International Journal of Educational Review, Law & Social Sciences (IJERLAS)

International Journal of Educational Review, Law And Social Sciences (IJERLAS Journal) | ISSN(e): 2808-487X
Volumes 5 No. 5 (2025)

# THE URGENCY OF LEGAL REGULATIONS RELATING TO THE AUTHENTICATION OF EVIDENCE ELECTRONICS IN THE INDONESIAN CRIMINAL JUSTICE SYSTEM

**Fayadh Ayyasi Regar[1], Milda Istiqomah[2], Faizin Sulistio[3]**
Master of Law Program, Faculty of Law/ Universitas Brawijaya, Malang
E-mail: fayadhar@student.ub.ac.id[1], milda.istiqomah@ub.ac.id[2], faizin@ub.ac.id[3]

| | | | |
|---|---|---|---|
| Received | : 30 June 2025 | Published | : 03 August 2025 |
| Revised | : 10 July 2025 | DOI | : https://doi.org/10.54443/ijerlas.v5i5.3773 |
| Accepted | : 28 July 2025 | Link Publish | : https://radjapublika.com/index.php/IJERLAS |

**Abstract**

This study aims to analyze the urgency of electronic evidence authentication in the Indonesian criminal justice system and formulate future legal regulations that provide legal certainty regarding the validity of electronic evidence. The research method used is a juridical-normative with a statutory and conceptual approach, which is based on a literature review of national regulations and international legal instruments such as the Budapest Convention. The results of the study indicate that the absence of provisions for electronic evidence authentication in the Criminal Procedure Code creates legal uncertainty and opens up opportunities for digital evidence manipulation in court. The discussion emphasizes the importance of digital forensics as a technical authentication mechanism to ensure the integrity, authenticity, and reliability of electronic evidence. In addition, the conformity of electronic evidence with the principles of relevance and legality is still not fully regulated in the criminal procedural law system. The conclusion of this study is that electronic evidence authentication needs to be immediately regulated firmly in legislation as a form of adaptation to developments in information technology to realize justice and legal certainty in the digital era.

**Keywords:** ***electronic evidence, authentication, criminal procedure, digital forensics, legal certainty***

## INTRODUCTION

The development of information technology has created significant changes in the criminal justice system in Indonesia, particularly in the aspect of evidence. Electronic evidence such as CCTV recordings, communication logs, digital transactions, and device metadata have become an integral part of criminal evidence. However, the presence of electronic evidence also raises new legal issues, one of which concerns its validity and authentication process. Although Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments has recognized electronic evidence as valid evidence, its application in court still faces obstacles due to the lack of technical provisions governing how electronic evidence can be authenticated and its legal integrity guaranteed. This is the main issue in the practice of criminal evidence in the digital era, not a lack of norms, but rather the blurring of norms regarding the authentication of electronic evidence.[1] This problem becomes even more complex when faced with the reality that electronic evidence is highly manipulable. Cybercrime evolves faster than the legal systems that regulate it. Digital evidence can be falsified, altered, or deleted without leaving a trace without adequate technical capabilities. This is where the urgency of authenticating electronic evidence in criminal cases lies. Authentication not only serves to prove that evidence truly originates from a legitimate source, but also to ensure that the evidence remains unchanged during the collection process until it is presented to the court. When authentication norms are insufficiently strict, the principle of due process of law and the right to a fair trial, for both victims and defendants, are at stake. This situation is reflected in several court decisions, such as criminal cases No. 297/Pid.B/2024/PN Kwg, 265/Pid.Sus/2017/PN Mtr, and 42/Pid.B/2024/PN Mgg. In both decisions, electronic evidence in the form of CCTV footage, video recordings from mobile phones, and digital data were used to support the charges, but not all were supported by accountable authentication procedures. In one decision, digital evidence was accepted because it

[1]Pratama, Herry Herlambang, Yos Johan Utama, and Aju Putrijanti. "Harmonization of the Law on State Apparatus and the ITE Law in the Provisions on Electronic Evidence as Additional Evidence in the State Administrative Court System." Journal of Indonesian Legal Development 6, no. 1 (2024): 61–81.

