Multidiciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volumes 6 No. 4 (2026)

LEGAL STUDY OF DEFENSE STRATEGIES IN CRIMINAL CASES BASED ON ELECTRONIC EVIDENCE

Muhammad Rusdi[1], Sunardi Purwanda[2], Muhammad Sabir Rahman[3], Bakhtiar Tijjang[4], Aksah Kasim[5]
Institut Ilmu Sosial dan Bisnis Andi Sapada/ Parepare
Institut Ilmu Sosial dan Bisnis Andi Sapada/ Parepare
Institut Ilmu Sosial dan Bisnis Andi Sapada/ Parepare
Institut Ilmu Sosial dan Bisnis Andi Sapada/ Parepare
Institut Ilmu Sosial dan Bisnis Andi Sapada/ Parepare
Email: rusdijuraij@gmail.com[1] , Sunardipurwandaa@gmail.com[2] , sabirrahman6471@gmail.com[3], btijjang62@gmail.com[4], aksah.kasim@gmail.com[5]

Received	: 01 May 2026	Accepted	: 26 May 2026
Revised	: 05 May 2026	Published	: 01 June 2026

Abstract

This study aims to determine and analyze the legal qualifications in the Criminal Procedure Code and the ITE Law regarding electronic evidence in criminal cases in Indonesia and effective defense strategies in facing electronic evidence-based criminal cases by adapting to the new criminal law system. This study uses a Normative research type with a Legislative Approach and a Conceptual Approach. The types of legal material sources use Primary legal materials, Secondary legal materials and Tertiary legal materials. Legal analysis will be studied in a qualitative prescriptive manner. The results of this study are the legal qualifications in the Criminal Procedure Code and the ITE Law regarding electronic evidence in criminal cases in Indonesia, namely the Legal Qualification of Electronic Evidence based on Law Number 20 of 2025 concerning the Criminal Procedure Code, namely formally recognized as evidence, obtained legally and authentically (original and not changed/manipulated) and materially related to the crime and the identity of the perpetrator. While the legal qualifications according to the 2024 ITE Law are Valid as evidence, Obtained legally. and Obtained from a secure and tested electronic system, Electronic evidence must be original (authentic), unchanged (integrity) and trustworthy (reliability) and Must be related to the case and Effective defense strategies in facing electronic evidence-based criminal case evidence by adapting to the new criminal law system, namely Delegitimization of electronic evidence, Reclassification of evidence, Testimonium de Auditu Digital attacks, Analysis of evidence linkages, psychological attacks and suggestions and Alternative narratives.

Keywords: *Strategy, Defense, Electronic Evidence, Criminal Cases*

INTRODUCTION

In law, justice is considered abstract; it is a sollen and lives in the human imagination. [1]Currently, we are in the midst of the industrial revolution 4.0, characterized by the integration of physical, digital, and biological spaces. In terms of achieving justice, the development of information and communication technology has brought significant changes in various aspects of life, including the criminal justice system, which aims to achieve justice. The increasingly massive digitalization of human activity has given rise to various forms of electronic interactions and transactions, which in turn produce digital footprints *that* can be used as evidence in law enforcement processes. In this context, electronic evidence has become a crucial element in proving criminal cases, both in conventional crimes involving technology and in *cybercrime* .

In general, proof in criminal law is the process of discovering and declaring material truth (*materiële waarheid*) through evidence presented in court. Material truth means the actual truth, not merely formal truth. [2]Therefore, developments in law and technology have also recognized electronic evidence as valid evidence (through the ITE Law). The recognition of electronic evidence as valid evidence in the Indonesian legal system has been

[1]Purwanda, S., Ambarwati, A., Darmawati, D., & Prayudi, P. (2024). The social welfare orientation in the discourse of justice theories. Journal of Legal Dynamics, 25(1), 152–161.

[2] Elvi Susanti Syam. (2024). Criminal Procedure Law. Makassar: De La. Macca.

accommodated in various laws and regulations, particularly through Law Number 1 of 2024 in conjunction with Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). Electronic evidence, which includes electronic information and/or electronic documents and their printouts, now has the same legal force as conventional evidence, such as letters and witness statements. This marks a paradigm shift in the criminal law evidentiary system, from one previously based on physical evidence to the recognition of digital evidence. In the criminal justice system, a defense is a fundamental right guaranteed by law for every defendant. The principle of a fair trial requires that every individual accused of a crime have an equal opportunity to defend themselves, including when confronted with evidence presented by the public prosecutor. Therefore, the presence of electronic evidence as a new form of evidence requires an adaptive and comprehensive defense strategy to ensure the defendant's rights are optimally protected.

