Journal of International Islamic Law, Human Right and Public Policy
(JISHUP Journal) | ISSN (e): 3031-2280
Website https://jishup.org/index.php/ojs/index | Volume 3 No. 2 (2025)

AUTHENTICATING ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS AT THE JAMBI DISTRICT COURT

Albi Ternando
Universitas Adiwangsa Jambi, Jambi, Indonesia
Email: albyternando@gmail.com

Received: 02/06/2025 | **Revised:** 08/06/2025 | **Accepted:** 25/06/2025 | **Published:** 30/06/2025

Abstract

Electronic evidence can establish communications, transactions, and events that conventional testimony cannot fully reconstruct. Its usefulness nevertheless depends on an adequate foundation connecting the material presented in court with its claimed source and history. This article examines the authentication of electronic evidence in criminal proceedings at the Jambi District Court under the legal framework applicable through 2025. It employs normative legal research using statutory and conceptual approaches, supported by constitutional jurisprudence, forensic guidance, and relevant scholarship. The analysis distinguishes lawful acquisition, authenticity, integrity, attribution, relevance, and evidentiary weight. It argues that neither a matching hash nor possession of a device independently establishes authorship or the truth of its contents. Equally, the absence of a forensic laboratory report does not automatically establish inadmissibility in every case. Authentication should address the actual dispute through a documented and proportionate evidentiary foundation. The article proposes an assessment framework linking acquisition records, preservation, examination, courtroom presentation, and judicial reasoning. Its contribution is a locally directed normative framework rather than an empirical assessment of court performance. Reliable adjudication requires transparent handling records, opportunities for challenge, and explicit findings concerning the limits of each digital item.

Keywords: uthentication; Criminal procedure; Digital forensics; Electronic evidence; Jambi District Court.

INTRODUCTION

Electronic evidence is relevant to the reconstruction of criminal events because communication and everyday activity leave records across devices, applications, and remote systems. A message may clarify an instruction, a transaction record may show the movement of funds, and a video may document an encounter. However, the appearance of information on a screen does not establish how it originated or whether the version presented is complete. The evidentiary task is to connect the material with a reliable account of its source, acquisition, preservation, and relationship to the allegation. Authentication supplies part of that foundation without independently resolving every issue of admissibility or guilt.

The Indonesian framework recognises electronic information, electronic documents, and their printouts through Article 5 of the Electronic Information and Transactions Law. For a study situated in 2025, that framework must include the amendments introduced by Law No. 1 of 2024, rather than reproduce the earlier formulation without qualification. Article 5(4), as amended, preserves circumstances otherwise regulated by statute, while the explanation of Article 5 distinguishes interception-related material. Legal recognition therefore provides a starting point for assessment, not an instruction to accept every digital item without examination (Republic of Indonesia, 2008, 2016, 2024).

Criminal proceedings during 2025 also require temporal precision. Law No. 8 of 1981 remained the operative general criminal procedure framework during that year. Although Law No. 20 of 2025 was promulgated in December 2025, its commencement date was 2 January 2026. This article consequently does not apply the new code's evidentiary provisions retrospectively to hearings conducted in 2025. The distinction matters because a statutory provision adopted during a research year is not necessarily already effective. Authentication must be assessed against

the law governing the relevant proceeding, together with applicable special legislation and constitutional interpretation (Republic of Indonesia, 1981, 2025).

The Jambi District Court provides a relevant institutional setting for examining these questions. Vanessa and Firmansyah (2025) discuss Decision No. 175/Pid.Sus/2024/PN Jmb and raise questions about electronic material accepted without a digital forensic examination. Their publication supplies a local scholarly reference, rather than an independent empirical finding of the present research. It does not establish that the court generally accepts unauthenticated evidence. Its relevance lies in the question of how a court should explain the foundation supporting a digital exhibit when laboratory examination has not been undertaken.

