Reviews custody methods and their difficulties	Links custody to authenticity and lawful acquisition under Law No 20 of 2025
Matijašević, Bingulac & Marinković (2024)	Collection, processing and admissibility in criminal proceedings	Links admissibility to regulation and methodology	Applies the question to Indonesia after 2 January 2026
Goodison, Davis & Jackson (2015)	Needs for digital evidence in the United States	Ranks training and education as top needs	Identifies the same need in Indonesian practice, subject to verification

Source: compiled by the authors from the studies cited.

Conclusion

This article asked how a digital forensic framework influences the effectiveness of proving cybercrime in Indonesia. On the first question, a framework consists of identification, acquisition, preservation, analysis and reporting, governed by the principle of forensic soundness; each stage controls a particular evidentiary risk, and the chain of custody links them. On the second, Law No 20 of 2025, in force since 2 January 2026, lists electronic evidence as a means of proof, requires evidence to be authentic and lawfully obtained and subjects intrusive measures to judicial control, building on the ITE Law and Constitutional Court Decision No 20/PUU-XIV/2016, but no Indonesian instrument prescribes how electronic evidence is to be imaged, hashed, analysed or recorded. On the third, the framework substantially improves the accuracy and effectiveness of proof through integrity, reliability, the disclosure of uncertainty, lawful acquisition and resistance to anti-forensic acts, although it does not by itself make evidence admissible or incontrovertible. On the

[44] Matijašević, Bingulac & Marinković, *supra* note 13.
[45] Goodison, Davis & Jackson, *supra* note 2.

fourth, the influence is limited by fragmented regulation, shortages of expertise and laboratories, and the absence of independent quality control.

Four recommendations follow. First, the government and the police should issue a national regulation on digital forensics that adopts ISO/IEC 27037 or a national equivalent, and that prescribes imaging with write protection, hash verification, documentation of tools and methods, and a standard form of chain-of-custody record. Second, laboratories that examine digital evidence should be accredited and audited periodically by a body independent of the investigating unit. Third, the Supreme Court and the Attorney General should issue guidelines to judges and prosecutors on assessing authenticity, integrity and reliability, supported by training and by digital forensics in legal education. Fourth, the rules on preservation orders and on data held by service providers, including foreign ones, should be aligned with the Convention on Cybercrime and the recent United Nations convention, with safeguards for personal data under Law No 27 of 2022.

The study has limits. It is doctrinal, analyses no court files and conducted no interviews, so the 'influence' of a framework on outcomes is shown analytically and not measured, and its statements on institutional capacity rest on the literature. The provisions of Law No 20 of 2025 were read through secondary commentary and should be checked against the official text. Further research should examine decisions applying the new Code to electronic evidence and collect official data on examiners and laboratories.

Ethics and Data Availability

This normative legal research did not involve human participants or personal data, so ethical approval was not required. All legal materials used are publicly available and no new data were generated.

Use of Generative AI

Generative AI was used only to improve the language of this article (grammar, clarity and style). The authors reviewed the output and are responsible for the content of the article.

Funding and Conflicts of Interest

The authors declare no conflict of interest. This research received no external funding.

References

Convention on Cybercrime, 23 November 2001, Eur TS 185 (entered into force 1 July 2004).

Law No 8 of 1981 on the Criminal Procedure Code (Indonesia).

Law No 31 of 1999 on the Eradication of Corruption (Indonesia), as amended by Law No 20 of 2001.

Law No 11 of 2008 on Electronic Information and Transactions (Indonesia), as amended by Law No 19 of 2016 and Law No 1 of 2024.

Law No 27 of 2022 on Personal Data Protection (Indonesia).

Law No 1 of 2023 on the Criminal Code (Indonesia).

Law No 20 of 2025 on the Criminal Procedure Code (Indonesia).

Government Regulation No 71 of 2019 on the Implementation of Electronic Systems and Transactions (Indonesia).

Chief of Police Regulation No 10 of 2010 on Procedures for Managing Evidence within the Indonesian National Police, as amended by Regulation No 8 of 2014.

Constitutional Court of the Republic of Indonesia, Decision No 20/PUU-XIV/2016 (7 September 2016).

Arshad, Humaira, Aman Jantan & Oludare Isaac Abiodun. "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence" (2018) 14:2 *Journal of Information Processing Systems* 346, DOI: <10.3745/JIPS.03.0095>.

Casey, Eoghan. "Error, Uncertainty, and Loss in Digital Evidence" (2002) 1:2 *International Journal of Digital Evidence* 1.

Deora, Raj Singh & Dhaval Chudasama. "Brief Study of Cybercrime on an Internet" (2021) 11:1 *Journal of Communication Engineering & Systems* 1.

"Doktrin Buah dari Pohon Beracun di KUHAP 2025: Eksklusi Bukti dan Tantangan Pembuktian Digital". *Dandapala*, online: <https://dandapala.com/article/detail/doktrin-buah-dari-pohon-beracun-di-kuhap-2025-eksklusi-bukti-tantangan-pembuktian-digital>.

Goodison, Sean E, Robert C Davis & Brian A Jackson. *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. Santa Monica, Cal: RAND Corporation, 2015.

Hakim, Muhamad Faishol & Alamsyah. "Development of Digital Forensic Framework for Anti-Forensic and Profiling Using Open Source Intelligence in Cyber Crime Investigation" (2024) 2:2 *Recursive Journal of Informatics*, DOI: <10.15294/7ytx8194>.

ISO/IEC 27037:2012. *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva: ISO, 2012.

"Kritik dan Tantangan Pembuktian Alat Bukti Elektronik di KUHAP Baru". *Hukumonline*, online: <https://www.hukumonline.com/berita/a/kritik-dan-tantangan-pembuktian-alat-bukti-elektronik-di-kuhap-baru-lt69a1432790a2b>.

Matijašević, J, N Bingulac & D Marinković. "Digital Evidence in Criminal Proceedings – Challenges and Solutions" (2024) 41:4 *Pravna teorija i praksa* 18, DOI: <10.5937/ptp2404018m>.

McKemmish, Rodney. *What is Forensic Computing?, Trends & Issues in Crime and Criminal Justice No 118*. Canberra: Australian Institute of Criminology, 1999.

Palmer, Gary. *A Road Map for Digital Forensic Research, Technical Report DTR-T001-01*. Utica, NY: Digital Forensic Research Workshop, 2001.

Prayudi, Yudi & Azhari SN. "Digital Chain of Custody: State of the Art" (2015) 114:5 *International Journal of Computer Applications* 1, DOI: <10.5120/19971-1856>.