Vol. 23 No. 1 June 2027 **YURISDIKSI**
Jurnal Wacana Hukum dan Sains
Universitas Merdeka Surabaya
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

Guidelines For The Authentication of Electronic Evidence In Criminal Proceedings

Muhammad Imron[1*], Faizin Sulistio[1], Alfons Zakaria[1]

[1]Faculty of Law, Brawijaya University Malang, Indonesia

*Corresponding Author Email:[*]imronlwyr@student.ub.ac.id, faizin@ub.ac.id, alfons@ub.ac.id

Article History: Received: September 18, 2026; Accepted: November 22, 2026

ABSTRACT

Electronic information and documents are increasingly relevant to the proof of criminal offences. Although Indonesian legislation recognizes electronic information and electronic documents as admissible legal evidence, practical questions remain concerning how their source, integrity, authenticity, and lawful acquisition should be demonstrated. This study examines the need for operational guidance on the authentication of electronic evidence through statutory, case-based, and comparative legal analysis. It argues that authentication should be assessed through identifiable and proportionate procedures, including source identification, documentation of acquisition, preservation, chain of custody, integrity verification, and disclosure of relevant examination methods. Digital-forensic examination may be necessary where the nature of the evidence or a genuine dispute requires it, but it should not be treated as an automatic requirement for every electronic item. The study proposes that the competent Indonesian authorities develop guidance specifying minimum authentication principles, roles and responsibilities, documentation standards, and safeguards for the rights of the parties. The comparative discussion of the United States and India is used to identify procedural options, not to transplant foreign rules without adaptation to Indonesian criminal procedure.

Keywords Authentication; Electronic Evidence; Criminal Proof; Digital Forensics; Legal Certainty.

1. INTRODUCTION

The development of information and communication technology has brought fundamental changes to the patterns of social interaction, including communication activities, transactions, data storage, and information exchange. Various activities previously conducted through conventional media have now shifted to electronic media, which offers convenience, speed, efficiency, and wider reach. This transformation has simultaneously changed the characteristics of crime. Crimes are no longer always committed through physical meetings between perpetrators and victims, but can be committed through electronic devices and internet networks, leaving traces in the form of digital data. Online fraud, extortion, threats via electronic media, online gambling, electronic document forgery, the distribution of prohibited content, and various other forms of technology-based crimes demonstrate that technological developments have created new spaces for criminal acts to occur. This situation requires the criminal justice system to be able to adapt, particularly in terms of obtaining, securing, examining, and assessing digital information that has the potential to become evidence.

These changes in the characteristics of criminal acts have direct implications for the evidentiary system in criminal procedure. Evidence is a fundamental stage in the criminal justice

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

process, as it provides the judge with a basis for assessing the facts charged against the defendant. In the context of crimes involving information technology, conventional evidence is often unable to describe the entire sequence of criminal events. Communication traces via messaging apps, emails, surveillance camera recordings, electronic transaction data, server logs, access history, metadata, and data stored on mobile phones and computers can be crucial in constructing a criminal event. Therefore, the existence of electronic evidence can no longer be viewed as merely a supplement to evidence, but in certain cases can be a crucial part in revealing the relationship between the perpetrator, the victim, the act, and the resulting consequences.

In Indonesian positive law, the existence of electronic evidence has received normative recognition. Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended several times, most recently by Law Number 1 of 2024, through Article 5 paragraph (1) confirms that Electronic Information, Electronic Documents, and/or printouts thereof constitute valid legal evidence. This provision provides a legal basis for the use of electronic information and documents in the evidentiary process. Regulations regarding Electronic Information and Electronic Documents also provide broad coverage of the forms of digital data that can be objects of evidence, ranging from writing, sound, images, electronic mail, transaction data, to various forms of data produced, sent, received, or stored through electronic systems. Thus, normatively, Indonesian law has given recognition to the existence of electronic evidence in the law enforcement process.

Regulations regarding electronic evidence have also undergone developments in criminal procedural law through Law Number 20 of 2025 concerning the Criminal Procedure Code. These regulations demonstrate an effort to adapt criminal procedural law to technological developments and contemporary evidentiary needs. One important provision is contained in Article 235 paragraph (1) letter f which places electronic evidence as one of the means of evidence, while Article 242 regulates the scope of electronic information, electronic documents, and/or electronic systems related to criminal acts. This recognition essentially provides a stronger foundation for the use of electronic evidence in criminal justice processes. However, recognition of the existence of electronic evidence does not in itself resolve the issue of how such evidence must be declared authentic and trustworthy in court.

This issue is important because the characteristics of electronic evidence are fundamentally different from those of conventional evidence. Electronic data is physically intangible, easily copied, moved, deleted, altered, or manipulated without always leaving any discernible changes. A screenshot, for example, can provide a snapshot of a conversation, but the presence of the image does not in itself indicate the source, time of creation, device used, context of the communication,

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

or whether or not there have been any changes to the original data. Similarly, an email can be used to demonstrate a particular communication, but issues regarding the identity of the sender, the integrity of the message, the existence of metadata, and the possibility of spoofing must be considered in determining its reliability. These characteristics indicate that the main problem with electronic evidence lies not only in its existence but also in the legal ability to ensure its authenticity and integrity.

