International Journal of Law Analytics (IJLA)
Vol. 4, No. 2 2026: 297-308

The Investigation and Inquiry Process for Uncovering Online Gambling Cases Under the ITE Law: A Technical and Legal Analysis of Digital Forensic Evidence

Muhammad Arief[1*], Ida Hanifah[2]
Universitas Muhammadiyah Sumatera Utara
m.arief08@gmail.com, idahanifah@umsu.ac.id
Corresponding Author: Muhammad Arief m.arief08@gmail.com

A R T I C L E I N F O

Keywords: Online Gambling, Investigation, Inquiry, Digital Forensics

Received : 24, January
Revised : 26, March
Accepted: 28, May

A B S T R A C T

This study aims to analyze the process of investigating and prosecuting online gambling crimes under the Electronic Information and Transactions Law (EIT Law), as well as to examine the role of digital forensics in evidence gathering from both technical and legal perspectives. This study employs a normative-empirical legal method using legislative, conceptual, case-based, and sociological-legal approaches. Data was obtained through a literature review of legislation, journals, books, and other legal materials, and supplemented with field data regarding law enforcement practices. The research findings indicate that the investigative and prosecutorial processes for online gambling cases fundamentally have a sufficient legal foundation; however, in practice, they still face various obstacles, such as the anonymity of perpetrators, the use of foreign servers, difficulties in digital evidence collection, and limitations in the resources and technical capabilities of law enforcement officials.

DOI: https://doi.org/10.59890/ijla.v4i2.199
ISSN-E: 3032-4041
https://journal.multitechpublisher.com/index.php/ijla/index

INTRODUCTION

The development of information and communication technology has had a significant impact on various aspects of modern society's life. Digital transformation opens up wider access to internet-based information, entertainment, and services, but at the same time also creates new space for the emergence of technology-based crime. One form of cybercrime that has increased drastically is online gambling. This activity is no longer traditional, but utilizes digital platforms such as websites, mobile applications, and social media, making it more accessible to people from various walks of life, including teenagers.

Online gambling is growing rapidly because it offers ease of access, anonymity, a digital payment system, and aggressive promotions through advertising and affiliate networks. These conveniences make gambling practices increasingly difficult to control, often even operating using overseas servers, making it difficult to be tracked by law enforcement officials. As a result, the number of public participation in online gambling is increasing, and this crime has become one of the cybercrimes with the highest number of reports in recent years.

The impact is not only economic, such as financial losses, fraud, and illegal fund flows, but also has a wide impact on the social conditions of the community. Many cases show that online gambling addiction triggers psychological disorders, domestic conflicts, continued criminal acts (such as theft or fraud to meet gambling needs), and family bankruptcy. In addition, online gambling practices are also often part of organized crime networks involving money laundering activities, digital identity trading, and the exploitation of banking systems and e-wallets.

With this complexity, online gambling can no longer be seen as a minor offense, but rather as a cybercrime that is structured and has a multidimensional impact. Therefore, law enforcement efforts require a more comprehensive approach, not only based on juridical aspects, but also through technological analysis, strengthening forensic digital capacity, and updating investigative strategies in the cyber domain.

The handling of online gambling poses a major challenge for law enforcement officials, especially at the investigation and investigation stages:

a. Jurisdictional Issues: Gambling servers are often located overseas, complicating the law enforcement process and requiring international cooperation (Mutual Legal Assistance).
b. Digital Evidence Issues: Digital evidence is volatile (easily lost/changeable) and requires specialized expertise (digital forensics) to be acquired, analyzed, and validated to be valid as evidence in court.
c. Anonymity of Actors: Actors often use VPNs, proxies, cryptocurrencies, and anonymous networks that make identity tracking difficult.

In the context of Indonesian law, online gambling is expressly qualified as a criminal offense that violates Article 27 paragraph (2) of Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) as amended by Law Number 19 of 2016. This section prohibits any person from distributing, transmitting, or making accessible electronic information that has a gambling

content. Thus, all activities of organizing, promoting, or participating in gambling through digital media are in the category of violations of the law that can be subject to criminal sanctions.