The principal difficulty is conceptual fragmentation. Authenticity may be confused with lawful acquisition, integrity with authorship, and technical readability with the truth of a recorded statement. A file can remain unchanged after collection while containing false information from the outset. A device may belong to a defendant while being accessible to other users. A genuine message may also be irrelevant to the charged conduct. Each example demonstrates why a single technical observation cannot answer all evidentiary questions. The court needs an explanation of what each item establishes, which inference remains disputed, and what additional foundation is required.

This article addresses three related questions: which legal requirements govern authentication in the 2025 framework; how forensic methods and supporting testimony can establish a defensible foundation; and how judges can explain the consequences of incomplete or disputed authentication. Its contribution is an integrated framework for institutional application at the Jambi District Court. The framework connects the handling of digital material with the reasons given for accepting and relying on it. It does not measure local compliance or replace examination of the complete record in any individual prosecution.

LITERATURE REVIEW

Authentication and the Scope of Forensic Conclusions

Supardi (2021) examines electronic evidence in corruption proceedings and identifies data integrity, competent examination, continuity of custody, and compliance with legal requirements as important safeguards. These observations are useful beyond the immediate discussion, provided the special evidentiary rules of corruption cases are not automatically extended to every criminal offence. The study supports a distinction between possessing digital material and demonstrating a reliable foundation for its use. The present article develops that distinction through a broader criminal procedure analysis, while retaining the need to identify the statutory framework applicable to the offence charged.

Kent et al. (2006) describe collection, examination, analysis, and reporting within a forensic process. Their guidance is written primarily for information technology incident response, rather than as a binding criminal evidence rule. Its value here is methodological: it helps distinguish the recovery of information from the interpretation subsequently attached to it. An examiner may extract a message database accurately, yet still need separate evidence to identify the person who authored a particular entry. The report should therefore explain both the method used and the limits of the conclusion, instead of treating successful extraction as proof of the entire prosecution narrative.

Preservation and Continuity of Handling

Guttman et al. (2022) address preservation as a distinct problem in digital evidence management. Their guidance explains why source documentation, protected storage, transfer records, and integrity checks matter throughout the life of an exhibit. These safeguards help establish whether the item examined and the item presented are connected by a reliable history. They do not transform an evidentiary handling record into proof that every statement in the file is true. Preservation supports confidence in the object, while the object's meaning remains a question requiring contextual and legal assessment.

Hashing illustrates both the usefulness and the limits of technical verification. Comparison of suitable cryptographic hash values can support the proposition that two defined byte sequences match. However, the comparison says nothing by itself about who created the original sequence, whether its contents were truthful, or whether the first acquisition was lawful. A hash generated after collection also cannot retrospectively demonstrate that no alteration occurred before it was calculated. These limitations call for integrity verification to be connected with documented provenance and independent evidence where authorship or factual accuracy is disputed.

Local Scholarship and Differentiated Assessment

Vanessa and Firmansyah (2025) compare the treatment of electronic evidence in a Jambi case and a case from another court. Their study raises questions about differences in forensic examination and judicial assessment. The present article develops a separate normative argument: the adequacy of authentication should be evaluated against

the disputed proposition and the applicable law. The existence of a laboratory report is relevant, but its title alone cannot establish that the examination resolved the issue before the court.

The research gap concerns the relationship between these separate inquiries. A technically oriented account may emphasise preservation while giving less attention to lawful acquisition or defence participation. A purely doctrinal account may recognise electronic evidence without explaining how source identity, copies, and presentation formats affect reliability. This article connects those concerns through an approach directed at the particular proposition being proved. The authentication required should correspond to what a party asks the court to infer, without imposing an unsupported requirement that every electronic exhibit undergo the same laboratory procedure.

METHOD

This article uses normative legal research through statutory and conceptual approaches. The legal cutoff is 31 December 2025. Primary materials comprise Law No. 8 of 1981, the Electronic Information and Transactions Law and its amendments through Law No. 1 of 2024, Law No. 48 of 2009, Constitutional Court Decision No. 20/PUU-XIV/2016, and Law No. 20 of 2025 in relation to its commencement date. These materials are read systematically to distinguish recognition of electronic evidence from the conditions and reasoning required for its use in a criminal judgment.