In this context, authentication is a crucial step in determining whether electronic evidence can be used to support a criminal case. Authentication essentially involves the process of ensuring that the evidence presented truly originates from the source stated, has not undergone unauthorized alteration, and has a verifiable relationship to the event being proven. Therefore, authentication addresses not only the question of whether data can be presented in court, but also how the data was obtained, who obtained it, the equipment used, how it was stored, whether there have been any changes to the data, and the methods used to verify its authenticity. In the examination of electronic evidence, these aspects are closely related to data integrity, chain of custody, acquisition methods, digital forensic examinations, and documentation of each stage of evidence management.

The need for authentication is increasingly relevant with the provisions of Article 235 paragraph (3) of the Criminal Procedure Code, which requires that electronic evidence must be authenticated and obtained through legally valid procedures. This provision shows that lawmakers have paid attention to the issue of authentication as a prerequisite for the use of electronic evidence. However, the norm requiring authentication does not automatically provide operational parameters regarding how such authentication must be carried out. The issues that then arise are regarding what standards must be used to declare electronic evidence as authentic, who is authorized to carry out authentication, what examination methods must be used, and the extent to which digital forensic examination is required for each type of electronic evidence.

The lack of detailed parameters has the potential to create differences in law enforcement practices and court proceedings. Electronic evidence submitted in a case must essentially meet certain requirements, both related to formal and material aspects. Formal aspects can include the legality of acquisition, procedures for seizure or security, documentation of the acquisition process, maintenance of the chain of custody, and the examination methods used. Meanwhile, material aspects relate to the relevance of the evidence to the case, data integrity, source reliability, connection to the criminal event, and the evidence's ability to support the elements of the crime. If these parameters are not clearly formulated, the assessment of the authenticity of electronic evidence has the potential to depend on the approach of each law enforcement officer and judge.

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

This issue can be seen in the differing approaches in judicial practice when assessing electronic evidence. In some cases, electronic evidence may be considered based on its relevance to the case and its relationship to other evidence, while in other cases, forensic laboratory results or expert testimony are used to strengthen the authenticity and integrity of digital evidence. These differences do not necessarily indicate that one approach is always correct or incorrect, as the assessment of evidence remains related to the characteristics of the case and the overall evidence presented. However, these variations demonstrate the need for clearer parameters regarding the authentication of electronic evidence, particularly to prevent the assessment process from relying solely on differing approaches to evidence with similar characteristics.

This urgency can be understood through several cases that demonstrate the issue of authenticating electronic evidence in practice. Decision Number 175/PID.SUS/2024/PN Jmb and the Jessica Wongso case, as discussed in relevant literature and news reports, demonstrate the debate regarding the position and assessment of digital evidence in the evidentiary process. Meanwhile, Decision Number 60/PID.B/2019/PN Drh demonstrates the use of forensic laboratory examination results in assessing evidence related to a case. The different approaches in these cases demonstrate that examining the authenticity of electronic evidence has an important practical dimension in the evidentiary process. Therefore, a study is needed that not only positions electronic evidence as a matter of admissibility but also analyzes the mechanisms to ensure that such evidence is authentic, intact, and legally accountable.

Risks to the authenticity of electronic evidence can also be seen in the possibility of digital data manipulation or falsification. One illustration presented by cybersecurity expert Dr. Harold D'Costa relates to the use of an email that is later discovered not to have been sent by the alleged sender. The message is suspected to have been created through a spoofing method, making it appear as if it originated from a specific email address. This illustration shows that the appearance of electronic data is not necessarily identical to the actual data source. In the context of criminal evidence, this condition is crucial because the acceptance of evidence without an adequate verification process can raise questions about the defendant's rights and the reliability of the judicial process. Therefore, the ability to distinguish between authentic electronic data and manipulated data is an integral part of a technology-based criminal evidence system.

In addition to issues at the trial stage, authentication issues also relate to the entire process of managing electronic evidence from the investigation and inquiry stages. Digital evidence can be altered if the process of retrieval, transfer, storage, or examination is not carried out using appropriate methods. Therefore, authentication should not be understood solely as the judge's action when evidence is presented in court, but rather as a series of processes that begin when

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

electronic evidence is discovered and obtained by law enforcement officials. Documentation regarding the source of evidence, the equipment used, the acquisition method, the hash value, the storage process, transfer, examination, and presentation in court are all elements that can be used to maintain the integrity of evidence. Such an approach is crucial to ensure continuity between the process of obtaining evidence and the process of presenting that evidence in the trial.

Another issue arises because the current regulations regarding the authentication of electronic evidence have not yet fully provided integrated technical guidelines for all law enforcement officials. This need applies not only to judges during the trial examination phase, but also to investigators and prosecutors, who have a role from the initial stages of collecting and managing electronic evidence. Clear guidelines are needed to provide parameters regarding authentication standards, examination procedures, the use of digital forensic methods, the competence of the parties conducting the examination, chain of custody documentation, and the mechanism for presenting examination results in court. With clearer parameters, it is hoped that the authentication process can be implemented more consistently and provide a basis for judges to assess the reliability of electronic evidence presented in criminal cases.

