*Journal of Golden Generation Legal Science*
*Volume:2, Nomor: 1, (2026), Januari: 59 - 70*
*Link Publish: https://ejournal.lppnusantara.com/index.php/JGGLS/article/view/71*
*E-ISSN : 3123-2884*

# WHEN DIGITAL FOOTPRINTS ARE NO LONGER VALID: AN ANALYSIS OF DIGITAL FORENSIC EVIDENCE FAILURE IN LEGAL PROCEEDINGS "Study Case: Online Gambling 2020"

**Ashuri [1], Hendratna Mutaqin [2]**
Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Islam Bandung [1,2]
*Corresponding Author: ashuri230368@gmail.com [1], hendratna.mutaqin@yahoo.com [2]*

***Info Artikel***
***Submitted:*** *05 Oktober 2025*
***Revised :*** *11 Oktober 2025*
***Accepted:*** *21 November 2025*
***Published:*** *13 Desember 2025*

***Keywords:*** *Digital Evidence, Digital Forensics, Legal Validity, Chain Of Custody, Data Privacy*

***Abstract***
*The advancement of digital technology has brought significant changes to the legal system, particularly in the use of electronic evidence as a means of proof in court. However, the validity of digital forensic evidence is often questioned due to various technical, procedural, and legal challenges. This study aims to analyze the factors contributing to the failure of digital forensic evidence in legal proceedings and to formulate recommendations for improving its validity. The method used is a Systematic Literature Review (SLR) by examining various academic sources that discuss issues of digital evidence validity, forensic standards, and emerging legal challenges. The results of the study indicate that the failure of digital evidence generally stems from non-compliance in the processes of data collection and preservation with chain of custody standards, insufficient competence of law enforcement officers in digital technical aspects, and conflicts between legal requirements and data privacy regulations, such as the GDPR and CCPA. The case study of online gambling 2020, at the South Jakarta District Court confirms that the absence of forensic verification and chain of custody documentation caused the digital evidence to lose its probative value. Therefore, it is necessary to establish standardized forensic procedures, provide training and certification for law enforcement officials and forensic experts, and develop national guidelines for managing digital evidence aligned with international standards. This research is expected to contribute to strengthening the integrity and validity of digital evidence, thereby enhancing the enforcement of justice in the digital era.*

***Kata Kunci****: Bukti Digital, Forensik Digital, Validitas Hukum, Rantai Pengawasan, Privasi Data*

***Abstrak***
*Kemajuan teknologi digital telah membawa perubahan signifikan pada sistem hukum, khususnya dalam penggunaan bukti elektronik sebagai alat pembuktian di pengadilan. Namun, validitas bukti forensik digital sering dipertanyakan karena berbagai tantangan teknis, prosedural, dan hukum. Studi ini bertujuan untuk menganalisis faktor-faktor yang berkontribusi terhadap kegagalan bukti forensik digital dalam proses hukum dan merumuskan rekomendasi untuk meningkatkan validitasnya. Metode yang digunakan adalah Tinjauan Pustaka Sistematis (SLR) dengan meneliti berbagai sumber akademis yang membahas isu-isu validitas bukti digital, standar forensik, dan tantangan hukum yang muncul. Hasil penelitian menunjukkan bahwa kegagalan bukti digital umumnya berasal dari ketidakpatuhan dalam proses pengumpulan dan pelestarian data dengan standar rantai pengawasan, kurangnya kompetensi petugas penegak hukum dalam aspek teknis digital, dan konflik antara persyaratan hukum dan peraturan privasi data, seperti GDPR dan CCPA. Studi kasus perjudian online 2020, di Pengadilan Negeri Jakarta Selatan menegaskan bahwa tidak adanya verifikasi forensik dan dokumentasi rantai pengawasan menyebabkan bukti digital kehilangan nilai*

*pembuktiannya. Oleh karena itu, perlu untuk menetapkan prosedur forensik yang terstandarisasi, menyediakan pelatihan dan sertifikasi bagi petugas penegak hukum dan ahli forensik, serta mengembangkan pedoman nasional untuk mengelola bukti digital yang selaras dengan standar internasional. Penelitian ini diharapkan dapat berkontribusi untuk memperkuat integritas dan validitas bukti digital, sehingga meningkatkan penegakan keadilan di era digital.*


