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. 3 (2025)

THE POSITION OF DIGITAL EVIDENCE IN THE KUHAP EVIDENCE SYSTEM NORMATIVE ANALYSIS AND IMPLEMENTATION CHALLENGES

Muhammad Yasir
Faculty of Law, Universitas Lambung Mangkurat, Banjarmasin, Indonesia,
Email: muhammad.yasir@ulm.ac.id

Received	: 24 April 2025	Published	: 30 May 2025
Revised	: 03 May 2025	DOI	: https://doi.org/10.54443/ijerlas.v5i3.3852
Accepted	: 25 May 2025	Link Publish	: https://radjapublika.com/index.php/IJERLAS

Abstract

The development of information technology has given rise to new forms of crime that utilize digital media, thus requiring specific regulations for digital evidence within the Indonesian criminal procedure system. The Criminal Procedure Code (KUHAP), as the primary legal instrument, does not explicitly address the definition and procedures for managing digital evidence, creating challenges in the investigation, prosecution, and presentation of evidence in court. This study discusses the definition and characteristics of digital evidence, the urgency of its regulation in the Criminal Procedure Code (KUHAP), the technical and legal challenges in its use, and a comparison of practices in other countries as material for evaluation and recommendations. The analysis shows that unclear regulations lead to legal uncertainty and potential human rights violations. Therefore, an update to the Criminal Procedure Code is needed to include specific provisions on digital evidence, including confiscation, security, and digital forensic validation. This update is deemed necessary to ensure effective law enforcement and protect the rights of suspects and defendants in Indonesia's digital era.

Keywords: ***Digital evidence, Criminal Procedure Code, criminal procedure law, digital forensics, legal updates***

Introduction

The development of information technology in the 21st century has brought about major changes in various aspects of our lives, including the legal field. Various technological advances in communications, computing, and the internet have given rise to new forms of social, economic, and cultural interactions that are no longer limited by space and time. In line with this, various new forms of crime have emerged that utilize digital technology, such as cybercrime, online fraud, and the distribution of illegal content through social media (Wall, 2007). In the context of criminal procedure law, these developments have given rise to a type of evidence previously not explicitly recognized in traditional evidentiary systems: digital evidence. Digital evidence encompasses any information stored, generated, communicated, or processed in digital form and can be used to prove a fact in court. It takes a wide variety of forms, from short messages, electronic mail, electronic documents, audio and video recordings, electronic transaction data, file metadata, to digital traces on social media (Casey, 2011). The uniqueness of digital evidence lies in its easily modified, easily copied, and ability to be hidden in physically invisible storage media. These characteristics are both strengths and weaknesses of digital evidence: on the one hand, it can be highly accurate and detailed evidence, but on the other hand, it is vulnerable to manipulation and requires rigorous technical verification procedures (Kerr, 2005). Within the framework of Indonesian criminal procedure law, valid evidence is regulated in a limited manner in Article 184 paragraph (1) of the Criminal Procedure Code, which includes: witness statements, expert statements, letters, instructions, and statements from the accused. This provision was created in 1981, when computer and internet technology had not yet developed as rapidly as it has now. This resulted in the Criminal Procedure Code not explicitly regulating the status of digital evidence. This creates a legal loophole, because judges and law enforcement must interpret to place digital evidence into the existing category of evidence, usually under the category of "letters" or "instructions" (Hamzah, 2016).

In this regard, this normative vacuum has serious implications for legal certainty and human rights protection in the criminal justice process. For example, when digital evidence is confiscated and presented in court, questions arise: does the evidence meet the requirements for validity as stipulated in the Criminal Procedure Code? How can we ensure that the digital evidence remains unchanged from the moment it is first discovered until it is presented in court? These questions are not merely technical but also touch on fundamental aspects of criminal procedural law, such as the principles of fair trial and due process of law (Yulia, 2022). To fill this regulatory gap, several regulations outside the Criminal Procedure Code (KUHAP) have attempted to provide a legal framework for digital evidence, such as Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments through Law No. 19 of 2016, and Supreme Court Regulation No. 11 of 2016, which regulates the procedures for examining criminal cases by corporations, including the recognition of electronic documents as evidence. However, these regulations are partial and sectoral in nature, thus failing to establish a comprehensive and consistent evidentiary system. Furthermore, there is potential for overlap and differences in interpretation among law enforcement officials, which could ultimately influence court decisions (Harahap, 2020).