The need for such guidelines can be seen through comparisons with several other legal systems, one of which is the United States' Federal Rules of Evidence. Rule 902(13) and Rule 902(14) recognize self-authentication mechanisms for certain categories of electronic records and data obtained through specific processes, with requirements determined by the rules of evidence. These mechanisms demonstrate an effort to provide more concrete parameters regarding certain circumstances under which electronic evidence can be declared authentic without always having to present an examiner as a witness to prove its authenticity. Meanwhile, the development of electronic evidence law in India also shows attention to certification requirements for electronic evidence, particularly in the context of proving copies of electronic data. This comparison is not intended to directly adopt foreign legal systems, but can be used as material to identify regulatory models that can be developed in accordance with the characteristics of the Indonesian criminal procedure system.

Based on the above description, the main issue in the use of electronic evidence in criminal proceedings is no longer solely about recognizing its status as valid evidence, but rather about how the authenticity of electronic evidence can be verified based on clear, measurable, and consistently applicable legal and technical parameters. Regulations that recognize electronic evidence without adequate authentication guidelines have the potential to lead to differences in assessments of evidence with similar characteristics and create uncertainty regarding the standards that must be met by law enforcement officials and parties in the evidentiary process. Therefore, research is

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

needed that examines the construction of regulations for the authentication of electronic evidence in criminal proceedings, including the relationship between the provisions of the Criminal Procedure Code, the ITE Law, the principles of criminal evidence, and the need for digital forensic examinations. This research is directed at analyzing the need for and formulating guidelines for the authentication of electronic evidence that can provide legal certainty while maintaining the integrity of the criminal evidence process amidst the development of digital technology.

2. RESEARCH METHODS

This research uses a normative legal or juridical normative research method, namely research conducted by reviewing and analyzing legal norms, laws and regulations, court decisions, and legal doctrines relevant to the regulation of electronic evidence authentication guidelines in criminal proceedings. This research uses three approaches: the statute approach, the case approach, and the comparative approach. The statute approach is used to review legal provisions governing the status, validity, and authentication of electronic evidence in Indonesia. The case approach is used to analyze court decisions related to the use and authentication of electronic evidence in criminal proceedings. Meanwhile, the comparative approach is carried out by comparing the regulation of electronic evidence authentication in Indonesia with the legal systems of the United States and India to identify similarities, differences, and the possibility of developing regulations that are in accordance with the Indonesian legal system.

The legal materials used consist of primary, secondary, and tertiary legal materials. Primary legal materials include relevant laws and regulations, including the Criminal Procedure Code, the Electronic Information and Transactions Law, regulations and guidelines issued by law enforcement institutions, and relevant court decisions. Secondary legal materials include law books, national and international scientific journals, academic articles, theses, and other literature relevant to criminal evidence and digital forensics. Tertiary legal materials include legal dictionaries, the Great Indonesian Dictionary, and other reference materials. The collection of legal materials was carried out through library research, documentation, and online legal source searches. Next, the legal materials were analyzed qualitatively using grammatical, systematic, and historical interpretation techniques to examine the meaning and interrelationships of legal norms governing the authentication of electronic evidence, identify gaps or ambiguities in the regulations, and formulate the need for authentication guidelines that can be applied consistently in the process of proving criminal acts.

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

3. RESULTS AND DISCUSSION

The Position of Electronic Evidence Authentication in the Criminal Evidence System

The development of information technology has brought about fundamental changes in the characteristics of evidence in the criminal justice process. This change occurs because human activities are increasingly conducted through electronic devices and systems, so that various events relevant to criminal acts do not always leave physical evidence. Communication via email and messaging applications, transactions through electronic banking systems, social media activity, surveillance camera recordings, location data, and various other forms of digital activity can leave electronic traces that are relevant to proving a crime. This condition requires the criminal evidence system to be able to accommodate evidence characteristics that differ from conventional evidence. Electronic evidence is inherently intangible and can be copied, transferred, reproduced, altered, and even manipulated with varying degrees of difficulty. Therefore, the issue of authentication is an integral part of the discussion regarding the position and strength of electronic evidence in the criminal evidence system.

Normatively, this development has been responded to through the regulation of electronic evidence in Indonesian positive law. Law Number 11 of 2008 concerning Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024, recognizes Electronic Information and/or Electronic Documents and their printouts as valid legal evidence. This provision forms an important basis for the use of digital information in law enforcement processes, including in criminal cases. This recognition demonstrates that Indonesian law has abandoned the evidentiary paradigm that focuses solely on physical evidence. Electronic information and documents can be used to explain a legal event as long as they meet the requirements stipulated by statutory regulations. However, the recognition of electronic evidence as valid evidence must be distinguished from the issue of its authenticity and reliability. In other words, while electronic information may be normatively categorized as valid evidence, it must still be ensured that it is truly authentic and obtained through legally justified procedures.