***Publisher : Lembaga Penerbit Penelitian Nusantara***

## INTRODUCTION

In today's digital era, the advancement of information technology has profoundly transformed almost every aspect of human life, including the field of law and the administration of justice. One of the most notable impacts of this transformation is the growing reliance on digital evidence in both investigations and judicial proceedings. Digital traces obtained from computers, smartphones, social media platforms, and network systems have become crucial tools for uncovering various types of crimes, ranging from online fraud and data theft to large-scale international cybercrimes. Consequently, the ability to obtain, analyze, and validate digital evidence in a legally admissible and forensically sound manner is essential to maintain the integrity and credibility of the justice system.

Despite its significant potential to reveal the truth, digital evidence frequently faces challenges concerning its authenticity and integrity in court. According to the International Association for Computer Investigative Specialists (IACIS, 2020), more than 80% of cases involving digital evidence encounter issues of validity, authenticity, or non-compliance with forensic standards. These problems arise because digital evidence is highly vulnerable to manipulation, alteration, or deletion without leaving visible traces. Moreover, the limited technical understanding among law enforcement officers regarding the proper procedures for collecting, preserving, and authenticating digital data often results in evidence losing its probative value before the court.

A concrete example of this issue can be found in the case of Online gambling case (Juny Maimun, also known as Acong), which was tried at the South Jakarta District Court through Decision Number 624/Pid.Sus/2020/PN JKT.SEL. The court documents revealed that investigators discovered several forms of digital data, including applications, player databases, and electronic transaction records allegedly related to online gambling activities (South Jakarta District Court, 2020). However, the panel of judges did not explicitly clarify whether these data had undergone authentication and digital forensic verification according to international

standards, such as ISO/IEC 27037:2012, which provides guidelines for the identification, collection, acquisition, and preservation of digital evidence (International Organization for Standardization, 2012). In addition, several media reports cited legal experts who argued that the law enforcement process in this case was procedurally flawed, as it failed to meet the formal and material requirements for electronic evidence (JPNN.com, 2020). This indicates weak implementation of the chain of custody principle and the lack of comprehensive forensic documentation to ensure the integrity and authenticity of the digital data presented in court. Consequently, the digital evidence lost its probative strength and was not used as the primary basis for the verdict.

This case exemplifies a broader issue concerning the failure of digital forensic evidence to be recognized and accepted in judicial proceedings, often rooted in errors related to the chain of custody—the process of documenting and tracking evidence from its collection to its presentation at trial. As Casey (2019) explains, the chain of custody is essential to guarantee that digital evidence remains unaltered and uncontaminated throughout handling. Any deviation or negligence in maintaining this documentation can create doubts about the evidence's authenticity and integrity, thereby diminishing its legal weight. Similarly, Karie and Venter (2018) emphasize that the reliability of digital evidence depends on transparent and consistent procedural documentation from acquisition to storage.

Another critical factor undermining the validity of digital evidence is the use of non-standardized forensic software and analytical methods. As Lillis et al. (2016) highlight, reliance on commercial forensic tools without sufficient scientific validation can lead to inaccurate results, particularly in metadata verification and digital timeline reconstruction. Metadata distortion or data loss, whether caused by system errors or human mistakes, often prompts courts to reject digital evidence for failing to meet authenticity and reliability standards (Karie, Kebande, & Venter, 2019). To prevent such outcomes, the consistent application of international forensic standards is essential. The National Institute of Standards and Technology (NIST), for example, through its Special Publication 800-86, underscores the importance of integrating forensic techniques at every stage of incident response, including systematic documentation and preservation of digital evidence (NIST, 2014).

Beyond technical shortcomings, legal and institutional challenges also play a major role in the rejection of digital evidence. Many legal systems, including Indonesia's, continue to adapt to the evolving landscape of digital forensics and electronic evidence. Although Law Number 11 of 2008 on Electronic Information and Transactions (ITE) and its amendments

recognize the admissibility of electronic evidence, inconsistencies in implementation persist. Divergent interpretations among investigators, forensic experts, and judges regarding the procedures for validating digital evidence often lead to disputes and the eventual rejection of evidence in court. This underscores the urgent need for harmonization between legal frameworks and technological standards to ensure consistent and fair treatment of digital evidence.

