# The Position of Electronic Evidence in The Police Investigation Process Based on The Criminal Procedure Code and Law Number 1 of 2024 Concerning ITE

Welfriede Siregar[1], Ahmad Ansyari Siregar[2*], Nimrot Siahaan[3]

[1,2,3] Faculty of Law, University of Labuhan Batu, Indonesia
*Corresponding Author:
E-mail: ansyarisiregar@gmail.com

***Abstract.***

*The development of information technology has brought significant changes to modern crime patterns, which are increasingly committed through electronic media and leave digital traces.This situation demands adjustments to the criminal evidence system, particularly regarding electronic evidence.The Criminal Procedure Code (KUHAP), as the main criminal procedure law in Indonesia, does not specifically regulate the existence of electronic evidence, thus creating a normative vacuum in investigative practice.However, Law Number 1 of 2024 concerning Electronic Information and Transactions (UU ITE) is present as a lex specialis regulation that fully legitimizes electronic information and/or electronic documents as valid legal evidence and has the same evidentiary force as written evidence.This article aims to analyze the position of electronic evidence in the police investigation process through a normative juridical approach by examining the Criminal Procedure Code, the UU ITE, and law enforcement practices in the field.The results of the study indicate that electronic evidence plays a strategic role in uncovering crimes, especially digital-based crimes. However, its implementation still faces technical obstacles, data validity, limited human resources, and differences in interpretation among law enforcement agencies. Therefore, it is necessary to harmonize regulations, increase the capacity of investigators, and strengthen digital forensic infrastructure so that the use of electronic evidence can be more effective and accountable in the criminal evidence process.*

***Keywords:*** *UU ite; kuhap and special crimes.*

## I. INTRODUCTION

Indonesia is a country based on the rule of law that upholds the principles of justice and legal certainty in law enforcement. In today's digital era, advances in information technology have brought significant changes to the mechanisms of criminal evidence, particularly with the emergence of electronic evidence. Electronic evidence has become crucial in investigations because many crimes involve electronic information. Therefore, a clear legal basis is needed to guide police officers in using this evidence to ensure the legal process can proceed fairly and legally. The Criminal Procedure Code (KUHAP) and Law No. 1 of 2024 concerning Electronic Information and Transactions (UU ITE) serve as the primary legal basis governing the status and use of electronic evidence in criminal investigations in Indonesia.The development of information and communication technology in the last few decades has changed various aspects of human life, including the patterns and modes of criminal acts. Crimes are no longer committed solely through conventional means, but also through digital media such as mobile phones, computers, social media, the internet, and other electronic devices. This phenomenon has given rise to various new forms of crime, such as phishing, hacking, defamation through social media, the distribution of illegal content, online fraud, and other e-commerce crimes. Traces of these activities are stored in electronic data, which serves as a crucial source of evidence in investigations.

On the one hand, the Criminal Procedure Code (KUHAP), the primary criminal procedure law instrument in Indonesia, does not explicitly regulate electronic evidence. The 1981 Criminal Procedure Code clearly failed to anticipate the development of modern digital technology. As a result, a legal vacuum exists when police investigators must handle crimes in which the evidence is largely sourced from electronic media. This situation has created a dilemma regarding the validity and

validity of electronic evidence in proving evidence.On the other hand, Law Number 1 of 2024 concerning Electronic Information and Transactions (UU ITE), which was later amended by Law Number 11 of 2008, provides a clear legal basis for the use of electronic information and/or electronic documents as valid evidence. Article 5 of the ITE Law explicitly states that electronic evidence has the same legal force as written evidence as stipulated in the Criminal Procedure Code. This marks an expansion of the concept of evidence in Indonesian criminal procedure law.This recognition is crucial to addressing the challenges of law enforcement in the digital age. Police investigators are required to collect, analyze, and verify electronic evidence using scientific methods to demonstrate its authenticity, integrity, and relevance to a crime.