The strengthening of the position of electronic evidence is then seen in Law Number 20 of 2025 concerning the Criminal Procedure Code. The 2025 Criminal Procedure Code places electronic evidence as one of the means of evidence in the criminal evidence system. Article 235 paragraph (1) letter f of the Criminal Procedure Code includes electronic evidence as one of the means of evidence, while Article 242 regulates the scope of electronic evidence related to criminal acts. These regulations are significant because they place electronic evidence in the construction of criminal procedure law more explicitly. While previously the use of electronic evidence was highly dependent on sectoral regulations, particularly the ITE Law and other special laws, the regulations

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

in the Criminal Procedure Code provide a more systematic basis in criminal procedure law. The existence of these provisions also shows that technological developments have directly influenced the construction of criminal evidence. Thus, criminal procedure law no longer only deals with evidence that can be seen and touched physically, but also with digital data that requires a simultaneous legal and technical approach.

However, the recognition of electronic evidence in the 2025 Criminal Procedure Code does not stop at granting it status as evidence. The legislators also provide requirements regarding authentication. Article 235 paragraph (3) of the Criminal Procedure Code stipulates that the evidence referred to in paragraph (1) must be authenticated and obtained in a lawful manner. This provision indicates that authentication is one aspect that determines the admissibility of evidence in the evidentiary process. Furthermore, Article 235 paragraph (4) gives the judge the authority to assess the authenticity and validity of the evidence presented in court. In fact, Article 235 paragraph (5) determines the consequences for evidence declared inauthentic and/or obtained unlawfully, namely that it cannot be used as evidence in court examinations and has no evidentiary force. Thus, it can be understood that authentication is not merely an administrative matter, but is part of the mechanism for filtering evidence before it is used in the evidentiary process.

In this context, authentication can be understood as the process of ensuring the identity, source, authenticity, and integrity of evidence so that it can be believed that the evidence presented in court is truly the evidence stated by the party submitting it. For electronic evidence, authentication is more complex than for physical evidence because digital data can be altered without always causing directly observable changes. For example, a screenshot of a conversation may show the content of a particular communication, but this does not automatically prove who created or sent the message, when the message was created, whether the content of the conversation is intact, or whether the data has been altered before being presented to the court. Therefore, authentication must be directed at answering a number of fundamental questions regarding the source of the evidence, how the evidence was obtained, the condition of the evidence when it was obtained, the storage process, and the possibility of changes to the data.

Authentication must also be distinguished from the assessment of relevance and evidentiary strength. Relevance concerns the relationship between evidence and the facts or elements of the crime being proven, while authentication concerns the authenticity and identity of the evidence presented. Meanwhile, evidentiary strength concerns the extent to which the evidence can provide a basis for the judge to form a belief regarding the facts being examined. This distinction is important because electronic evidence may be relevant to a case but not necessarily authentic. Conversely, evidence may be declared authentic but may not necessarily prove all

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

elements of the crime charged. Therefore, authentication should be considered as one stage in the evidence assessment process, not the sole parameter for determining whether a crime has been proven.

The issue of authentication is also closely related to the process of acquiring and maintaining the integrity of electronic evidence from the early stages of law enforcement. Electronic evidence is not only assessed once it reaches the courtroom; its quality is largely determined by the process leading up to its discovery or acquisition. In the context of digital forensics, the data acquisition process must be conducted in such a way that changes to the original data are minimized and each stage of evidence management can be documented. This relates to the concept of chain of custody, which is the recording of the possession, transfer, storage, examination, and use of an item or data as evidence. For electronic evidence, the chain of custody is crucial because digital copies can technically be made in unlimited quantities. Without adequate documentation, questions may arise as to whether the data examined by experts or presented in court is the same as the data originally obtained by investigators.

In addition to chain of custody, data integrity is also a crucial aspect of authentication. Integrity relates to the condition that submitted data has not undergone unauthorized changes from the time it is acquired until it is used in the evidence process. In digital forensic examinations, integrity can be verified through various technical methods, one of which is the use of hash values to compare data similarities. The use of these methods demonstrates that the authentication of electronic evidence cannot be completely separated from the technological aspect. The law determines the legal consequences and requirements, while technology and forensic science can provide methods to verify the condition of the data. Therefore, regulations regarding authentication require an approach that integrates legal and technical aspects so that the authentication process is not only based on assumptions regarding data authenticity but can be tested using accountable methods.

The position of authentication in the evidentiary system must also be placed in relation to the authority of the judge. Article 235 paragraph (4) of the Criminal Procedure Code gives the judge the authority to assess the authentication and the validity of the acquisition of evidence. This authority indicates that the judge has a central role in determining whether electronic evidence can be used in the examination of the case. However, this authority does not mean that the judge must carry out the entire technical process of examining electronic data himself. In certain cases, technical aspects may require the assistance of experts who have competence in the field of information technology or digital forensics. Therefore, a mechanism is needed that can help the judge distinguish between legal issues and technical issues in authentication. The judge still carries

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

out a legal assessment of the evidence, while technical aspects can be clarified through expert examination and documentation of the evidence management process.