Although the legal provisions are obvious, law enforcement against online gambling presents much more complex challenges when compared to conventional gambling crimes. This is due to the nature of cybercrime that is not limited by time and space, as well as the use of advanced technology by perpetrators to hide identities, server locations, and financial transaction flows. Online gambling operators generally use anonymity technologies such as VPNs, IP (proxy server) disguise, and the use of overseas servers to avoid detection. Meanwhile, users are often connected to the platform through private networks and digital accounts that are difficult to verify directly.

In terms of the law enforcement process, the investigation and investigation of online gambling cases requires adequate technical capabilities, including in terms of digital trace tracing, metadata analysis, electronic data security, and mapping digital relationships between perpetrators. Investigators must master a variety of digital forensic techniques to ensure that electronic evidence—such as chats, transaction screenshots, digital activity recordings, server logs, and payment histories can be obtained legally, has integrity, and has the power of proof in court.

Furthermore, the complexity of proof in online gambling cases is also influenced by the nature of electronic information that is easily manipulated, deleted, or encrypted. Therefore, investigations and investigations require cross-sector cooperation, including digital platform providers, banks, electronic payment service providers (e-wallets), and telecommunications authorities. The need for a multidisciplinary approach is what makes proving online gambling cases more technical, more sensitive, and demanding high precision to ensure the fulfillment of juridical aspects in accordance with the provisions of criminal procedure law.

This complexity arises because gambling activities are carried out in a digital space that is anonymous, cross-border, and utilizes encryption technology, making it difficult for law enforcement officials to identify the perpetrators directly. Therefore, the success of the disclosure of online gambling cases is highly dependent on mastery of digital forensic techniques, ranging from digital footprint tracking, analysis of electronic devices, identification of servers and electronic fund flows, to recovery and authentication of digital data as evidence.

In addition to the technical aspects, the investigation process of online gambling cases also faces juridical issues that are no less complex. One of the main challenges is to ensure the legality of the electronic evidence used in the evidentiary process. In Indonesian criminal procedure law, electronic evidence is recognized as valid evidence as stipulated in Article 5 of the ITE Law. However, this acknowledgment must still meet the formal and material requirements, namely that the evidence is obtained in a way that is legal, relevant, and accountable for its integrity. Failure to meet these requirements may result in evidence being considered legally defective and cannot be used at trial.

The next problem is related to the procedure for confiscating and securing digital devices, such as mobile phones, computers, servers, and storage media. The seizure of digital devices must be carried out based on a valid warrant, clear procedures, and forensic examinations in accordance with operational standards. Investigators should not conduct arbitrary data examinations because it can be considered a violation of procedural law and has the potential to damage the integrity of evidence. Small mistakes such as opening an app without forensic procedures or turning on a device without proper technique can change the data structure and remove the important digital footprint required in the proofing process.

In addition, the implementation of the chain of custody or the chain of control of evidence is a crucial aspect in proving technology-based crimes. Every transfer of evidence from one party to another must be recorded in detail, complete with information on the identity of the officer, time, location, and condition of the evidence. Without a well-documented chain of control, the defendant or his legal counsel can sue the validity of the evidence on the grounds of potential manipulation, contamination, or alteration of data. In the context of electronic evidence that is highly susceptible to alteration or removal, the precision in maintaining the chain of custody is a major factor determining the strength of the evidence.

Not only that, the investigation process must also comply with the evidentiary standards stipulated in the Criminal Procedure Code and the special provisions of the ITE Law. Investigators must be able to show the relationship between digital evidence and the alleged legal subject, including proving that the device used was actually controlled and operated by the suspect. This standard of proof often poses its own challenges when perpetrators use undercover technology, fictitious accounts, or foreign servers, requiring more in-depth forensic digital analysis expertise.

Thus, the success of the investigation and prosecution of online gambling cases is highly dependent on the accuracy of the simultaneous application of juridical and technical procedures. Errors in any one aspect alone can have a serious impact on the validity of the evidence and potentially thwart law enforcement efforts.

Seeing this phenomenon, it is important to conduct a comprehensive scientific study on how the investigation and investigation process of online gambling crimes is carried out, as well as how digital forensics play a role in proving the involvement of perpetrators technically and juridically. The complexity of cybercrime requires law enforcement officials to not only understand the normative aspects, but also master digital investigative techniques that are in accordance with international standards. Therefore, research on the work mechanism of investigators, electronic evidence collection methods, and forensic digital analysis procedures is very relevant in ensuring the effectiveness of law enforcement.