The use of digital forensics is now an integral part of the modern investigative process.However, the regulation of electronic evidence still faces a number of issues, including limited investigator capacity, a lack of digital forensic facilities and infrastructure, the potential for electronic data manipulation, and differing judges' interpretations of the probative value of digital evidence. Therefore, an in-depth study of the status of electronic evidence is essential to ensure that police investigations can proceed in accordance with the principles of legality, effectiveness, and human rights protection.Based on this background, this article comprehensively discusses the position of electronic evidence in the investigation process according to the Criminal Procedure Code and the ITE Law and its implications for law enforcement practices in Indonesia. This study is expected to provide a better understanding of the urgency of harmonizing criminal procedural law with developments in information technology. Article 184 of the Criminal Procedure Code (KUHAP) stipulates five types of valid evidence in criminal cases: witness testimony, expert testimony, letters, clues, and defendant testimony. However, technological developments require an expansion of these types of evidence. The ITE Law, specifically Articles 5 and 44, explicitly stipulates that electronic information and electronic documents, along with their printouts, are new forms of evidence recognized in the criminal evidence system.

This expands the scope of evidence beyond that already regulated by the Criminal Procedure Code, so that electronic evidence has equal standing with other forms of evidence in investigations and trials.During the investigation process, the police are required to collect and document electronic evidence, observing legal procedures and the validity of the electronic data's origin. Securing electronic evidence is crucial to ensure its integrity from initial collection to presentation to the court. The Digital Evidence First Responder (DEFR) method is often implemented, including securing devices such as mobile phones by digital forensic experts to prevent data manipulation. Investigators must also understand the technical and legal aspects of using electronic evidence to ensure its legal validity.Although electronic evidence has been formally recognized, challenges remain in its implementation. Difficulties in verifying data authenticity and the potential for manipulation are critical issues that must be addressed through technical expertise and strict procedural standards. With the introduction of the ITE Law, which complements the Criminal Procedure Code (KUHAP), the mechanisms for establishing evidence using electronic evidence have become clearer. However, enforcing legal certainty also depends on the professionalism of investigators and the understanding of judges in court regarding this evidence.

## II. METHODS

This research uses a normative juridical approach, focusing on analyzing the legal norms governing the status of electronic evidence in police investigations. This approach aims to examine the consistency, relationship, and synchronization between the Criminal Procedure Code (KUHAP) and Law Number 1 of 2024 concerning Electronic Information and Transactions (UU ITE) as the basis for modern evidence.

### *1. Type of Research*

This research is normative legal research, namely research based on literature review and an examination of primary, secondary, and tertiary legal materials. The focus of the study is directed at legal principles, theories of evidence, and the application of laws and regulations.

***2. Research Approach***

This research uses several approaches:

1. Statute Approach
   Analyze the provisions in the Criminal Procedure Code, the ITE Law, police regulations, and other relevant regulations.
2. Conceptual Approach
   Examines the concept of evidence, criminal evidence, digital forensics, and the position of electronic evidence in the Indonesian legal system.
3. Case Approach
   Using court decisions regarding electronic-based crimes as an example of the application of electronic evidence in practice.

***3. Sources of Legal Materials***

This research utilizes three types of legal materials:

a. Primary Legal Materials
   In the form of directly related laws and regulations, such as:
   1. Criminal Procedure Code
   2. Law No. 1 of 2024 concerning ITE and its amendments
   3. Supreme Court Regulations regarding electronic evidence
   4. Regulation of the Chief of Police regarding investigation management

b. Secondary Legal Materials
   In the form of literature, scientific journals, law books, opinions of legal experts, and previous research results that discuss electronic evidence.

c. Tertiary Legal Materials
   In the form of legal dictionaries, legal encyclopedias, and other supporting sources.

***4. Data Collection Techniques***

Data is collected through:

a. Library Research
   Reviewing legal documents, scientific articles, criminal procedure books, academic online sources, and court decisions related to electronic evidence.

b. Document Analysis
   Conduct a systematic review of legal provisions and court decisions relevant to the topic.