Based on this construction, it can be argued that the position of authentication in the criminal evidence system is an integral part of the admissibility and assessment of electronic evidence. The 2025 Criminal Procedure Code has provided a normative basis by positioning electronic evidence as evidence and requiring that its authenticity be proven. However, this normative recognition is not yet synonymous with the availability of a comprehensive authentication mechanism. Parameters are still needed that explain how evidence sources are identified, how data is obtained and secured, how data integrity is maintained, when forensic examination is necessary, how the chain of custody is documented, and how authentication results are presented in court. Thus, the issue of the position of authentication is not only related to the legal recognition of electronic evidence, but also relates to the need to ensure that such evidence is of accountable quality in the process of proving criminal acts.

Unclear Authentication Standards and Problems in Assessing Electronic Evidence

Although Indonesian law recognizes electronic evidence and requires authentication, a further issue lies in the lack of comprehensive operational standards for determining when electronic evidence can be declared authentic. Article 235 of the 2025 Criminal Procedure Code stipulates that evidence must be authenticated, but this norm remains general in nature. This provision does not yet provide detailed parameters explaining the authentication stages for various types of electronic evidence. This situation raises questions about the standards that must be met by the party submitting the evidence, the methods that can be used to test its authenticity, and the limits of examination that must be carried out by law enforcement officials and judges. This issue becomes increasingly important because the characteristics of electronic evidence are so diverse that not all types of evidence can be verified using the same methods. Therefore, the existence of norms regarding authentication still requires elaboration in the form of guidelines that can be used practically.

The ambiguity of these standards can be seen in the differing characteristics of each form of electronic evidence. Screenshots of conversations, for example, differ from data obtained directly from a mobile phone, and CCTV recordings differ from electronic banking transaction data or server logs. Screenshots are essentially a reproduction of the data's appearance, while data obtained through forensic acquisition can provide more extensive information about the source and structure of the data. These differences indicate that authentication methods cannot be applied uniformly without considering the characteristics of the source and type of data. Authentication guidelines therefore need to provide classifications, or at least parameters, that can be tailored to

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

the type of electronic evidence being examined. This approach will prevent overly simplistic procedures from being applied to evidence requiring technical examination and, conversely, disproportionate procedures from being applied to evidence that is relatively easy to verify.

Authentication issues can also arise from the method by which electronic evidence is obtained. Digital data can be obtained through device seizure, data extraction, requests to electronic system administrators, downloading from a system, documenting through screenshots, or other legally available mechanisms. Each acquisition method has consequences for the reliability of the resulting evidence. Data obtained directly from the original source has different characteristics than data that has undergone multiple stages of reproduction or conversion. Therefore, in determining the authenticity of evidence, the acquisition method must be examined. Authentication guidelines should outline the minimum procedures that must be followed from the time the evidence is first discovered, including recording the condition of the device, identifying the data source, the acquisition method, and the actions taken on the device or system. Therefore, authentication applies not only to the content of the data but also to the process that produced the data into evidence.

The chain of custody aspect becomes increasingly important when electronic evidence passes from investigators to experts, then to prosecutors, and then to court. Each such transfer must be explained administratively and technically to ensure that the evidence being examined remains the same. This issue differs from physical evidence, as digital copies can be made identically and are not always readily distinguishable from their source. Therefore, clear documentation of who received, who delivered, when the transfer took place, the media used, and how data integrity was verified is crucial to ensuring the reliability of evidence. If this process is not properly documented, parties dealing with the evidence may question the possibility of changes or manipulation during the acquisition process. Therefore, the chain of custody should be one of the parameters explicitly addressed in authentication guidelines.

Another issue relates to the need for digital forensic examination. In practice, not all electronic evidence requires the same level of technical examination. Some evidence may be verifiable through testimony from the party who created or received the data, while other evidence may require examination of the device or system from which it originated. Problems arise when there is no standard defining the circumstances under which evidence requires digital forensic examination. As a result, forensic examinations can be viewed differently in each case. The primary goal of digital forensics in the context of evidence is to provide a scientific method for identifying, acquiring, examining, and analyzing digital data while maintaining its integrity. Therefore, authentication guidelines need to clarify the relationship between forensic examinations

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

and the evidentiary process, including the circumstances under which such examinations are necessary and how the results are used by judges in assessing the authenticity of evidence.

These differences in approach can ultimately impact the consistency of court decisions. In one case, electronic evidence may be assessed based on its relationship to other evidence and the circumstances of the case, while in another case, technical aspects such as forensic laboratory examinations or expert testimony may be of greater importance. These differences in assessment do not automatically indicate an error in the decision, as judges must consider all the facts and evidence available in each case. However, if there are no minimum parameters that can serve as a common reference, there is the potential for variation in determining authentication standards. This situation can create uncertainty for law enforcement officials and the parties regarding the requirements that must be met for electronic evidence to be accepted and assessed in the judicial process.

This problem also relates to the potential manipulation of electronic evidence. Unlike physical evidence, whose changes in form are generally directly observable, electronic data can be manipulated in ways that are relatively difficult to detect without specific examination. Emails can be forged through spoofing techniques, images can be modified using image processing software, audio recordings can be edited, videos can be cropped or manipulated, and electronic documents can undergo changes that are not always visible in the final presentation. Developments in artificial intelligence technology are also increasingly expanding the possibility of synthetic data that can visually and audibly resemble the original. This situation demonstrates that simply displaying a file or image in court is not always sufficient to ensure its authenticity. A mechanism is needed that can test the relationship between data and its source and ensure that the data has not undergone changes that could affect its evidentiary significance.