This indicates a paradigm shift in the evidentiary system, from one that relied on conventional evidence to one that embraces technology-based evidence. The logical consequence of this shift is the urgent need for evidence that is relevant to the times, namely electronic evidence. Electronic evidence has now become the new "queen of evidence," often possessing more crucial evidentiary value than witness testimony or the defendant's testimony in revealing material truth in court. However, the normative recognition of electronic evidence does not necessarily resolve the various problems that arise in practice. Electronic evidence has different characteristics compared to conventional evidence, such as being easily modified, copied, or deleted without leaving a visible trace. Therefore, the aspects of authenticity , integrity , and reliability *of* electronic evidence are crucial issues that must be considered in the evidentiary process in court. In addition, the procedures for obtaining and managing electronic evidence, including *the chain of custody* , are also important factors in determining the validity of the evidence.

In criminal justice practice, the use of electronic evidence often generates debate, particularly regarding its validity and evidentiary weight. It is not uncommon for law enforcement officials, including investigators, prosecutors, and judges, to differ in their interpretation of electronic evidence. This situation can lead to legal uncertainty and potentially harm the parties to the case, particularly defendants who must confront technical and complex evidence. The problem has become even more complex with the implementation of reforms to the national criminal law system, including Law Number 20 of 2025 concerning the Criminal Procedure Code (the new Criminal Code), which prioritizes a modern and adaptive approach to technological developments. However, synchronizing substantive and formal law, particularly regarding electronic evidence, remains a challenge that requires in-depth study.

The problem has become increasingly complex with the implementation of reforms to the national criminal justice system, including through the new Criminal Code, which prioritizes a modern and adaptive approach to technological developments. However, synchronizing substantive and formal law, particularly regarding electronic evidence, remains a challenge that requires in-depth study. Furthermore, law enforcement officials, such as investigators and prosecutors, tend to have greater access to technological resources and digital forensic expertise than defense attorneys. This imbalance has the potential to create an imbalance in the evidentiary process, ultimately harming the defendant. In this context, a defense strategy is crucial for identifying weaknesses in the process of collecting and processing electronic evidence by law enforcement officials.

Defense strategies in criminal cases based on electronic evidence can no longer be carried out conventionally. Advocates are required to have a comprehensive understanding of not only the legal aspects but also the technical aspects of information technology. The ability to test the validity of digital evidence, bring in digital forensic experts, and critique electronic data collection and seizure procedures are essential parts of a modern defense strategy. Furthermore, the principles of *fair trial* (justice) fair) and *due Due process of law* must remain the primary foundation in any evidentiary process. The use of electronic evidence that does not meet legal standards can potentially violate human rights, particularly the right to privacy and the right to a fair trial. Therefore, it is crucial to formulate a defense strategy that is not only technically effective but also in line with applicable legal principles.

Defense strategies in criminal cases based on electronic evidence are crucial because they determine the protection of the rights of legal subjects. Electronic evidence is technical, complex, and susceptible to manipulation, requiring a scientific approach such as digital forensics. Its recognition in the ITE Law requires advocates to understand legal procedures precisely. Furthermore, its intangible nature makes clients vulnerable, so strategies are needed to ensure *a fair trial* . Advocates must also verify the validity of evidence in accordance with the new Criminal Procedure Code and adapt to technological developments to ensure an effective and fair defense. However, in practice, not all legal counsel have the adequate capacity to handle electronic evidence. Limited technical knowledge, access to digital forensic experts, and a lack of practical guidelines on defense strategies based on electronic evidence

are obstacles. This has the potential to create an imbalance between public prosecutors, who are supported by law enforcement officers with greater resources, and defendants who rely on the capabilities of their legal counsel.