Secondary materials include academic studies and technical publications addressing authentication, preservation, and forensic examination. The National Institute of Standards and Technology publications are used as technical references, not as Indonesian legislation or mandatory domestic standards. The Jambi-related study is used as an expressly attributed discussion of a local judgment. This research does not present that study's description as an independent examination of the original trial record. No interviews, unpublished forensic files, or observational data are used, and no statistical inference is drawn about the court's performance.

The analysis follows four steps. First, it identifies the operative legal framework and the status of the digital material. Second, it separates the factual propositions of source identity, integrity, attribution, and relevance. Third, it examines which forms of supporting material can address each proposition and what their limits are. Fourth, it develops a framework for courtroom assessment and judicial explanation. The resulting findings are normative propositions for application at the Jambi District Court, rather than empirical findings that any particular procedure has or has not been followed there.

RESULTS AND DISCUSSION

Legal Recognition and the Authentication Inquiry

Article 5 recognises electronic information, electronic documents, and their printouts, while Article 6 links relevant evidentiary recognition to accessibility, display, integrity, and accountability. These provisions should be interpreted together with the requirements concerning electronic systems and the procedural law applicable to the case. A printout is therefore not excluded merely because it is printed, but its relationship to the underlying data may require explanation. Conversely, producing a device in court does not automatically authenticate every file stored on it. The presenting party should identify the exhibit, its source, and the factual proposition for which reliance is sought (Republic of Indonesia, 2008, 2024).

The distinction between a physical object and the information extracted from it is particularly important. A seized telephone can be identified through physical characteristics and seizure records. A conversation exported from that telephone raises additional questions about extraction, completeness, and attribution. The report, screenshot, and printed conversation may each be representations of related information, rather than independent sources corroborating one another. A court should make that relationship visible. Otherwise, several outputs from the same underlying source may create an exaggerated impression of confirmation without supplying an additional evidentiary foundation.

Authentication should consequently be treated as an evidentiary process rather than a label attached to a device. The question is whether sufficient supporting information connects the material presented with what it is claimed to represent. The answer may depend on a combination of testimony, acquisition records, technical examination, and contextual evidence. Identifying this foundation helps the court explain why it accepts the material and what its acceptance means. It also prevents a finding that a file is genuine from being overstated as proof that the defendant committed the charged offence.

OPEN ACCESS

Lawful Acquisition and Authenticity

Constitutional Court Decision No. 20/PUU-XIV/2016 connects the use of electronic evidence with lawful law-enforcement acquisition and addresses the protection of private communications. In the framework applicable in 2025, the explanation of Article 5 as amended in 2024 specifically discusses interception, wiretapping, and recording forming part of interception. This language requires the court to identify how material was created and obtained. Stored communications acquired from a seized device, a business record supplied by its custodian, and an intercepted conversation should not be treated as procedurally identical without examining the applicable authority (Constitutional Court of the Republic of Indonesia, 2016; Republic of Indonesia, 2024).

Authenticity concerns whether the material is what its proponent claims it to be. Acquisition legality concerns whether the method of obtaining it satisfied the applicable law. A technically genuine recording does not cure an unlawful interception, while lawful seizure does not prove that every file recovered is authentic or attributable to the accused. The appropriate response to a challenge depends on which problem is established. The judgment should identify the relevant legal rule and its consequence rather than rely on a blanket proposition that all electronic evidence is admissible or that all privately originating material is inadmissible.

These distinctions also affect how objections should be examined. A challenge to the authority for interception requires a legal response concerning acquisition. An allegation that a conversation was edited requires examination of the file and its history. A denial of authorship raises an attribution question that may remain unresolved even where integrity is established. Addressing each objection according to its substance makes the assessment more precise. It also allows the judgment to explain whether a problem affects admissibility, evidentiary weight, or the ability to draw a particular inference.