was attached to the Criminalistics Laboratory Evidence Examination Report, while in another decision, the judge questioned its validity because it was not accompanied by adequate digital forensic results. This inconsistency reflects normative confusion and diverse practices, which actually threaten the uniformity of decisions and legal certainty.[2] This situation indicates the need for a more systematic and conceptual approach to restructuring criminal evidence law, particularly regarding electronic evidence. To address this issue, this study employs a normative juridical method, examining national laws and regulations such as the Criminal Procedure Code (KUHAP) and the Electronic Information and Transactions (ITE) Law, as well as analyzing court decisions. However, a normative approach alone is not sufficient. Legal interpretation methods are also needed to understand and explore the meaning contained in these vague norms, so that precise and applicable interpretations can be drawn. Furthermore, a comparative legal method is used to examine electronic evidence authentication models in various more advanced countries, particularly through a study of the 2001 Budapest Convention on Cybercrime, which provides international standards regarding the collection and validity of digital evidence.[3]

Within the theoretical framework, this research is based on several relevant legal theories. First, the negative evidentiary theory adopted by the Indonesian criminal procedural law system emphasizes that a judge can only impose a sentence if there are at least two valid and convincing pieces of evidence. This means that electronic evidence must meet the requirements of being legally valid and technically convincing, which requires testable and verifiable authentication procedures. Second, the legal certainty theory according to HLA Hart explains that unclear legal norms can lead to uncertainty in the application of the law, so that interpretation or even normative reconstruction is needed so that the law can address new challenges. Third, the theory of the rule of law (rechtstaat) places the law as the commander in all judicial processes, including the necessity of clear and fair rules in determining evidence and the accompanying procedures. Conceptually, electronic evidence authentication is a technical and legal process to ensure that digital evidence is authentic, intact, and accountable.

This process involves various techniques such as hash value comparison, metadata verification, and digital forensic procedures performed by certified experts. Without these procedures, electronic evidence is vulnerable to questioning in court and potentially even excluded. Therefore, authentication must be a mandatory and standardized procedure, not merely an optional option. In other words, the authentication of electronic evidence in criminal cases is a legal issue that can no longer be ignored, as it concerns the legitimacy of the judicial process.[4] This study aims to critically explain why electronic evidence authentication must be explicitly regulated in the criminal procedural law system, as well as formulate a design for future legal regulations that can provide legal certainty. It is hoped that the results of this study can serve as a reference in the formulation of regulations, as well as a reference for judges and law enforcement officers in processing digital evidence legally and fairly. Based on the description above, the formulation of the problem in this study is as follows: how urgent is the authentication of electronic evidence in the Indonesian criminal justice system, and how future legal regulations will provide certainty for the authentication of electronic evidence in the Indonesian criminal justice system.

## LITERATURE REVIEW

The development of electronic evidence in the criminal justice system has given rise to various academic discourses that are important to examine critically. This literature review focuses on the theoretical and conceptual foundations related to the authentication of electronic evidence, its regulation in Indonesian law, and comparative practices from other legal systems. This review not only maps the research's position within the scientific landscape but also identifies concrete gaps that need to be addressed through the development of more robust and measurable authentication regulations. In the context of the Indonesian criminal justice system, electronic evidence has been recognized as valid legal evidence, as affirmed by Law Number 11 of 2008 concerning Electronic Information and Transactions and reinforced by Constitutional Court Decision Number 20/PUU-XIV/2016. This recognition has normatively opened up space for the use of digital evidence in court. However, recognition alone is not enough. The absence of explicit and technical norms on how electronic evidence should be authenticated leads to differences in perception and implementation in the field. Existing norms tend to be vague and unable to provide legal certainty

[2]Wijaya, Farhan Nabil, Wibi Saputro, and Agus Dimyati. "Due Process of Law in Verification and Validation of Electronic Evidence on the Use of Fake Motor Vehicle Registration Numbers in the Enforcement of E-Tilang." Journal of World Science 4, no. 7 (2025): 998–1004.

[3]Susatyo, Febryan Alam. "Criteria for Valid Electronic Evidence in the Urgency of Reforming the Criminal Procedure Code." Scientific Journal of Law and Social Dynamics 21, no. 1 (2023): 51–65.