Furthermore, the use of electronic evidence in criminal cases also has implications for the protection of human rights, particularly the right to privacy and the right to a *fair trial* . The collection of electronic evidence that does not comply with legal procedures, such as unauthorized wiretapping or searches of digital data without a clear legal basis, can violate individual rights. Therefore, an effective defense strategy must be able to identify and criticize potential violations as part of efforts to protect the rights of the accused. The rapid dynamics of technological development are often not accompanied by adequate regulatory development. This results in a vacuum or lack of clarity in legal norms governing certain aspects related to electronic evidence. In such conditions, legal interpretation by law enforcement officials becomes crucial, which ultimately can lead to inconsistencies in the application of the law in practice. From the explanation above, it is clear that there is a gap between the legal norms governing electronic evidence and its practical application in the criminal justice system. This gap creates unique challenges in formulating effective defense strategies that adapt to technological developments. With a better understanding of effective defense strategies, it is hoped that the defendant's rights can be optimally protected, thereby truly realizing the principle of substantive justice.

METHOD

The type of research used is normative research. Normative legal research is also called doctrinal legal research, library research, or documentary study. It is called doctrinal legal research because it is conducted solely on written regulations or other materials. Normative research uses a theoretical-rational method with a deductive logical reasoning model (drawing conclusions from the general to the specific). [3]The approach used in this paper is a statutory approach, namely an approach carried out by examining all laws and regulations related to the legal issue being addressed. Conceptual legal research is a method that starts from the doctrines, thoughts, and views of legal experts to build legal arguments. This approach analyzes basic concepts to address legal issues when laws and regulations are inconsistent.[4]

RESULTS AND DISCUSSION

Legal qualifications in the Criminal Procedure Code and the ITE Law regarding electronic evidence in criminal cases in Indonesia

The development of information and communication technology has revolutionized various aspects of life, including criminal law enforcement in Indonesia. In the context of criminal cases, electronic evidence has become a crucial element due to the rise of cybercrime, digital transactions, and technology-based documentation. [5]The new Criminal Procedure Code (KUHAP), which has been ratified to replace the old KUHAP (Law No. 8 of 1981), introduces significant reforms, including the explicit recognition of electronic evidence as valid evidence. Meanwhile, Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) has strengthened the legal framework for electronic evidence by emphasizing the validity, integrity, and authentication of digital data.

The 1981 Criminal Procedure Code initially did not explicitly recognize electronic evidence, only mentioning "letters" and "witness statements" as primary evidence as in Article 184. [6]This raises legal doubts in the digital age, where evidence such as *emails* , *chat logs* , or CCTV recordings are often vital. Supreme Court decisions, such as No. 1234 K/Pid/2015, show the judges' inconsistent acceptance of electronic evidence, often relying on Article 5 Paragraph 4 of the earlier 2008 ITE Law. The ITE Law initially regulated Electronic Information and Electronic Documents (EID) as valid evidence as mentioned in Article 5, but limited it to civil transactions. The first (Law No. 19/2016) and second (Law No. 1/2024) amendments expanded its scope to criminal matters. In the development of criminal law and criminal procedure in Indonesia, electronic evidence has become increasingly important along with the rise in technology-based crimes. However, the recognition of electronic evidence does not occur automatically.

[3] Juliardi, B., Runtunuwu, YB, Musthofa, MH, TL, AD, Asriyani, A., Hazmi, RM, ... & Samara, MR (2023). Legal Research Methods. Padang: Gita Lentera.

[4] Syarif, M., Ramadhani, R., Graha, MAW, Yanuaria, T., Muhtar, MH, Asmah, N., Syahril, MAF, ... & Jannah, M. (2023). Legal Research Methods. Padang: Get Press Indonesia.

[5] Budiyanto . (2025). Introduction to Cybercrime in The Criminal Law System in Indonesia. Serang : Sada Kurnia Pustaka. Pg . 24.

[6] Rafika Nur, Amriyanto, Handar Subhandi Bakhtiar, Sunardi Purwanda . (2023). System Justice Criminal Law . Gorontalo: Cahaya Arsh Publisher & Printing. Pg . 45.