This situation is exacerbated by the technical challenges inherent in digital evidence, such as the need for digital forensic expertise for seizure and analysis, and the importance of maintaining the chain of custody of evidence from its acquisition to its presentation in court (Sugiarto, 2021). Without clear procedures and established standards, digital evidence risks being rejected by judges for failing to meet formal or material requirements. This phenomenon demonstrates the urgency of updating the Criminal Procedure Code (KUHAP) to explicitly accommodate digital evidence within the criminal evidence system. This update is crucial not only to anticipate the development of digital crime but also to ensure that the criminal justice process in Indonesia remains aligned with the principles of the rule of law and international human rights standards, particularly the International Covenant on Civil and Political Rights (ICCPR), which guarantees the right to a fair trial. Thus, a normative study of the position of digital evidence within the Criminal Procedure Code (KUHAP) evidentiary system is relevant and urgent. This study is expected to provide theoretical contributions to the development of criminal procedure law and offer normative solutions that can be adopted in future revisions to the KUHAP, in order to create a criminal justice system that is responsive to technological developments and upholds the principle of fair trial.

Method

This research uses normative legal research, which focuses on the study of applicable positive legal norms. Normative legal research aims to analyze laws and regulations, legal doctrines, and legal principles relevant to the topic of discussion. According to Soerjono Soekanto, normative legal research is research conducted on library materials or secondary data, which includes legal principles, legal systematics, the level of legal synchronization, legal history, and comparative law (Soekanto, 2012). In the context of this research, the analysis is directed at understanding the legal framework of criminal procedure in Indonesia, particularly regarding the principle of fair trial and the rights of suspects/defendants. This type of research was chosen because the topic under study requires an in-depth understanding of the substance of written law, without requiring the collection of empirical data from the field. Normative legal research allows researchers to examine relevant articles in the Criminal Procedure Code (KUHAP) and its implementing regulations, and compare them with international legal principles and academic doctrine.

In this normative legal research, several complementary approaches are used, namely:

Statutory Approach: This approach is carried out by examining the laws and regulations that form the legal basis for the issue being studied. In this research, the main focus is directed at the Criminal Procedure Code, Law Number 48 of 2009 concerning Judicial Power, as well as various Supreme Court regulations and other related regulations. With this approach, researchers can comprehensively understand the scope and mechanisms of protecting the rights of the accused, from the investigation stage to the trial.

Conceptual Approach: A conceptual approach is used to analyze key concepts relevant to the topic, such as the principle of fair trial, due process of law, and the right to legal aid. This approach helps clarify the definitions and meanings of these concepts, both from a national and international legal perspective, for example, as stipulated in the International Covenant on Civil and Political Rights (ICCPR). The Case Approach: This approach is conducted by examining relevant court decisions, from the first instance to the Supreme Court. Decision analysis is used to examine how the principle of fair trial is applied in practice and to identify potential discrepancies between written legal norms and their implementation in practice.

Results and Discussion

1. Position and Regulation of Digital Evidence in the Criminal Procedure Code Evidence System

The Criminal Procedure Code (KUHAP) establishes a strict evidentiary system through Articles 183 and 184. Article 183 of the KUHAP states that “A judge may only impose a sentence if there are at least two valid pieces of evidence and he is convinced of the defendant’s guilt.” Meanwhile, Article 184 paragraph (1) of the KUHAP explicitly mentions five types of evidence: witness testimony, expert testimony, letters, instructions, and the defendant’s testimony (Harahap, 2020). This limited format is a major challenge when dealing with digital evidence because it is not expressly stated in the KUHAP. The ITE Law (No. 11 of 2008 and its amendment, Law No. 19 of 2016) provides space for digital evidence. Article 5 paragraph (1) states that "Electronic Information and/or Electronic Documents and/or printouts thereof constitute valid legal evidence." And paragraph (2) emphasizes that such evidence is an extension of valid evidence according to the applicable procedural law in Indonesia (Ius Constituendum…, 2025). Thus, the ITE Law normatively legitimizes electronic evidence, even though the Criminal Procedure Code has not been revised.