[4]Asaad, Annisa Febriana. "The Legal Effectiveness of Electronic Evidence in the Examination of Evidence in the State Administrative Court." USM Law Review 6, no. 1 (2023): 279–290.

for law enforcement officials or parties in criminal proceedings.[5] In practice, electronic evidence can be manipulated, manipulated, or partially removed. Therefore, authentication is a crucial requirement to ensure the integrity, authenticity, and validity of digital evidence. Literature reviews indicate that authentication encompasses not only technical aspects such as verifying hash values, metadata, and file formats, but also legal mechanisms governing the process and standardization of electronic evidence. In the Indonesian context, digital evidence authentication is not yet a mandatory procedure in criminal procedure. The Criminal Procedure Code (KUHAP), as a formal law, does not specifically regulate the stages or requirements for authentication, while the National Police Chief's Regulation on Forensic Laboratories does not yet have the same legal force as a law to compel courts to adhere to specific authentication standards. This ambiguity creates legal uncertainty, as reflected in the differences in court decisions in cases involving electronic evidence.[6]

Three court decisions in criminal cases at the Magelang District Court and the Mataram District Court are clear examples of inconsistencies in the acceptance of digital evidence. In Decision Number 42/Pid.B/2024/PN Mgg, electronic evidence in the form of CCTV recordings was accepted and considered because it was supported by the Examination Report from the forensic laboratory and also in the ruling Ordered the Public Prosecutor to protect all electronic evidence from misuse, other than for evidence related to the Defendant's case. However, in Decision Number 297/Pid.B/2024/PN Kwg, digital evidence accompanied by authentication was accepted by the judge because it was considered convincing and its authenticity could be verified through the Examination Report from the forensic laboratory, Witness statements, and the Defendant's statement after being broadcast in court but did not contain a ruling Ordering the Public Prosecutor to protect all electronic evidence from misuse, other than for evidence related to the Defendant's case. Meanwhile, in Decision Number 265/Pid.Sus/2017/PN Mtr, the Panel of Judges did not accept electronic evidence even with laboratory authentication based on the Examination Results of Digital Evidence Number 220-XII-2016-CYBER by the Digital Forensic Examination Team at the IT & Cybercrime Sub-Directorate of the Directorate of Economic and Special Crimes of the Indonesian National Police Criminal Investigation Agency on the grounds that no data was found related to the purpose of the examination, namely related to the alleged crime of intentionally and without the right to distribute and/or transmit and/or make accessible electronic information and/or documents containing content that violates morality. These three decisions show that without clear and binding authentication norms, judges' decisions are highly dependent on personal beliefs and individual interpretations, not on uniform objective parameters. This not only creates uncertainty, but also opens up space for the misuse of digital evidence which should be an instrument of justice.

Various international literature emphasizes the importance of authentication in digital evidence systems. The 2001 Budapest Convention on Cybercrime, an international reference, emphasizes that electronic data used in judicial proceedings must undergo collection, storage, and analysis using auditable and verifiable methods. Ratified countries such as France, Germany, and South Korea have even integrated digital authentication into their criminal procedural laws, establishing regulations requiring electronic forensic results before evidence is admitted in court. In contrast, Indonesia lacks standards that universally mandate digital forensic verification. This results in a reliance on judicial discretion and a lack of consistency in the application of electronic evidence. If Indonesia is to align its criminal justice system with modern rule of law principles and international standards, authentication regulations are not only crucial but urgent.[7] Theoretically, this authentication issue is directly related to the negative burden of proof theory adopted in Indonesian criminal procedure law. This theory emphasizes that judges may not impose a sentence without at least two valid pieces of evidence and a belief in the truth of the material. In this context, electronic evidence must meet the requirements of legality and technical validity. Legality refers to normative recognition in law, while technical validity requires that the evidence be objectively verifiable through authentication that can be tested in court. Without authentication, judges lack a strong basis for establishing confidence, as the possibility of manipulation or fabrication cannot be scientifically ruled out. Therefore, authentication is not merely a practical necessity, but an integral part of fulfilling the principle of fair and legally valid evidence.

[5]Felicia Eugenia, Carla Joycelyne Limanto, and Dave David Tedjokusumo. 2024. "Practical Challenges in the Criminal Prosecution Process: Witness Credibility and the Validity of Electronic Evidence." Iuris Studia: Journal of Legal Studies 5 (2): 492–503.

[6]Daffa, Muh Faraz, Sufirman Rahman, and Abdul Qahar. "The Probative Power of Electronic Signatures as Evidence in Civil Cases." Journal of Lex Philosophy (JLP) 4, no. 1 (2023): 205–221.

[7]Pradipa, Arya. "Analysis of the Position of Electronic Evidence in Civil Case Proof Post-ITE Law and the Development of E-Court." Consensus: Journal of Defense, Law and Communication Sciences 2, no. 3 (2025): 191–203.