Table 1. Distinct inquiries in the assessment of electronic evidence

Inquiry	Principal question	Limit of the finding
Lawful acquisition	Was the material obtained under the applicable legal authority?	Does not independently prove its contents accurate
Authenticity	Is the exhibit what the presenting party claims?	Does not establish every factual statement as true
Integrity	Is the relevant data unchanged across the stages compared?	Does not identify its author
Attribution	What connects the relevant activity to a person?	Account ownership alone may be insufficient
Relevance	How does the material bear on an issue in the charge?	Genuine information may have limited relevance
Evidentiary weight	How strongly does the item support the proposed inference?	Must be assessed with the complete lawful record

Source: Author's normative synthesis of the statutory framework and technical literature.

Preservation and the History of Digital Material

A defensible handling history begins with a description of the source, its condition, the person receiving it, and the collection method. Subsequent transfers should record the responsible personnel and actions performed. Where the source is a device, preservation measures depend on its technical condition and the risk of change. Where the source is an online service, the relevant record may instead be a documented provider response or a preserved export. The objective is to explain continuity and changes, rather than produce paperwork that fails to identify what happened to the data.

Forensic copying, access controls, documented working copies, and integrity checks can strengthen this explanation. However, a universal requirement to obtain a complete physical image would be inappropriate where the platform permits only a logical extraction or where a live system requires a different justified approach. The examiner should describe the method, its scope, and known limitations. Similarly, not every change in a device's overall state proves alteration of the specific exhibit. The relevant question is whether a change affects the reliability of the information relied upon and whether that issue has been adequately explained (Kent et al., 2006; Guttman et al., 2022).

OPEN ACCESS

An incomplete handling record requires assessment of its significance. A missing administrative entry is not necessarily equivalent to a demonstrated alteration, but it may leave an important interval unexplained. The court should consider whether other reliable material accounts for that interval and whether the uncertainty affects the proposition being proved. This avoids two unsupported extremes: assuming that any documentation gap proves fabrication, or treating continuity records as irrelevant because the exhibit appears readable. The consequences should follow from the nature and seriousness of the identified problem.

Hash Values and Their Evidentiary Limits

An integrity report should identify the object hashed, the algorithm, the time of calculation, and the values being compared. Hashing an exported screenshot and comparing it with a later copy supports a proposition about those files. It does not establish that the screenshot accurately represents the entire original conversation. A hash generated after editing will identify the edited file. The temporal starting point of verification therefore matters. A court should ask what the comparison covers and avoid describing a matching hash as a guarantee that the material has never been manipulated.

A mismatch likewise requires interpretation before a legal conclusion is drawn. Re-encoding a video or exporting data into a different container can change the bytes even where relevant content remains recognisable. The examiner should preserve and distinguish the acquired material, analytical outputs, and presentation copies. A documented transformation may be legitimate for courtroom display, but the relationship with the preserved source must remain demonstrable. This analysis follows from the technical function of hashing; it does not create an exemption from authentication or justify reliance on an unexplained altered file.

The practical implication is that integrity verification must be described at the appropriate level. A report may verify a complete acquisition image, an individual file, or a particular export. Those objects should not be discussed as though they were interchangeable. The court should understand which version was analysed and which version was displayed during the hearing. This level of precision enables the parties to challenge the relevant comparison and prevents a technically valid result from being used to support a broader conclusion than the examination permits.

Attribution Beyond Device Ownership

Authorship is often the decisive dispute in a criminal case. A telephone number, profile name, or account registration may identify a connection with the accused, yet access can be shared, credentials compromised, or messages transmitted by another person. Attribution should therefore examine the circumstances of use at the relevant time. Device access records, linked sessions, surrounding exchanges, witness knowledge, and independently established conduct may assist. Their value depends on the allegation: evidence of account control must be distinguished from evidence that the defendant personally authored a particular message.