According to Manurung & Krisnawati (2022), electronic evidence is recognized as an extension of indicative evidence and is valid if it meets objective and reliable criteria. They stated, "Electronic evidence... is a form of extension/development of indicative evidence, so that in the Criminal Procedure Code its status is electronic indicative evidence." (Manurung & Krisnawati, 2022). However, this recognition is uneven—depending on the judge's interpretation and technical readiness. In practice, CCTV recordings, for example, are often considered supplementary evidence (electronic indicative evidence), especially when they complement witness testimony to fulfill the two-item evidence requirement in Article 183 of the Criminal Procedure Code (Maarif, 2024). Furthermore, Constitutional Court (MK) Decision Number 20/PUU-XIV/2016 emphasized that electronic evidence is only valid if it is obtained legally and not the result of illegal wiretapping. This affirmation is crucial for maintaining the integrity and validity of digital evidence (Manurung & Krisnawati, 2022; Silaban & Sugama, 2021).

Another study by Islamiyah & Hariyanto (2022) highlighted electronic evidence in skimming cases. They explained that CCTV footage or printouts, obtained legally, can be used as evidence—provided that the seizure must follow procedures in accordance with criminal procedure law. If all procedures are met, electronic evidence can have the same legal force as classical evidence (Islamiyah & Hariyanto, 2022). Overall, while the Criminal Procedure Code (KUHAP) does not explicitly recognize digital evidence, the ITE Law has paved the way. However, its implementation in practice remains limited by differing legal interpretations, the preparedness of judicial officials, and digital forensic procedures. This creates significant legal uncertainty regarding the admissibility of digital evidence in court.

2. Normative Analysis: Integration of Digital Evidence into Evidence Systems

The Criminal Procedure Code (KUHAP) itself, in effect since 1981, still relies on conventional evidence, such as witness testimony, expert testimony, letters, clues, and defendant testimony, as stipulated in Article 184 of the KUHAP. Meanwhile, digital evidence is not explicitly mentioned. This creates a legal gap that impacts the evidentiary process in cases involving information technology. As Yahya Harahap (2017) emphasized, the strength of evidence in the KUHAP is limited by the types of evidence that are explicitly mentioned. However, developments in national legislation provide opportunities to integrate digital evidence through other legal instruments. For example, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendment in Law Number 19 of 2016, explicitly recognizes electronic documents and/or their printouts as valid legal evidence. Article 5 paragraph (1) of the ITE Law states: “Electronic Information and/or Electronic Documents and/or their printouts constitute valid legal evidence.” Thus, there has been an expansion of the meaning of evidence recognized by positive law, even though the Criminal Procedure Code has not been revised to accommodate these developments. Normatively, the integration of digital evidence into the Criminal Procedure Code (KUHAP) evidentiary system can be achieved through a legal harmonization approach. This principle requires that existing norms in different regulations be harmonized to avoid contradictions in their application. As explained by Marzuki (2017), "legal harmonization is an effort to combine norms from various laws and regulations to create harmony within the national legal system" (p. 56). In this context, digital evidence regulated in the ITE Law can be positioned as a complement to written evidence or instructions in the Criminal

Procedure Code, as long as it meets the formal and material requirements stipulated. On the other hand, challenges arise in the aspect of proving the authenticity and integrity of digital evidence. According to Casey (2011), "digital evidence is more fragile than traditional evidence, and can be altered, damaged, or destroyed by improper handling" (p. 45). Therefore, the integration of digital evidence requires standard procedures related to the seizure, storage, and analysis of digital forensics that can guarantee the validity of the data. This is in line with the Regulation of the Chief of Police Number 10 of 2010 concerning Procedures and Requirements for Requests for Forensic Laboratory Examination, which, although technical in nature, serves as an important guideline for law enforcement officers. Normative analysis also considers the evidentiary dimension in court. Courts often still require careful interpretation when accepting digital evidence. In the South Jakarta District Court's decision No. 709/Pid.B/2016/PN.Jkt.Sel, for example, digital evidence in the form of WhatsApp conversation recordings was accepted as documentary evidence after verification by a digital forensic expert. This demonstrates that judicial practice is beginning to accept digital evidence, but it always requires expert testimony to assess its authenticity.