The role of digital forensic experts is therefore crucial in bridging the gap between the technical and legal domains. These professionals are responsible not only for identifying and analyzing digital evidence but also for ensuring that every investigative process complies with the principles of integrity, authenticity, and reliability. In this regard, collaboration among information technology specialists, forensic auditors, and law enforcement authorities is vital to the effective presentation of evidence. Moreover, enhancing human resource capacity through internationally recognized training and certification in digital forensics is essential to ensure professional, credible, and legally defensible evidence-handling practices.

Based on these considerations, this study aims to explore the factors contributing to the failure of digital forensic evidence in legal proceedings and to analyze practical solutions to strengthen its authenticity and integrity. Furthermore, this research seeks to provide recommendations for policymakers, law enforcement agencies, and forensic practitioners to develop more effective, adaptive, and standardized evidence-handling procedures. By integrating legal, technical, and ethical dimensions, it is expected that digital evidence can be optimized as a legally valid, accurate, and reliable instrument for achieving justice in the modern digital era.

## LITERATURE REVIEW

Digital forensic evidence refers to information obtained from electronic devices such as computers, mobile phones, or network systems, which can be used as proof in legal proceedings. According to Kahn et al. (2019), digital evidence encompasses various types of data, including emails, text messages, metadata, audio recordings, and traces of social media activity that may reflect an individual's digital behavior. For such evidence to be admissible in court, it must meet the standards of authenticity, integrity, relevance, and reliability as outlined in the Digital Evidence Standards Framework (Casey, 2019). Sweeney (2021) emphasizes that one of the main reasons for the rejection of digital evidence in court is the lack of understanding

among law enforcement officials regarding proper digital forensic procedures, particularly concerning the chain of custody and validation of analytical tools. This issue is further exacerbated by the absence of uniform implementation of international standards such as ISO/IEC 27037:2012, which governs the identification, collection, and preservation of digital evidence (International Organization for Standardization [ISO], 2012).

According to Reith et al. (2022), errors in the documentation process, such as changes in file access timestamps or mismatched hash values, can render evidence invalid because its integrity cannot be guaranteed. Furthermore, Maras (2020) argues that additional challenges arise from technological aspects, such as the use of end-to-end encryption and cloud-based storage systems, which may hinder the authentication process and the tracing of data sources. In the context of Indonesian law, Setiadi (2021) notes that gaps still exist in the understanding of law enforcement officers regarding digital forensic principles, particularly in distinguishing between legally admissible electronic evidence and mere screenshots without technical verification.

The effectiveness of digital forensic evidence largely depends on compliance with applicable technical and legal procedures. Evidence obtained without proper consideration of authenticity, integrity, and the chain of custody may be rejected by the court, even if it contains material truth. This underscores that the success of digital forensics is determined not only by technological sophistication but also by legal awareness and professional ethics among investigators. Moreover, Smith (2020) highlights that legal challenges related to privacy and personal data protection often become major obstacles in the use of digital evidence. This aligns with Casey's (2019) view that the process of digital data acquisition often intersects with individual constitutional rights; therefore, any act of seizure or analysis must adhere to the principles of legality and proportionality. On the other hand, Reith et al. (2022) explain that technological developments such as cloud computing, encrypted communications, and the Internet of Things (IoT) further complicate digital evidence handling, as data are not always stored within a single jurisdiction and may be easily modified. Therefore, the consistent application of international standards such as ISO/IEC 27037:2012 is essential to ensure the credibility of digital evidence in court.

Overall, the success of digital forensic-based evidence depends not only on the advancement of technology used but also on the competence of forensic experts, sufficient legal understanding, and the consistent implementation of standardized procedures.