***5. Data Analysis Techniques***

The data was analyzed using qualitative legal analysis, which involves describing, interpreting, and summarizing existing legal provisions to answer the problem formulation. The analysis was conducted by:

a. identify legal norms related to electronic evidence;
b. comparing the provisions in the Criminal Procedure Code and the ITE Law;
c. assess the application of electronic evidence in investigative practices;
d. compile logical and systematic legal arguments.

## III. RESULT AND DISCUSSION

The research results show that electronic evidence plays a crucial and effective role in supporting the police's criminal investigation process, particularly in cases involving information technology, such as theft. Electronic evidence such as CCTV footage, emails, and electronic messages are legally admissible if they meet the requirements of authenticity, integrity, and accountability as stipulated in the ITE Law. A study conducted in the Tarakan Police jurisdiction confirmed that electronic evidence has proven effective as evidence in criminal proceedings, as long as the collection and security procedures are conducted forensically and according to standards. However, this effectiveness still faces several obstacles, including a lack of technical understanding by investigators and challenges in the acceptance of electronic evidence in court. Therefore, close collaboration between investigators and digital forensic experts is essential to ensure the validity of evidence. Improved standard operating procedures (SOPs) and ongoing training for law

enforcement officers are key to improving the quality of electronic evidence management. Furthermore, developments in jurisprudence recognizing electronic evidence further strengthen its position in the Indonesian criminal justice system.

***1. Legal Position of Electronic Evidence in the Criminal Evidence System***

a. Gaps in the Criminal Procedure Code and Attempts at Interpretation

The Criminal Procedure Code, which was drafted in 1981, did not anticipate digital evidence, so it does not explicitly mention electronic evidence. However, law enforcement officers have expanded their interpretation of:

a. documentary evidence, to insert electronic documents such as screenshots, emails, or digital files;
b. Instruction, to include CCTV footage, metadata, and log data.
c. This expansion of interpretation refers to the principle:
*d.* The law must follow the development of society (ubi societas ibi ius).
e. However, the expansion of interpretation still gives rise to differences of opinion between judges because there is no explicit basis in the Criminal Procedure Code.

b. Strengthening Through the ITE Law as Lex Specialis

The ITE Law, especially Articles 5, 6, and 44, emphasizes the legality of electronic documents as evidence.

a. Article 5 paragraph (1)**:**Electronic information/documents are valid legal evidence.
b. Article 5 paragraph (2): Equated with written evidence.
c. Article 6**:**Electronic documents are recognized for their validity and legal force.

Thus, the ITE Law provides a strong legal basis for police investigators to collect, confiscate, and assess digital evidence.

***2. The Significance of Electronic Evidence in Police Investigations***

a. Effectiveness of Uncovering Modern Crimes

Digital evidence can reveal crimes that are difficult to detect through conventional evidence, such as:

a. online fraud;
b. insults/hate speech;
c. dissemination of personal data;
d. online trading crimes;
e. online gambling;
f. distribution of pornographic content.

For example, in cases of online fraud, evidence in the form of chat history, account numbers, IP addresses, and transfer metadata can show the transaction flow connecting the perpetrator and the victim.

b. Advantages of Electronic Evidence over Conventional Evidence

Digital evidence has a number of advantages:

1. Objective → does not depend on the witness's memory or perception;
2. Detail → able to show location, time and activity accurately;
3. Can be restoredthrough digital forensics;
4. Capturing real-time action, for example CCTV.

This advantage makes digital evidence often the primary evidence in cybercrime and general criminal cases.

***3. Investigation Process and Utilization of Digital Forensics***

a. Evidence Collection Stage

Investigators collected evidence from:

a. mobile phone;
b. computer/laptop;
c. e-mail;
d. social media;
e. server;
f. CCTV footage;
g. cloud storage.

Collection must be carried out in accordance with the SOP for confiscating electronic evidence so as not to damage data integrity.

b. Security Stage and Chain of Custody

All electronic evidence must:

a. labeled,
b. recorded in the minutes,
c. stored in special media,
d. protected from modification.

A broken chain of custody can lead to invalid evidence in court.

c. Forensic Analysis Stage

Digital forensics is performed to:

a. recover deleted data;
b. extract metadata;
c. check file authenticity;
d. analyze activity logs;
e. prove account-device-perpetrator relationship.