This study is also needed to identify the extent to which digital technology is optimally used in proving criminal acts, including in the process of disclosing the network structure of online gambling operators, financial transaction flows,

digital communications, and user activities on these illegal platforms. In addition, this study will examine the suitability of investigation practices with positive legal provisions such as the Criminal Code, the ITE Law, the Police Law, and technical rules regarding digital forensics. This evaluation is important to ensure that the evidence obtained is not only technically accurate but also legally valid and has strong evidentiary value at trial.

Furthermore, this study is expected to be able to provide a comprehensive overview of the various obstacles that arise in the investigation and investigation of online gambling cases, both technical ones—such as data encryption, overseas servers, or the use of anonymous accounts—as well as juridical obstacles, such as differences in interpretation of electronic evidence and procedures for confiscating digital devices. The findings of this study will serve as a basis for formulating strategic recommendations to improve the quality of law enforcement in the field of cybercrime, including increasing the capacity of law enforcement human resources, updating regulatory tools, and strengthening collaboration between agencies.

This study aims to critically examine whether the existing investigation and investigation procedures (based on the Criminal Procedure Code and the ITE Law) are adequate to uncover online gambling crimes. The main focus is to examine APH's ability to adopt digital forensics techniques in accordance with international standards, as well as the juridical challenges in recognizing and proving the validity of digital evidence at trial. Thus, this research is expected to make an academic and practical contribution to strengthening the technology-based law enforcement process, especially in the eradication of online gambling which is increasingly growing and increasingly difficult to handle without a modern, professional, and legal standard digital investigation strategy.

THEORETICAL REVIEW

Research on the handling of online gambling crimes indicates that advancements in information technology have presented new challenges for law enforcement agencies, particularly in the process of investigations based on digital evidence. According to various studies, the Electronic Information and Transactions Law (EIT Law) serve as the primary legal framework for prosecuting cybercriminals, including those involved in online gambling, although its implementation still faces challenges regarding evidence and jurisdiction. Other literature emphasizes that digital forensics plays a crucial role in identifying, collecting, and analyzing electronic evidence in a manner that is legally valid and admissible in court. Furthermore, previous research also underscores the importance of chain-of-custody procedures to maintain the authenticity and integrity of digital evidence throughout the legal process. On the other hand, some studies have criticized the limited technical capacity of law enforcement officials and the lack of specific technical regulations for addressing cross-border online gambling crimes. Therefore, integration between digital forensic technical approaches and a comprehensive legal framework is necessary to enhance the effectiveness of investigative and prosecutorial processes in uncovering online gambling cases under the ITE Law.

METHODOLOGY

This study uses a type of normative-empirical legal research, which is a mixed approach that combines analysis of written legal norms with the study of their application in practice. This approach was chosen because the problems studied are not only at the regulatory level, but also related to how the legal provisions are implemented in the field by law enforcement officials.

From the normative side, the research examines various laws and regulations, doctrines, and legal principles that are the basis for resolving cases, including provisions on investigator authority, the principle of restorative justice, and the regulation of conflict resolution mechanisms in the criminal justice system. Normative analysis also aims to assess the suitability between the investigator's actions and the applicable positive legal provisions.

Meanwhile, from the empirical side, the research examines the facts that occur in the field through interviews, observations, and analysis of case documents. Empirical research focuses on the behavior of law enforcement officials, community responses, social dynamics, and practical barriers in implementing legal provisions. Through this approach, research can show whether the rule of law has been applied effectively, consistently, and in accordance with the purpose of its formation.

By combining these two approaches, normative-empirical legal research allows researchers to see the gap between ideal law (das sollen) and practical law (das sein), while providing a comprehensive picture of the effectiveness of applying legal norms in actual social contexts. This blended approach is particularly relevant for examining legal issues that require theoretical and practical understanding at the same time.

a. Normative Law: Analyzing related regulations, namely Law Number 11 of 2008 jo. Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE), KUHAP, and Regulation of the Chief of Police on the investigation of cyber crimes.
b. Empirical Law: Collect field practice data on the challenges and procedures used by law enforcement officials, especially the Police's cyber unit, in tracking and collecting digital evidence of online gambling cases.