In the 1981 Criminal Procedure Code, the evidentiary system is a closed *system* , which only recognizes five types of evidence as regulated in Article 184 Paragraph 1: witness testimony, expert testimony, letters, clues, and the defendant's testimony. In this system, electronic evidence has not been explicitly recognized and is generally only positioned as part of the indicative evidence.[7] Fundamental changes occurred with the introduction of the new Criminal Procedure Code (KUHAP), which adopted an open system *of evidence* . Article 235 Paragraph 1 expands the scope of evidence to include witness testimony, expert testimony, letters, defendant testimony, physical evidence, electronic evidence, judges' observations, and anything else that can be used as evidence as long as it is obtained lawfully. This provision explicitly positions electronic evidence as independent and equal to other forms of evidence. [8]Furthermore, Article 242 of the new KUHAP explains that electronic evidence includes electronic information, electronic documents, and electronic systems related to criminal acts. This demonstrates that Indonesian criminal procedure law has responded to practical needs, given that many modern crimes, such as corruption, narcotics, and cybercrime, always leave digital traces. Thus, electronic evidence now holds a strategic position in the field of evidence.

The legal qualifications for electronic evidence in the new Criminal Procedure Code can be viewed from two aspects: formal and material. Formally, electronic evidence is recognized as valid evidence as long as it meets legal requirements. Article 235 Paragraph 3 emphasizes that evidence must be authentic and obtained lawfully. This means that electronic evidence must be obtained through legitimate procedures, by authorized officials, and must not violate human rights, particularly the right to privacy. The principles underlying this formal aspect include legality, *due process of law,* and accountability. If electronic evidence is obtained unlawfully, then based on Article 235 Paragraph 5, such evidence has no evidentiary force and must be disregarded by the judge. Furthermore, electronic evidence must meet the requirements of authenticity and integrity, namely that it originates from a legitimate source and remains unchanged from the time it is first created until it is presented in court.[9]

Materially, electronic evidence must be relevant to the crime being investigated. This relevance means that the content of the evidence must be able to prove the elements of the crime and the perpetrator's involvement. Evidence that is not relevant to the case has no probative value and can be ignored by the judge. This is in line with Article 244 Paragraph 2 of the new Criminal Procedure Code, which stipulates that the defendant must be acquitted if guilt is not legally and convincingly proven. [10]Therefore, relevance is a crucial factor in forming a judge's conviction. In addition to the Criminal Procedure Code, the Electronic Information and Transactions Law (UU ITE) also provides a legal basis for electronic evidence. Article 5 of the ITE Law states that electronic information, electronic documents, and printouts constitute valid legal evidence and constitute an extension of the evidence recognized in procedural law. With this provision, electronic evidence has strong legal legitimacy in various legal processes.

The ITE Law also emphasizes that electronic evidence must be obtained from legitimate and reliable electronic systems. Evidence acquisition must not be carried out through unlawful means, such as hacking or illegal wiretapping, as prohibited in Articles 30 and 32. [11]Legitimate electronic evidence is generally obtained through an investigative process by authorized law enforcement officials, such as the Indonesian National Police or Civil Servant Investigators (PPNS). Furthermore, there are three main requirements that electronic evidence must meet: authenticity, integrity, and reliability. Authenticity means the evidence is original and its source can be identified. Integrity means the data has not been altered or manipulated. Reliability means the electronic system that produces the evidence is trustworthy and functions properly. These three elements are interrelated, so if one is not met, the evidentiary force of the electronic evidence is weakened. Although the ITE Law does not explicitly mention relevance as a requirement, this principle still applies because the evidentiary value of electronic evidence is subject to criminal procedure law, namely the Criminal Procedure Code. Therefore, electronic evidence must remain relevant to the case and be able to explain the disputed facts.

The relationship between the new Criminal Procedure Code (KUHAP) and the ITE Law demonstrates harmonization. The KUHAP regulates the procedural aspects of evidence, while the ITE Law provides the technical basis for the validity and management of electronic evidence. In cases of conflict, the ITE Law tends to prioritize the technical aspects, while the KUHAP remains the primary reference in the criminal justice process. The relationship

[7] Vide article 184 paragraph (1) of the Law Number 8 of 1981 concerning Criminal Procedure Law .

[8] Vide Article 235 paragraph (1) of Law Number 20 of 2025 concerning the Criminal Procedure Code (KUHAP).

[9] Vide article 235 paragraph (5) of the Law Number 20 of 2025 concerning the Criminal Procedure Code (KUHAP).

[10] Vide article 242 of the Law Number 20 of 2025 concerning the Criminal Procedure Code (KUHAP).