The results are stated in the Forensic Expert Report which serves as supporting evidence.

***4. Main Obstacles in the Use of Electronic Evidence***

a. Technical and Technological Constraints

a. forensic equipment is not evenly distributed across all police stations/sectors;
b. analysis software is expensive and requires licensing;
c. technological developments are too fast so that officials are often left behind.

b. Lack of forensic expert human resources

Not all investigators have expertise in the following areas:

a. computer network,
b. cryptography,
c. cloud forensics,
d. log data analysis.

This leads to dependence on external experts.

c. Challenges to the Authenticity of Evidence

Digital evidence is vulnerable to:

a. edit, manipulate, cropping;
b. time change (timestamp);
c. account fraud;
d. IP spoofing.

Therefore, verification must be carried out scientifically.

d. Differences in Judges' Perspectives

Some judges still consider that:

a. digital evidence is weak when it stands alone;
b. digital evidence must be supported by witnesses and experts;
c. *screenshots*without verification is considered not authentic.

These differences hinder consistency of decisions.

***5. Urgency of Harmonizing the Criminal Procedure Code and the ITE Law***

Harmonization is needed so that:

1. electronic evidence is explicitly recognized in the Criminal Procedure Code;
2. electronic seizure procedures are regulated in detail;
3. digital forensics standards become national standards;
4. Citizens' privacy rights remain protected during the investigation.

Harmonization will strengthen legal certainty for investigators, public prosecutors, judges and the public.

## IV. CONCLUSION AND SUGGESTIONS

The legal and effective status of electronic evidence in Indonesian police investigations has been recognized as evidence in criminal cases. The Criminal Procedure Code (KUHAP) and the Electronic Information and Transactions (ITE) Law provide a strong legal basis for its use as evidence. Enhanced technical capacity, collaboration with digital forensics experts, and updated standard operating procedures (SOPs) and regulations are needed to address existing challenges and ensure the legitimacy and fairness of the criminal justice process.Police Professional Ethics is the moral basis and guideline for behaviorfor every member of the Indonesian National Police (Polri) in carrying out their duties. Police Regulation Number 7 of 2022 emphasizes that Polri members are not only professionally responsible but also obligated to uphold the values of integrity, honesty, justice, and respect for human rights. This ethic serves as a standard of behavior that must be adhered to in every action, decision, and exercise of police authority. To enhance institutional integrity,need to optimize ethical development, internal oversight, public reporting mechanisms, and consistent, impartial law enforcement. The Code of Ethics must be understood not merely as a formal obligation, but as a moral foundation that shapes the character of Polri members as professional, humane, and just.

## REFERENCES


[1] Abrian, Surya, Teguh Pahlawan, Authentication Proof, Evidence Analysis, and A Introduction. "Volume 6 Issue 3 Years 2025 E-ISSN : 2745-8369 Pages 708-719" 6, no. 3 (2025): 708–19.

[2] Premeditated Murder. "No Title," 2023.

[3] Evidence, Tools, Electronic Information, Fraud, and Online Crimes in "***IUS Journal of Law and Justice Studies"*** 9, no. 1 (2021).

[4] Faculty of Law, Sjakhyakirti University. "In Criminal Procedure Law Electronic Evidence As An Admissible Evidence In Criminal Law," 2017, 463–84.

[5] Ilham, Muhamad, Agus Salim, Master of Science, Law Program, Christian University, Indonesia Paulus, Master of Science, Law Program, Christian University, and Indonesia Paulus. "In The Process Of Proof According To The Law" 3 (nd): 1–13.

[6] Khatimah, Husnul, Sonia Winda Khairani, Dimas Ardiansyah, and Fauziah Lubis. "Legal Analysis of Electronic Evidence as Evidence in Civil Procedure Examination," no. April (2025).

[7] Law, Andrew, Andrew Law, Rica Regina Novianty, Dedy Saputra, and Hetty Ismainar. "Andrew Law" 4 (2025).