HLA Hart's theory of legal certainty also emphasizes that the law must be certain in its implementation. Norms that are vague, ambiguous, or open to multiple interpretations will weaken public trust in the law and create room for injustice. In this regard, authentication is part of the secondary norm that determines how the primary norm (the recognition of electronic evidence) can be effectively implemented. Without an authentication norm, criminal procedure law lacks a crucial instrument for guaranteeing the validity of evidence, leading to uncertainty and potential unequal legal treatment. Therefore, this study utilizes the theory of legal certainty as an important foundation for promoting authentication regulatory reform.[8] From the perspective of the rule of law theory, all actions in the legal process must be based on clear, written, and accountable rules. Unauthenticated evidence not only violates the principle of legal certainty but also undermines the principle of due process of law, which guarantees the protection of the rights of the accused and victims. A rule of law state demands that all judicial processes proceed within a definite legal framework and be open to oversight. Therefore, the absence of authentication norms in the Indonesian criminal procedural law system is not merely a technical issue but a violation of the fundamental principles of the rule of law itself. Therefore, the development of authentication regulations must be a strategic agenda for reforming Indonesian criminal law to align it with constitutional principles.

The gap in the literature further reinforces the urgency of this research. Previous studies have focused primarily on the validity of electronic evidence in a normative sense. Studies on the protection of crime victims, the provision of evidence in sexual crimes, and the application of the Electronic Information and Transactions Law in the criminal sphere have largely neglected the technical and normative aspects of authentication. This research addresses this gap by developing a theoretical and legal foundation that can serve as a basis for formulating an authentication mechanism for electronic evidence. This contribution is significant because it integrates procedural law, criminal law, and digital forensics approaches within a single legal analytical framework. By reviewing existing literature and comparing national and international legal practices, this study concludes that the authentication of electronic evidence in criminal cases is an urgent need. The current lack of clarity in norms creates legal uncertainty, discrimination in the assessment of evidence, and has the potential to undermine substantive justice. Therefore, this study is expected to provide concrete recommendations for legislators and law enforcement to develop comprehensive electronic evidence authentication regulations that are adaptive to technology and based on the principle of the rule of law that guarantees justice and certainty for all parties in the criminal justice process.[9]

## METHOD

This research is designed to address the legal issue of the validity of electronic evidence authentication in criminal cases in Indonesia, as well as how future legal regulations can provide legal certainty in this regard. Therefore, the methodological approach used must be able to explore legal concepts, trace jurisprudential practices, and compare evidentiary systems from several more established legal systems. In this case, the author applies a juridical-normative legal research method with a statutory approach and a conceptual approach, as well as adding legal interpretation and comparative law approaches to obtain a comprehensive picture in formulating precise and applicable legal solutions. The type of research used is juridical-normative, namely research that focuses on the analysis of positive legal norms as well as legal principles and doctrines that develop in legal science. This research examines legal norms in legislation and other legal documents to understand and answer the problems that have been formulated. In this research, the juridical-normative approach is highly relevant because the issue of electronic evidence authentication does not yet have explicit technical regulations in the national criminal procedural law system, so it is necessary to interpret existing norms, and examine their relevance to generally applicable legal principles. Therefore, a conceptual approach is used to analyze whether the spirit contained in the existing norms is still in line with the demands of justice and legal certainty in the digital era. This research also uses legal interpretation methods to explore the substantive meaning of existing norms related to electronic evidence and its authentication process. The interpretation is carried out on several laws, such as Law Number 8 of 1981 concerning Criminal Procedure Law (KUHAP), Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, and Law Number 1 of 2023 concerning the Criminal Code. The interpretation is carried out systematically, grammatically, historically, and teleologically to gain a deep understanding of authentication norms

[8]Lakada, Daniel David Julio. "The Development of Electronic Evidence Regulations in Criminal Procedure Law (Legal Study on Cyber Crime)." Lex Crimen 12, no. 5 (2024).
[9]Putra, Subhan Suryadi. The Power of Electronic Evidence in Proving Corruption Cases in Indonesia. Semarang: Sultan Agung Islamic University, 2024.