[11] Vide Law Number 1 of 2024 concerning Change Second on Constitution Number 11 of 2008 concerning Electronic Information and Transactions .

between the new Criminal Procedure Code (KUHAP) and the ITE Law demonstrates harmonization. The KUHAP regulates the procedural aspects of evidence, while the ITE Law provides the technical basis for the validity and management of electronic evidence. In cases of conflict, the ITE Law tends to prioritize the technical aspects, while the KUHAP remains the primary reference in the criminal justice process. In the author's analysis, the recognition of electronic evidence as independent evidence in the new Criminal Procedure Code (KUHAP) represents a progressive step towards a digital justice system . Judges can no longer reject evidence solely because it is digital; instead, they are required to assess it as they would any other form of evidence. [12]However, the effectiveness of its implementation depends heavily on the preparedness of law enforcement officials, technical standards, and the integrity of the judicial process. From a *fair trial perspective,* the legal qualifications of electronic evidence are not solely assessed from a formal perspective but must also ensure fairness. Defendants must be given the opportunity to test the validity of the evidence, including through access to digital forensic examination. Without such access, an inequality *of arms can occur* that is detrimental to the defendant.[13]

From a justice theory perspective, the qualification of electronic evidence reflects procedural fairness, where evidence obtained illegally cannot be used. However, substantive fairness must also be considered, especially given the easily manipulated nature of electronic evidence. Therefore, strict technical standards are needed to ensure material accuracy. Meanwhile, according to the theory of legal protection, the regulation of electronic evidence qualification in the Criminal Procedure Code (KUHAP) and the ITE Law constitutes a form of preventive protection for individual rights. This provision limits the use of evidence obtained illegally and provides a basis for judges to assess the validity and reliability of evidence. Thus, electronic evidence must not only be legally valid but also guarantee the protection of human rights throughout the judicial process. The legal qualification of electronic evidence in Indonesian criminal law requires that both formal and material aspects be met, namely that it must be obtained legally, authentically, intact, reliable, and relevant to the case. The integration of the new KUHAP and the ITE Law demonstrates the direction of legal development towards an evidence system that is adaptive to technology, while still upholding the principles of justice and legal protection.

Effective defense strategies in facing criminal cases based on electronic evidence by adapting to the new criminal law system

Advances in information and communication technology have brought fundamental changes to various aspects of society, including the criminal justice system. Massive digitalization has resulted in almost all human activity leaving electronic traces, such as text messages, *emails* , digital recordings, and even transaction data. This situation makes electronic evidence a crucial instrument in the evidentiary process in criminal cases. [14]According to applicable law in Indonesia, the recognition of electronic evidence as valid evidence has undergone significant development. This is evident from the provisions in the 2024 Electronic Information and Transactions Law and the updates in the new 2025 Criminal Procedure Code. Electronic evidence is no longer considered merely supplementary evidence, but has equal standing with conventional evidence such as witness statements, letters, and clues.[15]

However, the use of electronic evidence in criminal cases raises various complex legal issues. Unlike conventional evidence, electronic evidence has special characteristics such as being easily altered, copied, manipulated, and highly dependent on the technological system used. This poses serious challenges in ensuring the authenticity *,* integrity , and reliability *of such evidence. In judicial practice, according to the author ,* debates often arise regarding the validity of electronic evidence, particularly regarding the method of acquisition, data security processes, and analysis methods used. Evidence obtained illegally, for example through illegal wiretapping or hacking, has the potential to violate human rights and the principle of due process of law. Therefore, caution is needed in accepting and evaluating electronic evidence to avoid harming the accused.

Furthermore, the author observes that the reform of the criminal law system through the new Criminal Procedure Code (KUHAP) has brought a new paradigm to the evidentiary process. This system emphasizes the importance of protecting the rights of suspects/defendants, transparency in the judicial process, and the accountable use of technology. Within this framework, defense strategies can no longer rely solely on conventional approaches but must be able to adapt to the dynamics of technology-based evidence. Defense strategies in criminal cases based

[12] Ariana, IN (2022). Legal Review of the Position of Electronic Evidence Based on Constitutional Court Decision Number 20/Puu-Xiv/2016. UNES Law Review, 5(1), 1-19.

[13] Isima, N. (2022). The position of electronic evidence in criminal cases. Gorontalo Law Review, 5(1), 179-189.