[8] No., Vol., In Case, and Legal Justice. "***Progressive Law Journal***" 7, no. 6 (2024): 106–11.

[9] Pid, K. "Perpetrator Of The Criminal Act Of Prepared Murder (Analysis Of Decision No. 813," no. 813 (2024).

[10] Pribadi, Insan. "Legality of Electronic Evidence in the Criminal Justice System," nd, 109–24.

[11] Review, Law, Volume NO April, and Evidence in Criminal Cases. "Gorontalo" 5, no. 1 (2022): 179–89.

[12] Safrin, Mohammad. "The Position of Electronic Evidence in Proving Criminal Acts" 5, no. 2 (2023): 1207–14. https://doi.org/10.37680/almanhaj.v5i2.2878.

[13] Sucia, Yossiramah, and Meissy Putri Deswari. "Electronic Evidence in the Justice System: Understanding Its Role and Validity" 4 (2024): 13729–41.

[14] Udayana, Faculty of Law. "The Position of Electronic Evidence in the Criminal Evidence System in Indonesia" 10, no. 5 (nd).

[15] Vernandhie, Dhanar Dhono, National Police, Republic of Indonesia, and South Jakarta. "Information Technology As Evidence In Investigation Of Traffic Accident Criminal Acts At Polda Metro Jaya Resort" 10, no. 2 (2022): 141–52.

[16] Abrian, Surya, Teguh Pahlawan, Authentication Proof, Evidence Analysis, and A Introduction. "Volume 6 Issue 3 Years 2025 E-ISSN : 2745-8369 Pages 708-719" 6, no. 3 (2025): 708–19.

[17] Premeditated Murder. "No Title," 2023.

[18] Evidence, Tools, Electronic Information, Fraud, and Online Crimes in "***IUS Journal of Law and Justice Studies***" 9, no. 1 (2021).

[19] Faculty of Law, Sjakhyakirti University. "In Criminal Procedure Law Electronic Evidence As An Admissible Evidence In Criminal Law," 2017, 463–84.

[20] Ilham, Muhamad, Agus Salim, Master of Science, Law Program, Christian University, Indonesia Paulus, Master of Science, Law Program, Christian University, and Indonesia Paulus. "IN THE PROCESS OF PROOF ACCORDING TO THE LAW" 3 (nd): 1–13.

[21] Khatimah, Husnul, Sonia Winda Khairani, Dimas Ardiansyah, and Fauziah Lubis. "Legal Analysis of Electronic Evidence as Evidence in Civil Procedure Examination," no. April (2025).
[22] Law, Andrew, Andrew Law, Rica Regina Novianty, Dedy Saputra, and Hetty Ismainar. "Andrew Law" 4 (2025).
[23] No., Vol., In Case, and Legal Justice. "***Progressive Law Journal***" 7, no. 6 (2024): 106–11.
[24] Pid, K. "Perpetrator Of The Criminal Act Of Prepared Murder (Analysis Of Decision No. 813," no. 813 (2024).
[25] Pribadi, Insan. "Legality of Electronic Evidence in the Criminal Justice System," nd, 109–24.
[26] Review, Law, Volume NO April, and Evidence in Criminal Cases. "Gorontalo" 5, no. 1 (2022): 179–89.
[27] Safrin, Mohammad. "The Position of Electronic Evidence in Proving Criminal Acts" 5, no. 2 (2023): 1207–14. https://doi.org/10.37680/almanhaj.v5i2.2878.
[28] Sucia, Yossiramah, and Meissy Putri Deswari. "Electronic Evidence in the Justice System: Understanding Its Role and Validity" 4 (2024): 13729–41.
[29] Udayana, Faculty of Law. "The Position of Electronic Evidence in the Criminal Evidence System in Indonesia" 10, no. 5 (nd).
[30] Vernandhie, Dhanar Dhono, National Police, Republic of Indonesia, and South Jakarta. "Information Technology As Evidence In Investigation Of Traffic Accident Criminal Acts At Polda Metro Jaya Resort" 10, no. 2 (2022): 141–52.