and their relevance in evidentiary practice.[10] Furthermore, comparative legal methods are used to examine how electronic evidence authentication systems are implemented in countries that already have digital evidence standards, such as the 2001 Budapest Convention on Cybercrime. This study includes technical and normative comparisons of the implementation of electronic evidence authentication in several countries, such as Germany, France, and South Korea. This comparison aims to identify best practices that can be adopted into the Indonesian legal system, while also demonstrating regulatory gaps that urgently need to be addressed. The data sources in this study were collected through a literature review, including primary, secondary, and tertiary legal materials. Primary legal materials consist of applicable laws and regulations, such as the 1945 Constitution, the Criminal Code, the Criminal Procedure Code, the Electronic Information and Transactions Law (UU ITE), and other related regulations, such as the Laws on the Supreme Court, General Courts, and Judicial Power. Secondary legal materials were obtained from legal literature books, scientific articles, journals, papers, and relevant research results. Tertiary legal materials used include legal dictionaries, legal encyclopedias, and other supporting sources that help explain legal terms or concepts related to the authentication of electronic evidence.

Data collection in this study was conducted using two main techniques: document study and interviews. Document study was conducted on relevant laws and regulations, court decisions, expert opinions, and legal doctrines. Specifically, court decision documents were the primary focus for analyzing how electronic evidence authentication is applied in practice. Interviews were conducted with officials or experts authorized in the field of digital forensics, judges, or investigators to obtain factual and in-depth information about authentication constraints and practices in law enforcement processes.[11] To search for relevant legal materials, the author employed a systematic search technique based on normative legal studies. The search was conducted through law library catalogs, national and international journal databases, and official Indonesian legal regulations websites. This technique enabled the author to obtain accurate and up-to-date legal information related to the research topic. The data analysis in this study was conducted using a descriptive-analytical approach. Descriptive analysis techniques were used to describe and classify relevant legal regulations, doctrines, and court decisions. A qualitative analysis was then conducted to evaluate the relationship between these norms and electronic evidence authentication practices. This analysis aims to identify weaknesses in the applicable legal system and formulate applicable normative recommendations for improving future authentication regulations.

In conducting this research, the writing system is organized into four main chapters. Chapter I contains an introduction explaining the background, problem formulation, research objectives, and methods used. Chapter II contains a literature review that outlines relevant legal theories and literature. Chapter III is the core section, presenting the results of the analysis of electronic evidence authentication practices and comparisons with other countries' legal systems. Chapter IV contains conclusions and suggestions, formulated based on the analysis results and directed at establishing clearer, more robust, and more implementable authentication norms. Through this structured methodology, it is hoped that this research will make a significant contribution to the development of Indonesia's criminal procedural law system, particularly in addressing the challenges of digitalizing evidence and the need for legal certainty regarding the authentication of electronic evidence. Normative, interpretive, and comparative legal approaches are the three main pillars for building a comprehensive analytical framework to address the legal issues raised in this research.[12]

## RESULTS AND DISCUSSION

### The Role of Electronic Evidence in Proving Criminal Cases

The development of digital technology has revolutionized various aspects of life, including the criminal justice system. Criminal cases that previously relied solely on conventional evidence such as witness testimony, letters, or defendant statements are now beginning to involve electronic evidence as the primary evidentiary instrument. In this context, CCTV footage, screenshots, communication logs, metadata, and other digital files are elements frequently presented in the investigative process, all the way to court. The criminal case involving defendant Fedo Dira Saputra, which was tried in Decision Number 42/Pid.B/2024/PN Mgg, provides a clear illustration of how electronic evidence, particularly CCTV footage, has become a key pillar in the evidentiary process.

[10]Laguens, Judex. "The Existence and Role of Electronic Evidence in the Indonesian Judicial System: Electronic Evidence." Judex Laguens 2, no. 1 (2024): 97–107.
[11]Eriani, Windi. "Digital Forensic Regulations in Proving Cyber Crime." Legal Studies, 2022.
[12]Anam, Muhammad Khoirul. The Existence of Legislation on Digital Forensics in the Criminal Evidence System. Yogyakarta: Islamic University of Indonesia, 2022.

In this case, the defendant was charged with committing aggravated theft in the early hours of the morning in the victim's yard. The items taken included a canary and its cage, a helmet, and an LPG gas cylinder. The incident was recorded by a CCTV camera installed in the housing complex. The recording was copied onto a flash drive and submitted by the Public Prosecutor as evidence. The CCTV recorded the defendant's actions chronologically, from parking his motorbike, entering the victim's yard, taking the items, and leaving the premises. Testimonies from witnesses who witnessed the recording, including the neighborhood head and the victim's neighbor, also confirmed that the person in the recording was indeed the defendant.[13] However, although the CCTV footage practically serves as crucial evidence, it is not clearly explained whether the recording files were authenticated. A digital authentication process is essential to ensure that the recording content is truly valid, unmodified, and taken from the original source. In this case, there is no mention of a digital forensic examination or the involvement of digital experts to verify the video metadata, file hash values, or other signs of digital file integrity. This raises important questions regarding the legitimacy of electronic evidence in criminal justice.