[14] Rasiwan, I. (2026). Open Evidence of the New Criminal Procedure Code. AMU Press, 1-260.

[15] Susilo, E. (2026). Examining the Certainty of Determining Suspect Status in the New Criminal Procedure Code. Al-Adl: Journal of Law, 18(1), 206-225.

on electronic evidence are becoming increasingly crucial because the defendant is often in an imbalanced position compared to law enforcement officials who have access to technology and digital forensic expertise. Without an appropriate strategy, electronic evidence that is actually weak or invalid can be considered strong and convincing in court. Therefore, an effective, systematic defense strategy is needed, based on a deep understanding of the legal and technical aspects of electronic evidence. This strategy includes examining the legality of evidence acquisition, analyzing the authenticity and integrity of data, and using digital forensic experts to refute or weaken the evidentiary strength of evidence presented by the public prosecutor. The defense strategy must be aligned with the principles of a fair trial, such as the presumption of innocence, the right to an effective defense, and the right to examine evidence presented in court (balance between the public prosecutor and the defense in accessing and examining evidence). In this context, the success of the defense is determined not only by the ability to argue legally, but also by the ability to understand technology and utilize it in the evidentiary process. Defense strategies in criminal cases based on electronic evidence in the new criminal law system require a more critical, structured approach, and one based on the principles of fair trial and due process of law. Regulatory changes through the 2025 Criminal Procedure Code and the 2024 Electronic Information and Transactions Law have expanded the legitimacy of electronic evidence as a stand-alone form of evidence. However, this expansion also carries serious consequences in the form of potential misuse, misinterpretation, and imbalance in the evidentiary process if not balanced with an appropriate defense strategy.

First, delegitimization of electronic evidence, which is a systematic effort to demonstrate that electronic evidence is legally invalid, inauthentic, unreliable, or irrelevant to the case. This strategy emphasizes that all evidence must be obtained legally, not in violation of the law (for example, through illegal access), and its authenticity can be verified. [16]In this context, advocates need to ensure that the data seizure and retrieval process is carried out in accordance with digital forensic procedures. If violations are found, the defense attorney can file an objection based on the exclusionary rule principle. The 2025 Criminal Procedure Code expressly states that evidence obtained unlawfully has no evidentiary force. Furthermore, the defense attorney must also examine technical aspects such as metadata, hashes, and data integrity to ensure that the evidence has not been manipulated. Without adequate forensic testing, the evidence can be considered mere assumptions.

The second strategy is evidence reclassification, which involves changing the legal position of electronic evidence within the evidentiary system. [17]The goal is not to eliminate the evidence, but rather to reduce its probative value. In practice, electronic evidence can be shifted from being the primary form of evidence to merely an indication requiring support from other evidence. This is important because in the criminal evidentiary system, the quality and type of evidence significantly determine its probative value. By reclassifying evidence, defense attorneys can encourage judges to disregard electronic evidence as the primary basis for decisions, thereby allowing for reasonable *doubt* . The third strategy is *the digital testimonium de auditu attack* , an approach that highlights the often circumstantial nature of electronic evidence (digital hearsay). [18]Electronic information presented in court does not always originate from the direct experience of the party presenting it, but rather from a system or other party. Therefore, the defense can assert that the evidence cannot be optimally tested, its original source is unclear, and its meaning is open to interpretation. This strategy is effective in reducing the evidentiary value without having to reject the evidence altogether.

The fourth strategy, analyzing the relationship between evidence, is crucial in testing the relevance of electronic evidence. Evidence must not only be formally valid; it must also have a direct connection to the elements of the crime and the defendant. The defense can challenge aspects of ownership, access, digital identity, time, location, and intent to demonstrate that the evidence lacks a strong connection. The basic principle is that without a clear connection, evidence is simply data with no probative value. This strategy aims to sever the connection between the evidence, the event, and the perpetrator.[19] The fifth strategy is psychological attacks and suggestion, which focus on exposing bias in the evidentiary process. [20]Electronic evidence does not stand alone but rather undergoes a process of selection, interpretation, and narrative by investigators, prosecutors, witnesses, and judges. In this process,

[16] Pahlawan, SAT (2025). The Position of Electronic Evidence in Proving Information and Electronic Transaction Crimes. Iuris Studia: Journal of Legal Studies, 6(3), 708-719.