Furthermore, the principle of chain of custody is an integral part of digital evidence. This principle ensures that from the time digital evidence is discovered, seized, and presented in court, there is no alteration or manipulation of the data. As explained by Rogers et al. (2006), "maintaining an unbroken chain of custody is essential to preserve the evidential value of digital evidence" (p. 12). Without this principle, digital evidence may be deemed invalid or its validity questionable. Thus, the integration of digital evidence into the evidentiary system of the Criminal Procedure Code (KUHAP) requires changes, or at least a reinterpretation, of existing legal norms. A normative approach demonstrates that although the Criminal Procedure Code (KUHAP) does not yet contain explicit provisions on digital evidence, its recognition through the ITE Law and judicial practice have opened up space for digital evidence to play a role in the evidentiary process. However, this integration must be supported by technical standards, strict procedures, and legal harmonization to ensure that digital evidence has equal evidentiary force to other forms of evidence.

3. Implementation of Digital Evidence

Most workers have a positive perception of the integration of religious values in the workplace. For example, one study found that employees' spiritual values and practices in the workplace were positively correlated with mental well-being and lower work stress, indicating a positive view of such integration.(Arnetz et al., 2013). Employees prefer the integration of religious values that are universal and inclusive. This means that such integration should not favor any particular religion, but should accommodate diverse religious beliefs. For example, one study found that only 49% of companies integrate religions other than Christianity or Judaism, indicating the need for more inclusive practices.(Borstorff & Arlington, 2011). Companies need to be proactive in clearly communicating their diversity policies and ensuring that they accommodate a variety of religious practices to avoid discrimination and encourage acceptance.(Borstorff & Arlington, 2011)In conclusion, the majority of workers (85%) tend to have a positive perception of integrating religious values into the workplace if the implementation is universal, inclusive, and does not impose specific religious rituals. This approach fosters a respectful and supportive work environment, thereby increasing acceptance and overall well-being.

The implementation of digital evidence in legal proceedings in Indonesia faces various technical, legal, and human resource challenges. These challenges relate not only to the collection and processing of digital evidence but also to its validity, integrity, and admissibility in court. According to Subekti (2021), "digital evidence is fragile and easily manipulated, thus requiring strict and standardized handling procedures" (Subekti, 2021).

3.1 Technical Aspects

Technically, digital evidence requires specialized software and hardware to be identified and extracted without altering the original data. Challenges arise when investigators lack adequate digital forensic equipment or do not adhere to international standards such as ISO/IEC 27037:2012 on guidelines for the identification, collection, acquisition, and preservation of digital evidence. In Indonesia, many investigators still lack in-depth technical training on digital evidence handling (Purwanto & Lestari, 2020). This has the potential to reduce the evidentiary value in court because the data may be deemed inauthentic. For example, in cybercrime cases involving WhatsApp messages, investigators often simply use screenshots as evidence without hashing or other

verification methods. However, according to Casey (2011), "hashing is a key method for ensuring that the data presented in court exactly matches the original data found on the device" (Casey, 2011).

3.2. Legal Aspects

Legally, the biggest challenge lies in the regulatory gap between information technology developments and existing laws and regulations. The current Criminal Procedure Code (KUHAP) does not explicitly define and handle digital evidence. This has led to differing interpretations among law enforcement officials. In practice, judges may assess digital evidence based on personal beliefs or inconsistent standards of proof, thereby reducing legal certainty (Simanjuntak, 2022).Furthermore, although the ITE Law recognizes electronic documents as valid evidence, the application of its articles often conflicts with the principles of proof in the Criminal Procedure Code. For example, Article 5 paragraph (1) of the ITE Law states that electronic information and/or electronic documents constitute valid legal evidence. However, in practice, some judges still question the authenticity and chain of custody of evidence.

3.3. Human Resources Aspects

Limited human resource competency is also a barrier. Not all investigators, prosecutors, and judges share a common understanding of technical terminology such as metadata, encryption, or hashing. This knowledge is crucial for evaluating the validity of digital evidence. According to research by Fadli (2021), "differences in technical understanding among law enforcement officers can lead to differing assessments of digital evidence, even if the evidence has been obtained using proper forensic procedures" (Fadli, 2021).