Indonesian criminal procedure law, under Article 184 of the Criminal Procedure Code (KUHAP), does not explicitly mention electronic evidence. Evidence such as CCTV footage is typically classified as "letters" or "indications," depending on the judge's interpretation. This ambiguity creates a gap between digital reality and legal norms. Yet, in today's information age, electronic evidence is not merely complementary but often forms the backbone of the evidentiary process, especially in the absence of direct eyewitnesses or the defendant's confession. In this case, the defendant's confession and witness testimony supported the CCTV footage. However, it must be emphasized that an ideal legal process must ensure the validity of all evidence, not rely solely on confessions or verbal corroboration. Especially if the defendant denies the charges or denies involvement, proving the authenticity of electronic evidence becomes crucial. Courts should establish strict authentication standards to ensure that digital video is legitimate, unedited, and consistent with its context.[14]

**Electronic Evidence Authentication Issues and Challenges to Criminal Procedure Law**

The main issue arising in this case is the lack of authentication of the electronic evidence. In practice, the CCTV footage was simply copied onto a flash drive and taken by the witness to investigators. It is not clear who made the copy, whether there was a report of the file handover, or whether investigators checked the file hash to ensure authenticity. Even though it was stated that the CCTV footage came from a neighborhood DVR, the original footage was not stored in a forensic system. The recording lasted only a week and was then automatically deleted. In other words, the only copy of the electronic evidence used was the witness's personal copy on a flash drive. In modern legal systems, the authentication of electronic evidence should be standard procedure. Authentication is the process of proving that evidence is truly authentic, unchanged since its initial acquisition, and verifiable as to its source. In countries with advanced legal systems, such as the United States and the United Kingdom, electronic evidence is inadmissible in court without a statement of authentication, either through digital forensic expertise or hash value testing to demonstrate data integrity. This procedure provides protection for prosecutors, defendants, and judges, as all parties can be confident that the evidence used is untainted by manipulation.[15]

Unfortunately, Indonesia does not yet have a digital forensics system integrated into its criminal procedural law. Although the Electronic Information and Transactions Law (ITE) and its derivative regulations recognize the validity of electronic documents, their application is more focused on civil and administrative cases, rather than criminal ones. As a result, the use of electronic evidence in criminal cases exists in a gray area: its existence is acknowledged, but the procedures for its acceptance and validation remain unclear. This creates significant potential for criminalization, misjudgment, or even manipulation of evidence by irresponsible parties. In this case, although the defendant did not deny his involvement and admitted to the theft, this does not eliminate the legal obligation to ensure that all evidence has undergone proper authentication. The court should still inquire about how the digital evidence was obtained, who holds the original copy, and whether there was any technical validation process. Otherwise, this precedent could become a disadvantage in future cases, especially if the defendant steadfastly denies

[13]Sujatmiko, Bambang, and Bambang Soesatyo. "The Urgency of Using Electronic Evidence in Trials as an Effort to Answer the Challenges of Law Enforcement in the Digital Era and Social Media Dynamics." Asian Journal of Social and Humanities 3, no. 9 (2025): 1604–1613.

[14]Lubis, Fauziah, Indana Halwa Shabri, Siti Adinda Puspita, Chairun Nissa Eprianty, Trisnanda Rielta, and Jannatun Naim. "An Analysis of the Validity of Digital Evidence in the Modern Technological Era." Fox Justi: Journal of Legal Studies 15, no. 02 (2025): 479–486.