[17] Arifatunnisa, S., & Wiraguna, SA (2026). The Position of Electronic Evidence in Civil Case Evidence After the Implementation of Digital Justice. Indonesian Legal Media (MHI), 4(1), 365-374.

[18] Tokan , B. (2025). Cross-Examination as a Method to Verify the Truth of Witness Statements. Lex Mandiri, 1(01), 34-45.

[19] Setyadi, HB, & Utari, IS (2025). The Legal and Sociological Relevance of Testimonium De Auditu in Proving Criminal Acts of Sexual Violence. Bookchapter of Law and the Environment, 1, 724-773.

[20] Helmawansyah, M. (2021). The use of electronic evidence as evidence in criminal cases. Journal of Law, 7(2), 527-541.

cognitive biases such as *confirmation bias* , *anchoring bias* , or *authority bias are highly likely to occur* . The defense can expose these biases to neutralize the influence of the suggestion and demonstrate that the evidence's meaning is not singular. This strategy is not manipulation, but rather an effort to maintain objectivity and balance in the evidence.

The final strategy is an alternative narrative, which involves constructing a reconstruction of events that differs from the prosecutor's version of events, but remains factually based. The alternative narrative aims to challenge the prosecutor's dominant narrative, demonstrate that the evidence supports more than one conclusion, and create reasonable doubt. In electronic evidence-based cases, an alternative narrative is crucial because electronic evidence is often open to multiple interpretations and contexts. By presenting alternative, logical interpretations, the defense can transform seemingly strong evidence into inconclusive evidence. The implementation of these strategies is reflected in real-world practice, such as in the case of Decision Number 61/Pid.Sus/2024/PN Parepare. In this case, the prosecutor presented a recording of the victim's interview as primary electronic evidence. However, the defense successfully demonstrated that the recording was not a recording of the incident, but rather a re-recording of the victim's account after the incident occurred. Using a digital testimonium de auditu approach, the defense argued that the evidence did not originate from direct experience at trial and could not objectively identify the perpetrator. Furthermore, through a linkage analysis, the defense asserted that the evidence had no direct connection to the defendant. The defense or advocate also reclassified the evidence by classifying it as supporting evidence, rather than primary evidence. Furthermore, through an alternative narrative, the defense demonstrated that other evidence, such as photos of the location and bloodstains, could not stand alone without the support of other valid and verified evidence. With this approach, the defense successfully established reasonable doubt, leading the panel of judges to declare the charges not legally and convincingly proven.[21]

Based on this explanation, it can be concluded that the effectiveness of a defense strategy depends heavily on the advocate's ability to identify weaknesses in electronic evidence, both in terms of legality, authentication, and relevance. Although the 2025 Criminal Procedure Code recognizes electronic evidence as independent evidence, defense attorneys can still weaken it through reclassification and critical examination. This demonstrates that the strength of evidence is determined not only by its formal status but also by its quality and relevance. From a fair trial theory perspective, a defense strategy must ensure a balance between the prosecutor and the defendant, including the right to examine evidence and witnesses. The defense should not be solely oriented toward victory, but also toward procedural fairness. Alternative narratives are an important instrument for creating reasonable doubt as the standard of proof in criminal cases.

Meanwhile, from the perspective of legal protection theory, defense strategies must function as a protective mechanism against the potential misuse of technology in evidence. Electronic evidence that is not guaranteed to be authentic or obtained illegally can become a tool of criminalization. Therefore, defense attorneys must actively prevent the unfair use of prejudicial evidence, both through preventive and repressive efforts. According to the theory of justice, an effective defense is one that ensures the judicial process runs according to legal procedures. Justice in criminal cases is not only about the outcome, but also about proper process. Therefore, electronic evidence that does not meet legality and authentication standards should not be used as a basis for criminal prosecution.[22] Ultimately, defense strategies in electronic evidence-based cases must be understood as an effort to maintain the integrity of the criminal justice system. The defense attorney's role is not only to represent the accused, but also to ensure that the law is enforced fairly, equitably, and respects human rights. In the digital age, the ideal defense is one that balances the power of technology with the sharpness of legal analysis, thereby preventing miscarriage of justice.