The same distinction applies to timestamps and location information. A displayed time may reflect a device setting, server convention, or export configuration. A location record may concern a device rather than establish a person's exact physical presence. Before relying on either, the court should understand how the value was generated and what uncertainty remains. Such explanation is especially important where chronology links the accused to the alleged conduct. A technically accurate record can still support an overstated inference if the judgment does not distinguish the system's recorded event from the human activity attributed to it.

Attribution may be strengthened when several independent circumstances support the same conclusion. A message may refer to information known to the accused, correspond with an independently established action, and originate from an account shown to be under that person's control at the relevant time. Nevertheless, the reasoning should identify those circumstances rather than presume identity from a profile photograph or saved contact name. The issue is not whether another user is theoretically imaginable, but whether the lawful evidence adequately supports the attribution required by the charge.

Screenshots and Audiovisual Files

Screenshots can preserve visible content but may omit messages, metadata, account context, or information outside the captured frame. The court should ask who created the image, when it was captured, and what source was displayed. A participant's testimony may help explain a conversation, while a fuller export or independent records may address a challenge to completeness. The absence of a screenshot's native metadata does not, by itself, establish fabrication. Equally, an image resembling a familiar application is not sufficient proof of authorship, context, or faithful reproduction.

OPEN ACCESS

Audio and video raise related questions about recording conditions, continuity, editing, synchronisation, and the identity of people represented. Specific indications of manipulation may justify specialist analysis. However, every speculative objection does not necessarily require identical laboratory testing, and an automated manipulation detector cannot independently settle authenticity. The examination should address the actual issue and report its limits. A video can be genuine but incomplete, while an edited excerpt may accurately depict a relevant event if its selection and relationship with the source are transparently explained and legally assessed.

Courtroom presentation introduces a further distinction between source material and explanatory output. Enlarged images, subtitles, transcripts, and slowed video may assist comprehension, but they can also introduce interpretation. A transcript, for example, may contain disputed words that are unclear in the recording. The court should identify the underlying exhibit and explain the status of the aid used to present it. Where interpretation is contested, the parties should be able to examine the source rather than be confined to a presentation prepared by one side.

Table 2. Foundations for examining different forms of electronic evidence

Material	Foundation to examine	Main issue requiring explanation
Messaging screenshot	Source identification and capture circumstances	Missing context and attribution
Application export	Extraction method and scope	Whether relevant records were omitted
CCTV recording	System source and export history	Continuity and time settings
Audio or video excerpt	Preserved source and documented transformation	Editing and significance of omitted content
Provider or transaction record	Custodian identification and retrieval process	Meaning of the fields and connection with the accused
Forensic report	Examiner competence and described method	Whether conclusions exceed the method's capabilities

Source: Author's proposed framework informed by Kent et al. (2006) and Guttman et al. (2022).

Forensic Expertise and Judicial Assessment

A laboratory report can offer substantial assistance when authenticity, extraction, or attribution presents a technical dispute. Its value depends on the examiner's competence, the method described, the material examined, and the reasoning connecting observations with conclusions. A report that merely declares a device examined may leave the central issue unresolved. The court should identify whether the expert addressed file integrity, source recovery, identity, or another question. It should then assess that conclusion within its stated scope rather than equate the authority of the laboratory with proof of the charged offence.

There is also no sound basis for assuming that a laboratory report is the sole possible means of authenticating every electronic item under the 2025 framework. Depending on the circumstances, source testimony, system documentation, admissions, or other supporting material may contribute to a sufficient foundation. This does not remove the requirement of legal evidence or the prosecution's burden. It means that the court should explain why the foundation addresses the disputed issue. Where a credible technical challenge remains unresolved, reliance requires careful justification rather than a reference to judicial conviction alone.

An expert's conclusion should remain open to focused examination. Relevant questions include whether the method was suitable, what data was unavailable, whether the result can be reproduced, and which alternative explanations were considered. The expert should distinguish observations from assumptions and identify any uncertainty affecting the finding. These questions support the court's understanding without requiring judges to conduct the forensic examination themselves. Judicial responsibility concerns evaluating the evidence and its legal significance, while technical expertise assists with matters requiring specialised knowledge.