## RESEARCH OF METODOLOGY

This study adopts the Systematic Literature Review (SLR) method, which aims to identify, evaluate, and synthesize prior research relevant to a specific topic in a systematic and transparent manner (Kitchenham & Charters, 2007). The SLR approach provides a structured framework to collate evidence across multiple disciplines, enabling researchers to critically assess the quality, reliability, and relevance of existing studies. This method was particularly suitable for investigating digital evidence failures in legal proceedings because the topic spans diverse domains, including law, criminology, information technology, and digital forensics. By systematically reviewing peer-reviewed articles, legal case studies, technical reports, and international standards, the study seeks to capture both theoretical perspectives and practical challenges. Furthermore, SLR facilitates the identification of research gaps, methodological inconsistencies, and emerging trends, which can inform evidence-based recommendations for improving the validity and admissibility of digital forensic evidence. Through this rigorous approach, the study ensures that conclusions are grounded in a comprehensive understanding of prior knowledge while maintaining transparency and reproducibility in the research process.

## DISCUSSION

The case of Juny Maimun, also known as Acong, which was tried at the South Jakarta District Court through Decision Number 624/Pid.Sus/2020/PN JKT.SEL, reveals a crucial issue in the application of digital evidence as admissible proof in criminal proceedings. Based on the court documents, investigators had in fact discovered various forms of digital data, such as applications, player databases, and electronic transaction records, which were strongly suspected to be connected to online gambling activities. However, the panel of judges did not explicitly explain the process of authentication and digital forensic verification of these pieces of evidence, raising doubts about the validity and integrity of the data presented.

The absence of clarification regarding the technical standards for collecting and preserving digital evidence, as stipulated in the international guideline ISO/IEC 27037:2012, indicates that the evidentiary process did not fully comply with the globally recognized principle of forensic soundness. Furthermore, legal experts' criticism that the law enforcement process against Juny Maimun was procedurally flawed reinforces the indication of a weak chain of custody and the lack of systematic forensic documentation to maintain the authenticity of the digital data.

As a result, the digital evidence in this case lost its probative value and was not used as a primary basis in the judges' legal considerations. This situation illustrates that digital evidence is highly vulnerable to legal rejection if it is not supported by standardized forensic procedures and robust regulatory frameworks. Therefore, it is essential to establish national standards for digital forensics and enhance the competence of law enforcement officers so that the process of electronic evidence examination in Indonesia can comply with the principles of evidentiary validity as regulated in Law Number 11 of 2008 on Electronic Information and Transactions (ITE) and Government Regulation Number 82 of 2012 on the Implementation of Electronic Systems and Transactions.

In today's hyperconnected digital era, digital forensic evidence plays a crucial role in the adjudication of legal cases, whether in criminal, civil, or cyber domains. However, the validity and admissibility of digital evidence cannot always be guaranteed due to the complex and error-prone processes of collection, storage, and analysis. Failures in maintaining the integrity of digital evidence often lead to its rejection in court, thereby hindering the pursuit of justice. Therefore, it is essential to comprehensively examine the factors contributing to the failure of digital evidence in order to formulate effective strategies for improvement within modern judicial systems.

One of the primary causes of digital forensic evidence failure lies in data collection processes that do not comply with forensic standards. Evidence gathered without adherence to the chain of custody principle may result in altered metadata, corrupted files, or even physical damage to storage media. In United States v. McGowan (2018), for instance, the court rejected digital evidence because data extraction from a storage device did not follow proper forensic procedures. This ruling demonstrates that negligence during the early stages of investigation can be fatal to the admissibility of evidence, even when it is substantively relevant to the case.

Empirical findings reinforce the urgency of this issue. According to Wiggins (2022), approximately 70% of cases involving digital evidence encounter similar challenges, where non-standardized collection procedures compromise data integrity. This highlights the weak implementation of international standards such as ISO/IEC 27037:2012, which regulates the identification, acquisition, and preservation of digital evidence. Moreover, discrepancies among forensic tools and the limited competence of investigators increase the likelihood of extraction errors. Thus, technical aspects not only affect evidentiary quality but also the credibility of law enforcement institutions in handling digital crimes.