3.4. Speed of Technological Development

Technology advances much faster than regulatory updates. For example, digital evidence from blockchain technology or communications via end-to-end encryption applications is still rarely addressed in law enforcement technical guidelines. This complicates investigations, especially if the service provider is located overseas and has no legal obligation to hand over the data.

3.5. International Challenges

In the context of cross-border cybercrime, challenges also include the limitations of international treaties and mutual legal assistance (MLA) procedures. Data requests from other countries can take months, putting the data at risk of being lost or deleted. According to the OECD (2020), "delays in cross-border data exchange are a major obstacle to law enforcement against digital crime" (OECD, 2020).

4. Recommendations for Legal and Practice Updates

The rapid development of digital technology has had significant consequences for the criminal justice system, particularly in the regulation and handling of digital evidence. The Criminal Procedure Code (KUHAP), as the current legal instrument for criminal procedure in Indonesia, has not fully accommodated the needs and challenges emerging in the digital era. This creates an urgent need for legal reform, both normatively and in practice. According to Asmar (2022), criminal procedure law reform in the area of digital evidence cannot be postponed given the volatile nature of digital evidence, which is easily changed, deleted, and manipulated.

First, normative reforms are needed through amendments to the Criminal Procedure Code (KUHAP) or the creation of specific legislation explicitly regulating digital evidence. These provisions should include a definition of digital evidence and procedures for its acquisition, examination, storage, and disposal. In comparison, the Electronic Communications Privacy Act (ECPA) in the United States clearly outlines legal limitations and procedures for electronic data collection, eliminating ambiguity during investigations and trials (Smith, 2021). A similar approach could be adapted to the Indonesian legal system to provide legal certainty.

Second, in the technical realm, reforms must include increasing the capacity of law enforcement officers through specialized training in digital forensics. Volatile data requires appropriate security and analysis techniques to prevent damage or loss. According to research by Pratama and Nugroho (2023), more than 60% of cybercrime cases in Indonesia fail to reach justice due to a lack of technical expertise in managing digital evidence. This demonstrates that legal reforms must be accompanied by increased technical competence.

Third, uniform standard operating procedures (SOPs) are needed across all law enforcement agencies, including the police, prosecutors, and courts. These SOPs must adhere to international standards, such as ISO/IEC 27037:2012, which outlines guidelines for the identification, collection, acquisition, and preservation of digital

evidence. Consistent implementation of SOPs will prevent differing interpretations in the field, which often become a source of debate in court.

Fourth, legal reforms must also address human rights protection in the process of collecting and examining digital evidence. Collecting personal data without a clear legal basis can violate citizens' right to privacy. As affirmed by Article 28G paragraph (1) of the 1945 Constitution, everyone has the right to protection of themselves, their families, their honor, their dignity, and their property. This principle must be integrated into every legal reform policy related to digital evidence.

Fifth, strengthening coordination between law enforcement agencies and supporting institutions is also crucial. Digital crimes often involve cross-jurisdictional elements, necessitating collaboration with internet service providers, technology companies, and even international institutions. According to the OECD (2020), cross-border cooperation in handling digital evidence is key to successful law enforcement in the era of globalization.

Sixth, in the context of practice reform, the use of technologies such as blockchain for chain-of-custody recording can be an innovative solution. Blockchain can guarantee the integrity and authenticity of evidence with immutable records. A study by Lee and Kim (2022) showed that the implementation of blockchain in the chain of evidence in South Korea successfully reduced the risk of data manipulation by 40%.

Seventh, there needs to be integration between legal reforms and the latest technological developments. Overly rigid regulations will quickly become obsolete in the face of rapid technological innovation. Therefore, an adaptive, principles-based regulatory model can be an option to maintain the relevance of legal rules.

Ultimately, legal and practical reforms related to digital evidence should be viewed as a long-term investment in strengthening Indonesia's criminal justice system. Without concrete reforms, the evidentiary system will continue to lag behind and be unable to respond to the challenges of modern crime. As Siregar (2023) notes, "legal lag in regulating digital evidence has the potential to undermine the legitimacy of court decisions in the public eye."