Judicial Reasoning at the Jambi District Court

The local scholarly discussion provides a reason to examine how an authentication foundation is explained, rather than to presume a court-wide defect. The absence of laboratory testing should prompt inquiry into the alternative basis relied upon. A finding that evidence was accepted without a forensic report does not independently

establish that it was false, that no authentication occurred, or that its acceptance necessarily violated the law. Those conclusions require examination of the applicable rules, the objections raised, and the reasons supporting reliance.

A judgment should distinguish the exhibit, its claimed source, the legal basis of acquisition, the foundation for integrity and attribution, and the inference drawn. It should also address material objections and identify limitations affecting weight. This recommendation follows the duty to provide legally grounded reasons under Articles 50 and 53 of Law No. 48 of 2009. Under Articles 183 and 184 of the Criminal Procedure Code operating in 2025, proof must satisfy the prescribed lawful evidentiary foundation and judicial conviction. Reproducing the same digital source in several formats does not dispense with that requirement (Republic of Indonesia, 1981, 2009).

For practical application, each disputed digital exhibit could be accompanied by a concise explanatory record identifying provenance, acquisition authority, preservation, examination, and intended use. This is a proposed organisational aid, not a new statutory document requirement. It would help the prosecution disclose its foundation, the defence formulate a focused challenge, and the court explain its conclusion. Where access to sensitive material is involved, examination can be organised with appropriate protections while preserving meaningful opportunities to test the evidence.

The framework also provides questions for subsequent empirical research. A study of verified Jambi District Court judgments could examine whether courts distinguish authenticity from attribution, explain acquisition legality, and address objections concerning completeness or manipulation. Evidence-handling records would be needed to assess procedures that are not fully described in published judgments. Such research would extend the present analysis while preserving the distinction between a normative recommendation and a demonstrated account of institutional practice.

CONCLUSION

Authentication of electronic evidence requires a foundation connecting the exhibit with its claimed source and handling history. In the framework applicable through 2025, legal recognition under the Electronic Information and Transactions Law operates alongside criminal procedure, constitutional interpretation, and the duty to give reasons. Authenticity, lawful acquisition, integrity, attribution, relevance, and evidentiary weight remain distinct inquiries. Matching hash values support a limited integrity proposition, while device ownership and account labels do not independently establish authorship. Forensic examination can resolve technical disputes, but its necessity and adequacy must be assessed against the issue presented rather than assumed uniformly for every exhibit. At the Jambi District Court, the proposed framework directs attention to documented provenance, transparent examination, defence participation, and explicit judicial findings. The local scholarly discussion supports further inquiry without establishing a court-wide pattern. Empirical evaluation requires verified case records and should remain separate from the normative conclusions advanced here.

REFERENCES

Constitutional Court of the Republic of Indonesia. (2016). *Decision No. 20/PUU-XIV/2016*. Official judgment.

Guttman, B., White, D. R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers* (NIST IR 8387). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8387

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

Republic of Indonesia. (1981). *Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana*. Official legal database.

Republic of Indonesia. (2008). *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*

Republic of Indonesia. (2009). *Undang-Undang Nomor 48 Tahun 2009 tentang Kekuasaan Kehakiman*. Official legal text.

Republic of Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.*

Republic of Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Official legal database.

Republic of Indonesia. (2025). *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*. Official legal database.

OPEN ACCESS

Supardi. (2021). Mengukur kekuatan alat bukti elektronik dalam pembuktian perkara tindak pidana korupsi. *Syntax Literate: Jurnal Ilmiah Indonesia, 6*(5). https://doi.org/10.36418/syntax-literate.v6i5.2724

Vanessa, & Firmansyah, H. (2025). Analysis of the validity of electronic evidence in criminal trial proceedings and the implementation of its admissibility (judgment study). *Indonesian Journal of Law and Economics Review, 20*(4). https://doi.org/10.21070/ijler.v20i4.1395

OPEN ACCESS