In normative-empirical legal research, the research approach used is combinative because it combines the study of written legal norms with the reality that occurs in the field. Therefore, this study uses several approaches as follows:

a. Statute *Approach*. This approach is used to examine various legal provisions that govern research topics. The researcher examines relevant laws and regulations, ranging from laws, government regulations, to other implementing regulations. This approach is important to know how positive law governs the object of research as well as the applicable limitations, authorities, and procedures. Analyze the formulation of the criminal articles *of online gambling* (Article 27 paragraph 2 of the ITE Law) and their relevance to proof in the digital era.
b. Conceptual Approach. This approach is used to understand the legal concepts that are the basis of analysis, such as the concept of investigation, investigation, evidence, and the concept of criminal responsibility. Through this approach, the researcher uses legal theories from experts as a basis for building arguments. Analyze the concepts of *digital evidence*, chain *of custody*, and *cyber jurisdiction*.
c. Case Approach. The case approach is used to examine court decisions or concrete cases related to the object of research. Through this approach, researchers can see how the application of the law in practice, the pattern of judges' considerations, and the development of legal interpretation by law enforcement officials. Examining court decisions or major *cases of online gambling* as an illustration of the obstacles and success of the investigation.
d. Socio-Legal *Approach*. This approach is used to obtain data directly from the field through interviews, observations, or documentation of related parties (investigators, prosecutors, forensic experts, and others). The purpose of this approach is to understand how legal provisions are implemented in practice, the barriers faced, and the factors that affect the effectiveness of law enforcement. Examine how the legal norms of Diversion are accepted and implemented by the community (victims, children's families) and law enforcement officials in the field.

The sums of data used are as follows:

a. Primary Data: *In-depth interviews* with cyber crime investigators/Cyber Crime Directorate, digital forensic experts, and Public Prosecutors handling ITE cases.
b. Secondary Data: Primary Legal Materials (ITE Law, Criminal Procedure Code), Secondary Legal Materials (scientific journals, cyber law books), and Tertiary Legal Materials (institutional reports, *police standard operating procedures*).
c. Tertiary legal materials are legal materials that function as instructions or complements derived from dictionaries, encyclopedias, magazines, newspapers and so on.

The technique of collecting legal materials is carried out through library research, namely by collecting, reading, and reviewing laws and regulations, legal literature, and court decisions related to the object of research.

The analysis of legal materials in this study is carried out qualitatively, namely by debunking, connecting, and interpreting existing legal norms to answer the formulation of problems. The analysis was carried out by the method of grammatical, systematic, and teleological legal interpretation of the provisions that regulate illegal content on social media.

RESEARCH RESULTS AND DISCUSSION

Investigation and Investigation of Online Gambling Cases by Cyber Crime Investigators

Based on the results of the research, the handling of online gambling cases by cyber-crime investigators is basically carried out through two main stages, namely investigation and investigation. At the investigation stage, law enforcement officials first identify suspected criminal acts through public reports, cyber patrols, site searches, social media, promotional accounts, and digital transaction activities that lead to online gambling practices. In this stage, investigators seek to find the existence of a criminal event and gather preliminary information about operational patterns, accounts used, and possible parties involved.

After an alleged criminal act was found, the process continued to the investigation stage. At this stage, investigators carry out legal actions such as examining witnesses, summoning related parties, confiscating electronic devices, securing digital accounts and transactions, as well as tracing the relationship between perpetrators, devices, and fund flows. In the case of online gambling, investigations are not enough to be carried out with conventional approaches, because perpetrators generally utilize anonymous accounts, loan accounts, and digital networks spread across various platforms.

The main challenge in this process lies in the issue of jurisdiction and anonymity of the perpetrator. Many online gambling sites use foreign servers, foreign domains, and digital payment systems that are not fully within the reach of national law. Additionally, perpetrators often use VPNs, fake accounts, virtual numbers, and other parties' identities to disguise their existence. This condition causes investigators not only to have to prove the existence of gambling activities, but also to be able to connect those digital activities with the responsible legal subjects.