[15]Gunarto, G., Y. Yusri, and S. Kusriyah. "Reconstruction of Evidence Regulations in Civil Jurisdiction Based on Justice Value." Scholars International Journal of Law, Crime and Justice 6, no. 08 (2023): 447–452.

involvement and claims the video was doctored. Authentication is also crucial to guarantee the defendant's right to a fair trial. Without assurance that evidence has not been manipulated, the defendant could be seriously harmed. For example, if a video is cut, edited, or audio is inserted, it could create a false narrative and frame someone for a crime they did not commit. Therefore, authentication is not merely an administrative formality, but the essence of the principle of fair trial in the modern criminal justice system.[16]

**Criminal Procedure Reform: Addressing Digital Challenges**

The urgency of regulating electronic evidence authentication in the Indonesian legal system cannot be delayed any longer. This case demonstrates that despite the widespread use of electronic evidence by law enforcement officials, the legal system has not provided clear guidelines for its use. This directly impacts the quality of justice, the professionalism of law enforcement officials, and the protection of citizens' legal rights. One urgent solution is to revise the Criminal Procedure Code (KUHAP) to include electronic evidence as a separate category, rather than simply being included in the "letter" or "instruction" classification. The regulation should detail the procedures for obtaining, storing, validating, and presenting electronic evidence in court. The authentication process should be carried out by digital forensics experts or authorized and skilled institutions. Metadata examination, hash analysis, time stamp verification, and chain of custody procedures should be made mandatory standards.

Furthermore, law enforcement officers must be provided with training on digital evidence and its management. Currently, many investigators lack a grasp of digital forensic principles. This results in electronic evidence being handled only physically, like regular files, without considering its digital integrity. If not addressed promptly, this lack of preparedness will become a stumbling block in combating cybercrimes and conventional crimes involving electronic devices.[17] The role of judges is also crucial in assessing electronic evidence. Judges need to have at least some digital literacy to understand how electronic evidence can be manipulated and how to distinguish genuine evidence from fabricated evidence. Therefore, training for judges and prosecutors is essential. Likewise, the provision of digital forensic equipment and laboratories in each high court jurisdiction ensures that the authentication process is not dependent on external parties.

Regulatory strengthening must also encompass the rights of the accused. The law needs to regulate the accused's right to request forensic testing of electronic evidence against them. The state must provide equal access to digital experts, not simply favor the public prosecutor. The principle of balance of evidence must be the foundation of procedural law, so that the judiciary does not become an instrument of one-sided domination. Finally, a monitoring mechanism for the management of electronic evidence needs to be developed. As in this case, if CCTV footage is simply copied by the witness to a personal flash drive, without a record or file integrity check, the potential for interference is significant. Therefore, a digital evidence management system needs to be established, starting with initial recording, encrypted storage, audit logs, and even the destruction of evidence after the case is concluded. All of this will create a criminal justice ecosystem that is adaptive to modern developments while still upholding the principles of justice, transparency, and accountability.[18]

## CONCLUSION

This research begins with the issue of unclear legal norms regarding the authentication of electronic evidence in the Indonesian criminal justice system. This ambiguity creates legal uncertainty, opens up opportunities for disparities in court decisions, and undermines the principle of justice for all parties involved in the legal process. A review of three court decisions reveals inconsistencies in the admissibility of electronic evidence due to the lack of standard authentication guidelines. Meanwhile, a comparison with the legal systems of other countries, particularly those that have ratified the Budapest Convention, emphasizes the importance of formulating objective, measurable, and legally accountable authentication standards. Therefore, it is necessary to update Indonesian criminal procedure law by explicitly and systematically incorporating norms for authenticating electronic evidence. This step will not only provide legal certainty but also ensure human rights protection, ensure due process, and enhance judicial integrity in the digital age. Future development plans include developing operational standards for digital

[16]Putra, Surya Dwi, and Stanislaus Riyanta. "Digital Forensic Governance Strategy in Indonesia to Realize the Credibility of Accountable and Efficient Public Law Enforcement Agencies." Journal of Social Research 4, no. 7 (2025): 1316–1327.
[17]Purwoleksono, Didik Endro, Iqbal Felisiano, and Silvania Soviana. "Autopsy as Electronic Evidence in Proving Criminal Acts." Syiah Kuala Law Journal 8, no. 2 (2024).
[18]Syarief, Elza. "Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia." International Journal of Cyber Criminology 16, no. 2 (2022): 32–46.

authentication, strengthening state forensic institutions, and providing technical training for law enforcement officers to meet the challenges of establishing evidence in technology-based criminal cases fairly and professionally.

## REFERENCES

Pratama, Herry Herlambang, Yos Johan Utama, dan Aju Putrijanti. "Harmonisasi Hukum UU Peratun dan UU ITE dalam Ketentuan Alat Bukti Elektronik sebagai Alat Bukti Tambahan dalam Sistem Peradilan Tata Usaha Negara." Jurnal Pembangunan Hukum Indonesia 6, no. 1 (2024): 61–81.