In addition to technical barriers, the knowledge and understanding of legal practitioners significantly influence the admissibility of digital evidence. Johnson (2021) revealed that many judges and lawyers lack a sufficient understanding of digital evidence mechanisms, such as encryption systems, activity logs, and hash verification. As a result, they struggle to determine whether evidence meets the principles of authenticity and integrity. In People v. McGhee (2019), valid digital evidence was dismissed because the judge deemed the data collection method unreliable, despite the issue stemming from a misunderstanding of technical processes. This phenomenon highlights the need to enhance digital literacy among judicial authorities.

To bridge this gap, collaboration among digital forensic experts, investigators, and legal practitioners is vital. Continuous training on digital investigation techniques, management of the digital chain of evidence, and implementation of international standards can enhance professionalism and minimize procedural errors. Institutions such as the International Association of Computer Investigative Specialists (IACIS) and the National Institute of Standards and Technology (NIST) provide training guidelines that can be adapted by law enforcement agencies globally. Hence, strengthening human resource capacity remains a key factor in ensuring the admissibility of digital evidence in court.

Beyond technical and competency-related issues, legal concerns surrounding privacy also present significant challenges in the use of digital evidence. Regulations such as the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR) impose strict limitations on the collection and processing of personal data. The case of R. v. Spencer (2019) illustrates how evidence obtained from social media was deemed a violation of individual privacy rights, despite its legal relevance. According to the European Union Agency for Fundamental Rights (2020), more than 60% of digital evidence cases in Europe face obstacles due to conflicts between investigative needs and data protection rights.

This underscores the importance of achieving a proportional balance between law enforcement objectives and the protection of digital human rights, particularly in safeguarding privacy and personal freedoms in cyberspace. As the complexity of digital crimes increases, legal systems face a growing dilemma between accessing personal data for investigative purposes and protecting citizens' privacy rights as mandated under the GDPR and CCPA (European Union Agency for Fundamental Rights, 2020; Smith, 2020). Imbalances in the application of these principles may lead to violations of digital rights and diminish the legitimacy of judicial processes.

The failure of digital forensic evidence in judicial proceedings fundamentally results from the interaction of multiple interrelated factors. Technical issues include errors in data acquisition and preservation, while procedural problems involve weak implementation of the chain of custody and inadequate documentation (Karie & Venter, 2018). On the other hand, limited professional competence and insufficient training among investigators, prosecutors, and judges increase the risk of misinterpretation in court (Johnson, 2021). Legal frameworks that have not fully adapted to technological developments also contribute to inconsistencies in evaluating the admissibility of digital evidence across jurisdictions (Casey, 2019; Wiggins, 2022).

Addressing these challenges requires a holistic approach that integrates technological, legal, and ethical dimensions within digital forensic practice. This approach emphasizes the adoption of international standards such as ISO/IEC 27037:2012 on the identification, collection, acquisition, and preservation of digital evidence, as well as the NIST Special Publication 800-86, which outlines the integration of forensic techniques into incident response (NIST, 2014; International Organization for Standardization, 2012). Through the consistent application of these standards, law enforcement agencies can ensure that every piece of digital evidence is obtained and maintained lawfully, systematically, and verifiably.

Furthermore, enhancing human resource capacity should be a top priority. Law enforcement officers, investigators, and digital forensic experts must receive continuous training in encryption technologies, data recovery, log analysis, and metadata verification. Such training not only strengthens technical competence but also reinforces ethical understanding and professional responsibility in maintaining data integrity (Rogers & Seigfried-Spellar, 2020). Additionally, professional certifications such as those offered by the International Association of Computer Investigative Specialists (IACIS) can serve as benchmarks of competence in this field.

In the long term, multidisciplinary collaboration among legal scholars, information technology academics, and forensic auditors should be reinforced to build a credible and adaptive digital evidentiary system. Such collaboration can foster the creation of national regulations aligned with global standards while accommodating emerging issues such as artificial intelligence (AI), blockchain forensics, and cloud-based analysis (Lillis et al., 2016; Karie, Kebande, & Venter, 2019). Therefore, digital evidence should not only function as a legitimate and reliable tool of proof but also as an instrument of justice that upholds the

principles of transparency, accountability, and digital human rights within the modern legal landscape.