This issue demonstrates that authentication should not be understood solely as a matter of proving that "the data exists." Authentication should be directed at ensuring that the submitted data actually originates from the stated source and is in a trustworthy state. For example, the presence of a screenshot on a person's mobile phone merely indicates that the screenshot exists on that device, but does not necessarily prove that the communication depicted is the communication that occurred as depicted. Similarly, the existence of a file on a computer does not in itself prove who created it, when it was created, or whether the file has been modified. Therefore, authentication guidelines need to establish indicators that can distinguish between the existence of data and its authenticity.

A comparison with the United States legal system shows that these issues can be addressed by formulating authentication standards that combine legal provisions with certification mechanisms and technical examination. Federal Rules of Evidence Rule 902(13) and Rule 902(14)

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

provide self-authentication mechanisms for certain categories of electronic records and data obtained through specific processes. Rule 902(14), for example, regulates data copied from electronic devices or storage media and allows authentication through certification of the digital identification process used. This approach demonstrates that legal systems can provide more concrete parameters regarding the conditions under which electronic evidence is deemed to meet authentication requirements. Meanwhile, India, through the Bharatiya Sakshya Adhiniyam 2023, also regulates requirements for electronic records, including certificates containing information on the identification of the recording, how the recording was produced, the device used, and other technical information. This comparison demonstrates that technical aspects can be integrated into legal mechanisms for evidence without diminishing the judge's discretion in making judgments.

Based on this description, the main problem with electronic evidence authentication in Indonesia lies not in the lack of legal recognition, but rather in the lack of clarity in determining the parameters of its implementation. Norms requiring authentication must be translated into procedures that provide certainty for investigators, prosecutors, experts, and judges. Without clear standards, the authentication process potentially depends on the approach of each party and the characteristics of the case being examined. This condition can lead to variations in assessments regarding the need for forensic examination, the validity of acquisition methods, the adequacy of chain of custody documentation, and data integrity. Therefore, the lack of clarity in these standards is one of the main reasons indicating the need for establishing guidelines for the authentication of electronic evidence in criminal proceedings.

The Urgency of Regulating Guidelines for Authenticating Electronic Evidence in Proving Criminal Acts

The urgency of establishing guidelines for the authentication of electronic evidence can be seen primarily in the development of law that has positioned electronic evidence as an integral part of the criminal evidence system. When the law grants electronic evidence its status as evidence and simultaneously mandates authentication, an instrument is needed to explain how to fulfill this obligation. Without adequate guidelines, provisions regarding authentication have the potential to stop at the level of general norms that impose obligations but do not provide clear procedures for implementing them. In fact, in criminal procedural law, each stage of the evidentiary process must have a justifiable basis and procedure because the results of the evidence are directly related to the determination of a person's guilt or innocence. Therefore, the regulation of authentication guidelines is necessary as an instrument to operationalize the provisions of Article 235 of the Criminal Procedure Code so that authentication is not merely a normative concept but can be applied consistently in practice.

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

The next urgent need relates to the need to establish minimum standards applicable to all law enforcement agencies. Investigators are the parties who typically encounter electronic evidence from the initial stages, so the security and acquisition procedures implemented by investigators will determine the quality of the evidence at subsequent stages. Public prosecutors must then ensure that the evidence to be used in indictments and for proof has been obtained and managed according to accountable procedures. At the trial stage, judges have the authority to assess the authentication and legality of evidence acquisition. If each institution uses different standards, continuity issues can arise between the investigation, prosecution, and trial stages. Authentication guidelines are needed to establish minimum standards applicable across stages, ensuring continuity in the electronic evidence management process from discovery to assessment by the judge.

Authentication guidelines are also crucial to ensure that the electronic evidence collection process focuses not only on data quantity but also on its quality and integrity. Electronic devices can store vast amounts of data, and not all of this data is relevant to a case. In such circumstances, law enforcement officials require procedures that allow relevant data to be identified without compromising the integrity of the source data. Guidelines can provide standards for identification, acquisition, storage, examination, and documentation, allowing for systematic evidence management. Thus, authentication guidelines serve not only during trial but also as a preventative measure from the outset, minimizing the possibility of damage, loss, alteration, or contamination of electronic data intended for use as evidence.

The urgency of regulation also relates to protecting the rights of defendants and other parties involved in the criminal justice process. The use of electronic evidence can provide law enforcement officials with significant capabilities to uncover crimes, but at the same time, there is a risk that inauthentic or incomplete data will be used to support charges. Therefore, the authentication process serves as a control mechanism against the possible use of data that has been manipulated or obtained through unlawful means. Clear authentication standards allow defendants and their legal counsel a more objective opportunity to verify the authenticity of the evidence presented against them. In this context, authentication guidelines are not only a technical instrument for law enforcement officials but also part of ensuring a fair trial, as any evidence used to restrict a person's rights must be able to be verified for authenticity and legality.