Susatyo, Febryan Alam. "Kriteria Alat Bukti Elektronik yang Sah dalam Urgensi Pembaharuan KUHAP." Jurnal Ilmiah Hukum dan Dinamika Masyarakat 21, no. 1 (2023): 51–65.

Asaad, Annisa Febriana. "Efektivitas Hukum Alat Bukti Elektronik dalam Pemeriksaan Bukti di Pengadilan Tata Usaha Negara." USM Law Review 6, no. 1 (2023): 279–290.

Daffa, Muh Faraz, Sufirman Rahman, dan Abdul Qahar. "Kekuatan Pembuktian Tanda Tangan Elektronik sebagai Alat Bukti dalam Perkara Perdata." Journal of Lex Philosophy (JLP) 4, no. 1 (2023): 205–221.

Lakada, Daniel David Julio. "Perkembangan Pengaturan Alat Bukti Elektronik dalam Hukum Acara Pidana (Kajian Hukum Tentang Cyber Crime)." Lex Crimen 12, no. 5 (2024).

Pradipa, Arya. "Analisis terhadap Kedudukan Alat Bukti Elektronik dalam Pembuktian Perkara Perdata Pasca UU ITE dan Perkembangan E-Court." Konsensus: Jurnal Ilmu Pertahanan, Hukum dan Ilmu Komunikasi 2, no. 3 (2025): 191–203.

Putra, Subhan Suryadi. Kekuatan Bukti Elektronik dalam Pembuktian Perkara Tindak Pidana Korupsi di Indonesia. Semarang: Universitas Islam Sultan Agung, 2024.

Laguens, Judex. "Eksistensi dan Peran Alat Bukti Elektronik dalam Sistem Peradilan di Indonesia: Alat Bukti Elektronik." Judex Laguens 2, no. 1 (2024): 97–107.

Eriani, Windi. "Pengaturan Digital Forensik dalam Pembuktian Tindak Pidana Cyber Crime." Ilmu Hukum, 2022.

Anam, Muhammad Khoirul. Eksistensi Perundang-undangan terhadap Digital Forensik dalam Sistem Pembuktian Pidana. Yogyakarta: Universitas Islam Indonesia, 2022.

Sujatmiko, Bambang, dan Bambang Soesatyo. "The Urgency of Using Electronic Evidence in Trials as an Effort to Answer the Challenges of Law Enforcement in the Digital Era and Social Media Dynamics." Asian Journal of Social and Humanities 3, no. 9 (2025): 1604–1613.

Lubis, Fauziah, Indana Halwa Shabri, Siti Adinda Puspita, Chairun Nissa Eprianty, Trisnanda Rielta, dan Jannatun Naim. "An Analysis of the Validity of Digital Evidence in the Modern Technological Era." Fox Justi: Jurnal Ilmu Hukum 15, no. 02 (2025): 479–486.

Putra, Surya Dwi, dan Stanislaus Riyanta. "Digital Forensic Governance Strategy in Indonesia to Realize the Credibility of Accountable and Efficient Public Law Enforcement Agencies." Journal of Social Research 4, no. 7 (2025): 1316–1327.

Gunarto, G., Y. Yusri, dan S. Kusriyah. "Reconstruction of Evidence Regulations in Civil Jurisdiction Based on Justice Value." Scholars International Journal of Law, Crime and Justice 6, no. 08 (2023): 447–452.

Purwoleksono, Didik Endro, Iqbal Felisiano, dan Silvania Soviana. "Autopsy as Electronic Evidence in Proving Criminal Acts." Syiah Kuala Law Journal 8, no. 2 (2024).

Syarief, Elza. "Security Concerns in Digital Transformation of Electronic Land Registration: Legal Protection in Cybersecurity Laws in Indonesia." International Journal of Cyber Criminology 16, no. 2 (2022): 32–46.

Wijaya, Farhan Nabil, Wibi Saputro, dan Agus Dimyati. "Due Process of Law in Verification and Validation of Electronic Evidence on the Use of Fake Motor Vehicle Registration Numbers in the Enforcement of E-Tilang." Journal of World Science 4, no. 7 (2025): 998–1004.

Felicia Eugenia, Carla Joycelyne Limanto, dan Dave David Tedjokusumo. 2024. "Tantangan Praktis dalam Proses Pembuktian Perkara Pidana: Kredibilitas Saksi dan Validitas Bukti Elektronik." Iuris Studia: Jurnal Kajian Hukum 5 (2): 492–503.