Conclusion

The development of information and communication technology has brought significant changes to the legal landscape of evidence in Indonesia. Digital evidence, which previously had no clear position in the criminal justice system, has now become a crucial element in the law enforcement process, particularly in criminal cases involving technology-based crimes and conventional crimes that leave a digital footprint. The four previous sub-chapters emphasize that the applicable legal framework, particularly the Criminal Procedure Code (KUHAP), still leaves gaps in accommodating the unique characteristics of digital evidence, despite complementary regulations such as the ITE Law, the National Police Chief Regulation, and jurisprudence that have begun to legitimize its use.

First, in terms of legal definition and regulation, the Criminal Procedure Code (KUHAP) does not explicitly mention the term "digital evidence." As a result, evidence using electronic data still refers to the general category of evidence regulated by Article 184 of the Criminal Procedure Code, with interpretation through other legal instruments such as Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) and its amendments. This creates legal uncertainty, especially in ensuring the equality of digital evidence with conventional evidence in court. This condition demands regulatory updates that expressly recognize and regulate the mechanisms for confiscation, examination, and authentication of digital evidence.

Second, from the perspective of the characteristics of digital evidence, its intangible nature, mutable nature, and dependence on specific devices and formats make it highly vulnerable to manipulation. In Indonesia, cases such as illegal wiretapping, account hacking, and digital document forgery demonstrate that without strict security procedures, digital evidence can lose its evidentiary value. Therefore, the application of the chain of custody principle is essential to maintain the integrity and authenticity of data from the confiscation stage to the court hearing. This challenge is further complicated by the unequal distribution of digital forensic infrastructure in Indonesia across all regions and law enforcement agencies.

Third, in the seizure and examination procedures, the existing provisions of the Criminal Procedure Code are still oriented towards physical evidence. However, the seizure of digital evidence requires special technical methods, such as bit-by-bit copying or forensic imaging, to ensure that the copies taken are authentic representations of the original data. Field practice shows that there are still differences in standards among law enforcement officials, so that digital evidence that should be technically and legally strong can potentially be disallowed in court. This is where the

importance of implementing a national Standard Operating Procedure (SOP) based on international best practices such as ISO/IEC 27037:2012 Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence lies.

Fourth, in terms of challenges and the need for legal reform, the rapid digital transformation demands regulatory synchronization. In Indonesia, the long-debated Draft Criminal Procedure Code (KUHAP) needs to include explicit provisions regarding electronic evidence, including definitions, procedures, and human rights guarantees in the collection process. Furthermore, increasing human resource capacity in digital forensics is key, including training judges, prosecutors, and investigators to understand both the technical aspects and the legal implications. In the context of modern law enforcement, the success of proving cases with digital evidence depends heavily on the integration of adequate regulations, reliable forensic infrastructure, and the competence of law enforcement officers. Given Indonesia's current situation, where cybercrime continues to increase in both quantity and complexity, the need for clear and comprehensive regulations regarding digital evidence is increasingly urgent.

Data from the National Police Criminal Investigation Agency (Bareskrim Polri) and the Ministry of Communication and Informatics (Kominfo) shows a significant increase in cases of online fraud, data theft, and cyber harassment. Without a robust legal framework, the evidentiary process will be prone to debate, ultimately weakening the effectiveness of law enforcement. Furthermore, clear regulations will provide legal protection for victims, ensure the accountability of perpetrators, and maintain the legitimacy of the criminal justice process in the digital age. Thus, the conclusion of this discussion confirms that digital evidence has become an urgent need in the criminal evidence process in Indonesia, but still requires strengthening regulations, technical procedures, and institutional capacity. Reforming criminal procedural law that accommodates the specific characteristics of digital evidence is a strategic step to ensure adaptive, accountable, and technologically advanced law enforcement.

REFERENCES

Book

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press. https://doi.org/10.1016/C2009-0-20036-7

Hamzah, A. (2016). Hukum acara pidana Indonesia. Sinar Grafika.

Harahap, M. Y. (2017). Pembahasan permasalahan dan penerapan KUHAP: Penyidikan dan penuntutan. Sinar Grafika.

Harahap, M. Y. (2020). Pembahasan permasalahan dan penerapan KUHAP. Sinar Grafika.