## CONCLUSION

This study concludes that the failure of digital forensic evidence in legal proceedings is caused by several interrelated factors, including errors in data collection methods, limited technical understanding among law enforcement officers, and legal obstacles related to data privacy protection. The case of online gambling 2020, demonstrates that the weak implementation of the chain of custody principle and the absence of standardized forensic verification resulted in the loss of the probative value of digital evidence in court. To improve the validity of digital evidence, it is necessary to strengthen professional capacity through regular training, competency certification for investigators and forensic experts, and the implementation of standardized technical guidelines for the collection and analysis of evidence. In addition, harmonization between legal regulations and international technical standards must be established to ensure that digital evidence can be legally admissible in court. By reinforcing procedural, technical, and human resource aspects, digital forensic evidence can play a more effective role in supporting justice and law enforcement in the digital era.

## RECOMMENDATIONS

1. Strengthen law enforcement competence through regular training on digital evidence handling, including chain of custody, encryption, and hash data validation.
2. Require certification for investigators and digital forensic experts to ensure measurable professional competence.
3. Utilize internationally certified forensic tools (e.g., FTK, EnCase, Autopsy) and ensure all processes are digitally documented to maintain evidence integrity

## REFERENCES

Casey, E. (2019). Digital evidence and computer crime: Forensic science, computers, and the Internet (4th ed.). Academic Press.

European Union Agency for Fundamental Rights. (2020). Data Protection and Privacy in the Digital Age.

IACIS. (2020). Digital Evidence and the Law: A Comprehensive Guide. International Association for Computer Investigative Specialists.

International Association for Computer Investigative Specialists. (2020). Annual report on digital evidence admissibility challenges. IACIS Publications.

International Organization for Standardization. (2012). ISO/IEC 27037:2012 – Guidelines for identification, collection, acquisition, and preservation of digital evidence. ISO Standards.

Johnson, P. (2021). "Legal Professionals and Digital Evidence: A Skills Gap." The Legal Profession Review, 29(4), 78-95.

Kahn, R., Smith, J., & Lee, T. (2019). "The Role of Digital Evidence in Modern Legal Proceedings." Journal of Digital Forensics, Security and Law, 14(2), 45-62.

Karie, N. M., & Venter, H. S. (2018). Taxonomy of challenges for digital forensic investigation. Digital Investigation, 24, 1–11.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. Computer Science Review, 22, 35–49.

National Institute of Standards and Technology (NIST). (2014). Guide to integrating forensic techniques into incident response (NIST SP 800-86). U.S. Department of Commerce.

Rogers, M. K., & Seigfried-Spellar, K. C. (2020). Digital forensics and investigations: People, process, and technologies to defend the enterprise. CRC Press.

Smith, A. (2020). "Privacy Concerns in Digital Evidence Collection." Harvard Journal of Law & Technology, 33(1), 123-145.

Sweeney, L. (2021). "Challenges in Digital Evidence Admissibility." Forensic Science International, 320, 110701.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58.

Wiggins, J. A. (2022). The integrity dilemma in digital forensics: Challenges in evidence collection and preservation. Forensic Science International: Digital Investigation, 40, 301–312. https://doi.org/10.1016/j.fsidi.2022.301312

International Organization for Standardization. (2012). *ISO/IEC 27037:2012—Information technology—Security techniques—Guidelines for identification, collection, acquisition, and preservation of digital evidence.* Geneva, Switzerland: ISO.

JPNN.com. (2020, January 14). *Criminal law expert says the legal action against Juny Maimun is procedurally flawed.* Retrieved from https://www.jpnn.com/news/ahli-pidana-sebut-proses-penindakan-terhadap-juny-maimun-cacat-hukum

South Jakarta District Court. (2020). *Decision Number 624/Pid.Sus/2020/PN JKT.SEL.* Retrieved from https://putusan3.mahkamahagung.go.id

Republic of Indonesia. (2008). *Law Number 11 of 2008 concerning Electronic Information and Transactions.* State Gazette of the Republic of Indonesia Year 2008 Number 58.

Republic of Indonesia. (2012). *Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions.* State Gazette of the Republic of Indonesia Year 2012 Number 189.