On the other hand, authentication guidelines must be developed proportionally to avoid overly formalizing the criminal evidence process. Not all electronic evidence should be subjected to the same examination procedures. For example, certain data originating directly from electronic systems with recording and security mechanisms may have different authentication characteristics than manually generated screenshots. Therefore, guidelines need to consider the level of risk of

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

manipulation, the characteristics of the source, the method of acquisition, and the relevance of the evidence to the case. This risk-based approach allows authentication procedures to be applied proportionally without compromising evidentiary integrity. Thus, guidelines serve not only to tighten the admissibility of electronic evidence but also to provide certainty regarding when and to what extent certain examinations are necessary.

The digital forensic aspect is one component that needs to be considered in developing these guidelines. Digital forensics provides scientific methods for identifying, acquiring, preserving, examining, analyzing, and reporting digital data. In the context of authentication, these methods can be used to provide an objective basis for the source and integrity of electronic evidence. However, the use of digital forensics also requires standards regarding examiner competence, examination procedures, tools used, documentation, and the format of the resulting report. Without guidelines, there is a possibility that technical examination results will lack a uniform format and parameters, making it difficult for judges to understand and assess their relevance to authentication issues. Therefore, the regulation of authentication guidelines needs to reconcile the legal needs of evidence with digital forensic technical standards.

Authentication guidelines can also provide clarity regarding the role of experts in the evidentiary process. Experts are essentially needed to explain technical aspects that are beyond the judge's general knowledge. In cases involving digital data, experts can explain how the data was obtained, the methods used in the examination, the results of the integrity verification, and the possibility of changes or manipulation of the data. However, expert opinion should not replace the judge's authority in assessing evidence. Guidelines are needed to distinguish between the technical aspects that must be explained by experts and the legal aspects that fall within the judge's authority. Thus, the relationship between expert examination and the judge's authority can be balanced, so that the results of the technical examination serve as the basis for information for the judge without diminishing the judge's independence in assessing the entire evidence.

The urgency of establishing guidelines can also be seen in the need to create consistency in judicial practice. When electronic evidence is used in various types of crimes, the potential for variations in the characteristics of the evidence increases. Without minimum standards, there is a risk that evidence with relatively similar characteristics will be treated differently due to differing interpretations of authentication requirements. Consistency does not mean eliminating the authority of judges to assess cases based on specific circumstances, but rather providing basic parameters for assessments based on a responsible framework. With guidelines, judges can still consider the characteristics of each case, but there are minimum standards that can be used to assess whether

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

evidence meets authentication requirements. This is crucial for creating legal certainty and predictability in the criminal evidence process.

Experiences in other countries also demonstrate that authentication regulations can be formulated more concretely by integrating law and technology. The United States, through the Federal Rules of Evidence, has provided a self-authentication mechanism for certain categories of electronic records and data, including through certification of specific processes or methods. India has also developed a certification mechanism for electronic records, including information on devices, data production or storage processes, and other technical characteristics. These regulations cannot be directly implemented in Indonesia because each country has a different legal system, judicial structure, and evidentiary principles. However, these experiences can serve as comparative material to see how the law can provide clearer parameters for authentication without eliminating the judge's role in making judgments. In the Indonesian context, this approach can be developed by considering the criminal evidence system, the structure of law enforcement institutions, and developments in information technology in Indonesia.

Ultimately, the urgency of establishing guidelines for the authentication of electronic evidence can be defined as the need to bridge the gap between legal norms and the technical practice of evidence. While the 2025 Criminal Procedure Code (KUHAP) recognizes electronic evidence and requires authentication, these norms still require implementing instruments that provide clear and measurable parameters. Authentication guidelines should ideally address at least the identification of evidence sources, acquisition and security procedures, data preservation, chain of custody, integrity verification through relevant technical methods, the use of digital forensic examinations, the qualifications of examiners or experts, documentation of examination results, and the mechanisms for presenting and evaluating evidence in court. These regulations are necessary to ensure that the authentication process does not rely solely on differing interpretations but establishes minimum standards that can be applied consistently while still allowing judges to make judgments based on the specific circumstances of each case.

Thus, based on the overall discussion, it can be emphasized that the urgency of establishing guidelines for the authentication of electronic evidence in criminal proceedings is based on three main needs: normative needs, practical needs, and the need for legal protection. Normatively, the 2025 Criminal Procedure Code requires authentication of evidence, thus requiring implementing regulations that provide concrete parameters for its implementation. Practically, the characteristics of electronic evidence that are easily copied, transferred, changed, and manipulated require procedures that can guarantee authenticity, integrity, and continuity of the chain of custody. Meanwhile, from a legal protection perspective, authentication guidelines are

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

necessary so that evidence used in the judicial process can be truly tested and accounted for so as not to harm the rights of the parties. Therefore, the establishment of authentication guidelines is not intended to limit the use of electronic evidence, but rather to ensure that the expansion of its use is in line with legal certainty, justice, evidentiary integrity, and the principles of fair criminal justice.