CONCLUSION

Legal qualifications in the Criminal Procedure Code and the ITE Law regarding electronic evidence in criminal cases in Indonesia, namely the Legal Qualification of Electronic Evidence based on Law Number 20 of 2025 concerning the Criminal Procedure Code, namely formally it is legally recognized as evidence, obtained legally and authentically (original and not changed/manipulated) and materially it is related to the crime and the identity of the perpetrator. While the legal qualifications according to the 2024 ITE Law are Valid as evidence, Obtained legally. and Obtained from a secure and tested electronic system, Electronic evidence must be original (authentic), unchanged (integrity) and trustworthy (reliability) and Must be related to the case and Effective defense strategies in facing electronic evidence-based criminal cases by adapting to the new criminal law system, namely Delegitimization of

[21] Vide Decision Number 61/ Pid.Sus /2024/PN Parepare .

[22] Agus Wibowo. (2026). Reform of the Criminal Code and Criminal Procedure Code as a Reconstruction of the Legal System in Indonesia. Semarang: Prima Agus Teknik. P. 103.

electronic evidence, Reclassification of evidence, Testimonium de Auditu Digital attacks, Analysis of evidence linkages, psychological attacks and suggestions and Alternative narratives.

REFERENCES

Agus Wibowo. (2026). PembaruaN KUHP dan KUHAP sebagai Rekonstruksi Sistem Hukum Di Indonesia. Semarang: Prima Agus Teknik.

Ariana, I. N. (2022). Tinjauan Yuridis Terhadap Kedudukan Alat Bukti Elektronik Berdasarkan Putusan Mk Nomor 20/Puu-Xiv/2016. UNES Law Review, 5(1), 1-19.

Budiyanto. (2025). Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia. Serang: Sada Kurnia Pustaka.

Budiyanto. (2025). Pengantar Cybercrime dalam Sistem Hukum Pidana di Indonesia. Serang: Sada Kurnia Pustaka.

Elvi Susanti Syam. (2024). Hukum Acara Pidana. Makassar: De La. Macca.

Helmawansyah, M. (2021). Penggunaan barang bukti elektronik yang dijadikan alat bukti dalam perkara pidana. Journal of Law (Jurnal Ilmu Hukum), 7(2), 527-541.

Isima, N. (2022). Kedudukan alat bukti elektronik dalam pembuktian perkara pidana. Gorontalo Law Review, 5(1), 179-189.

Juliardi, B., Runtunuwu, Y. B., Musthofa, M. H., TL, A. D., Asriyani, A., Hazmi, R. M., ... & Samara, M. R. (2023). Metode Penelitian Hukum. Padang: Gita Lentera.

Pahlawan, S. A. T. (2025). Kedudukan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana Informasi Dan Transaksi Elektronik. Iuris Studia: Jurnal Kajian Hukum, 6(3), 708-719.

Rafika Nur, Amriyanto, Handar Subhandi Bakhtiar, Sunardi Purwanda. (2023). Sistem Peradilan Pidana. Gorontalo: Cahaya Arsh Publisher & Printing.

Rasiwan, I. (2026). Pembuktian Terbuka KUHAP Baru. AMU Press, 1-260.

Setyadi, H. B., & Utari, I. S. (2025). Relevansi Yuridis Dan Sosiologis Testimonium De Auditu Dalam Pembuktian Tindak Pidana Kekerasan Seksual. Bookchapter Hukum dan Lingkung
an, 1, 724-773.

Purwanda, S., Ambarwati, A., Darmawati, D., & Prayudi, P. (2024). Haluan kesejahteraan sosial dalam diskursus teori-teori keadilan. Jurnal Dinamika Hukum, 25(1), 152–161.

Susilo, E. (2026). Meneropong Kepastian Penetapan Status Tersangka Dalam Kuhap Baru. Al-Adl: Jurnal Hukum, 18(1), 206-225.

Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., Syahril, M. A.F., ... & Jannah, M. (2023). Metode Penelitian Hukum. Padang: Get Press Indonesia.

Tokan, B. (2025). Cross-Examination Sebagai Metode Untuk Memverifikasi Kebenaran Keterangan Saksi. Lex Mandiri, 1(01), 34-45.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-undang Hukum Acara Pidana.

Putusan Nomor 61/Pid.Sus/2024/PN Parepare.