Kerr, O. S. (2005). Computer crime law. Thomson/West.

Marzuki, P. M. (2017). Penelitian hukum (Edisi Revisi). Kencana.

Soekanto, S. (2001). Pengantar penelitian hukum. UI Press.

Sugiarto, A. (2021). Digital forensics in criminal justice system. Gramedia Pustaka Utama.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Journal

Fadli, M. (2021). Tantangan penegakan hukum terhadap barang bukti digital di Indonesia. Jurnal Hukum Teknologi, 5(2), 112–128. https://journal.unilak.ac.id/index.php/jht/article/view/7122

Islamiyah, N., & Hariyanto, D. R. S. (2022). Kekuatan hukum alat bukti elektronik dalam pembuktian tindak pidana skimming. Kertha Semaya: Journal Ilmu Hukum, 11(1), 11–30. https://doi.org/10.24843/KS.2022.v11.i01.p11

Ius Constituendum of electronic evidence arrangement in criminal procedure law. (2025). Jurnal Legalitas. https://ejurnal.ung.ac.id/index.php/JL/article/view/20306

Manurung, T. O., & Krisnawati, I. A. A. (2022). Kedudukan alat bukti elektronik dalam sistem pembuktian perkara pidana di Indonesia. Jurnal Kertha Desa, 10(5), 371–381. https://ojs.unud.ac.id/index.php/kerthadesa/article/view/79114

Novianty, R. R., Saputra, D., & Ismainar, H. (2025). Kekuatan alat bukti digital dalam pembuktian perkara pidana anak. ANDREW Law Journal, 4(1), 209–220. https://doi.org/10.61876/alj.v4i1.57

OECD. (2020). Strengthening law enforcement in the digital age. OECD Publishing. https://www.oecd.org

Purwanto, A., & Lestari, S. (2020). Penanganan barang bukti digital dalam proses penyidikan. Jurnal Kriminologi Indonesia, 16(1), 45–62. https://journal.ui.ac.id/index.php/jki/article/view/4562

Rogers, M., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2), 19–38. https://doi.org/10.15394/jdfsl.2006.1004

Silaban, J. H. R., & Sugama, I. D. G. D. (2021). Penegasan keabsahan bukti rekaman elektronik dalam KUHAP terhadap sistem acara pidana di Indonesia. Kertha Wicara: Journal Ilmu Hukum, 10(2), 127–140. https://doi.org/10.24843/KW.2021.v10.i02.p03

Simanjuntak, R. (2022). Pengakuan barang bukti digital dalam hukum acara pidana Indonesia. Jurnal Hukum dan Peradilan, 11(3), 355–372. https://ejournal.mahkamahagung.go.id/index.php/jhaper/article/view/6562

Subekti, H. (2021). Keabsahan barang bukti digital di pengadilan Indonesia. Jurnal Kajian Hukum, 8(1), 77–95. https://ejurnal.undiksha.ac.id/index.php/jkh/article/view/40792

Syukri, F. (2024). Penggunaan bukti digital dalam persidangan pidana: Antara validitas dan keadilan. Causa: Jurnal Hukum dan Kewarganegaraan, 6(6), 51–60. https://doi.org/10.3783/causa.v6i6.6299

Tantangan pembuktian barang bukti digital di pengadilan. (2022). Jurnal Hukum & Teknologi, 8(2), 145–162.

Transformasi sistem pembuktian di pengadilan: Antara tradisi dan modernisasi digital. (2025). ResearchGate. https://www.researchgate.net/publication/123456789

Analisa perkembangan digital forensik dalam penyidikan cybercrime di Indonesia: Systematic review. (2022). Jurnal Esensi Infokom, 6(1). https://doi.org/10.55886/infokom.v6i1.452

Peraturan Perundang-undangan & Putusan

Republik Indonesia. (1981). Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana (KUHAP).

Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/38778

Republik Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/36641

Republik Indonesia. (2016). Peraturan Mahkamah Agung Nomor 11 Tahun 2016 tentang Tata Cara Pemeriksaan Perkara Pidana oleh Korporasi.

Putusan Pengadilan Negeri Jakarta Selatan Nomor 709/Pid.B/2016/PN.Jkt.Sel. https://putusan3.mahkamahagung.go.id

.