4. CONCLUSION

Based on the results of the discussion, it can be concluded that the authentication of electronic evidence has an important position in the criminal evidence system because the existence of electronic evidence must not only be recognized normatively, but also must be able to ensure its authenticity, integrity, source, and acquisition process. The provisions in the Electronic Information and Transactions Law have provided the basis for recognizing electronic information, electronic documents, and their printouts as valid evidence, while the Criminal Procedure Code provides confirmation regarding the existence of electronic evidence while also requiring that such evidence can be authenticated and obtained legally. Thus, authentication is an inseparable stage of the evidence process because it is the basis for ensuring that the electronic evidence presented in court truly comes from a source that can be accounted for and has not undergone changes that could affect its substance.

However, regulations regarding the authentication of electronic evidence still face operational challenges. Existing provisions provide normative requirements, but do not yet provide comprehensive and uniform parameters for authentication procedures based on the characteristics of each type of electronic evidence. The differences in characteristics between video recordings, electronic conversations, emails, transaction data, metadata, and data obtained from electronic devices mean that the authentication process cannot be fully standardized. Furthermore, clearer standards are needed for acquisition methods, preservation, chain of custody, integrity checks, the use of digital forensic techniques, and documentation of the evidence security process. This situation has the potential to lead to differences in investigative practices, prosecutions, and judges' assessments of the authenticity and strength of electronic evidence.

Therefore, there is an urgency to establish electronic evidence authentication guidelines that can operationalize existing legal provisions into clearer, more measurable, and consistently applicable standards. These guidelines should ideally regulate at least the identification of evidence sources, procedures for acquisition and security, preservation, chain of custody, integrity checks, the use of digital forensic methods and techniques as needed, documentation of the examination process, and the qualifications of those conducting technical examinations. These guidelines should also maintain the position of judges as the parties with the authority to assess authentication

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

and evidentiary strength based on criminal procedure law. With comprehensive and proportional guidelines, the authentication process is expected to provide legal certainty, maintain the integrity of electronic evidence, reduce differences in practices between law enforcement officials, and provide better protection for the rights of parties in the process of proving criminal acts.

REFERENCES

Antoro, Hendri, Danrivanto Budhijanto, and Somawijaya. (2026). "Admissibility of Artificial Intelligence as Electronic Evidence: Comparative Perspectives from Indonesia, the United States, and Japan." IUS Journal of Law and Justice Studies, Vol. 14, No. 1, pp. 122–139.

Army, Eddy. (2022). Electronic Evidence in Court Practice. Jakarta: Sinar Grafika.

Casey, Eoghan. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Third Edition. Waltham: Academic Press.

Fuady, Munir. (2012). Theory of Criminal and Civil Evidence Law. Bandung: Citra Aditya Bakti.

Hamzah, Andi. (1984). Introduction to Indonesian Criminal Procedure Law. Jakarta: Ghalia Indonesia.

Harahap, M. Yahya. (2012). Discussion of Problems and Implementation of the Criminal Procedure Code: Court Hearing, Appeal, Cassation, and Judicial Review. Jakarta: Sinar Grafika.

Hiariej, Eddy OS (2012). Theory and Law of Proof. Jakarta: Sinar Grafika.

India. (2023). Bharatiya Sakshya Adhiniyam, 2023. New Delhi: Government of India.

Indonesia. (2024). Law of the Republic of Indonesia Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. Jakarta: Government of the Republic of Indonesia

National Institute of Standards and Technology. (2006). Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. Gaithersburg: National Institute of Standards and Technology.

Otto, Jan Michiel. (2009). "Rule of Law Promotion, Land Tenure and Poverty Alleviation: Questioning the Assumptions of Hernando de Soto." Hague Journal on the Rule of Law, Vol. 1, No. 1, p. 20–31.

Otto, Jan Michiel. (2012). "Real Legal Certainty in Developing Countries." In AW Bedner, S. Irianto, and TD Wirastri (Ed.), Socio-Legal Studies. Denpasar: Pustaka Larasan.

Pardo, Michael S. (2013). "The Nature and Purpose of Evidence Theory." Vanderbilt Law Review, Vol. 66, no. 2, p. 547–616.

Sasangka, Hari and Lily Rosita. (2003). Law of Evidence in Criminal Cases. Bandung: Mandar Maju.

Copyright (c) 2027 Author(s)

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License
ISSN print 2086-6852 and ISSN Online 2598-5892

Subekti. (2003). Law of Evidence. Jakarta: Pradnya Paramita.

Sukma, Galang Adhe. (2026, May 10). "Electronic Evidence Cannot Be Taken at Face Value: Dr. D'Costa Presents Digital Authentication and Forensics Standards for Judges." Suara BSDK.

United States Congress. (2017). Federal Rules of Evidence: Rule 902—Evidence That Is Self-Authenticating. Washington, DC: United States Congress.

Wasserman, Rhonda. (2004). Procedural Due Process: A Reference Guide to the United States Constitution. Santa Barbara: Greenwood Press.

Widodo Dwi Putro. (2024). Philosophy of Law: The Struggle between Western Philosophy, Eastern Philosophy, Islamic Philosophy, Indonesian Legal Thought, and Metajuridics in the Metaverse. Jakarta: Kencana.

Urbanization, Atalla Mufid. (2026). "Evaluation of the Position of Digital Evidence in Criminal Cases in the Era of Artificial Intelligence and Deepfake in Indonesia." Nusantara, Vol. 13, No. 1.

Copyright (c) 2027 Author(s)