According to the author's analysis, the stages of investigation and investigation in online gambling cases basically have a sufficient legal basis, but their effectiveness still depends heavily on the ability of investigators to adjust working methods to the characteristics of cybercrime. In this context, online gambling investigations cannot only rely on a formal procedural approach, but must be supported by digital tracing capabilities, account analysis, and electronic network mapping in a more modern and integrated manner.

The Role and Stages of Digital Forensics in Electronic Evidence Collection

Based on the results of the research, digital forensics has a very important role in the disclosure of online gambling cases, because the proof of this case relies on electronic evidence such as mobile phones, laptops, digital conversations, screenshots, transaction history, e-wallet accounts, metadata, and system activity logs. In online gambling cases, digital forensics functions to find, secure, examine, and analyze digital evidence so that it can be used legally in the judicial process.

In general, the stages of digital forensics include identification, preservation, acquisition, analysis, and reporting. At the identification stage, investigators determine digital devices or accounts that are suspected of being related to criminal acts. Furthermore, at the security stage, electronic devices and data must be kept from altering, erasing, or contaminating. After that, forensic data acquisition is carried out, which is taking copies of data without changing the original data. The next stage is the analysis of the device's content, digital communication, access history, and transaction patterns. The results of the examination are then stated in a forensic report to support the evidence in court.

In order for electronic evidence to have legal force, the evidence must meet formal and material requirements. Formal requirements are related to the way they are obtained, which must be obtained legally and through the correct legal procedures. Meanwhile, material requirements are related to the authenticity, integrity, relevance, and relevance of the data to the criminal act being examined. Therefore, in practice, the existence of a chain of custody or a chain of custody of evidence is also very important to ensure that evidence does not change from being secured to being submitted at trial.

According to the author's analysis, digital forensics is a very decisive element in proving online gambling crimes. Without proper forensic processes, digital evidence such as screenshots, chats, and transaction history will be easily debated for its validity. Thus, digital forensics not only serves as a technical tool, but also as a legal evidentiary instrument that ensures that electronic evidence is admissible and has strong evidentiary value in court.

Juridical and Technical Constraints and Solution Strategies in Online Gambling Law Enforcement

Based on the results of the research, the obstacles faced by law enforcement officials in uncovering online gambling cases can be divided into juridical obstacles and technical obstacles. From a juridical perspective, the main obstacle lies in proving the relationship between digital accounts, devices, electronic transactions, and the actual perpetrators. Although electronic evidence has been recognized in Indonesian law, the practice of proof still demands high scrutiny as perpetrators often use fake identities, third-party accounts, and fragmented transaction systems.

From the technical side, the main obstacles include the nature of digital evidence that is easily deleted, modified, or encrypted, the use of VPNs and anonymous accounts by perpetrators, limited digital forensic means, and the uneven capacity of human resources of the apparatus in handling electronic evidence. In addition, the large volume of data in digital devices also often makes it difficult to select and analyze data that is really relevant to the case.

To overcome these obstacles, strategies that can be implemented include increasing the capacity of investigators in the cyber sector, standardizing procedures for handling digital evidence, strengthening cross-sector cooperation, and optimizing international cooperation in tracing servers, accounts, and cross-border fund flows. In addition, the follow the money approach is also very relevant in online gambling cases, because tracking financial transactions is often more effective in uncovering the perpetrator's network than relying solely on tracking digital accounts.

According to the author's analysis, the biggest obstacle in law enforcement against online gambling lies not only in the difficulty of finding the perpetrators, but in the fact that the conventional criminal proof system has to deal with crimes that are digital, anonymous, and cross-border. Therefore, law enforcement strategies must be directed at strengthening digital investigation capabilities, forensic-based evidence, and inter-agency collaboration so that the handling of online gambling cases does not stop at site blocking, but is able to reach operators, fund flows, and crime network structures as a whole.

CONCLUSIONS AND RECOMMENDATIONS

Based on the results of the research, it can be concluded that the investigation and investigation of online gambling crimes has basically been carried out in accordance with applicable legal procedures, but in practice it still faces various obstacles, especially because of the anonymous, cross-border, and technology-based nature of this crime. Investigators are not only required to understand legal aspects, but also must be able to conduct digital searches appropriately.

Digital forensics has a very important role in proving online gambling cases, especially in collecting, secureing, and analyzing electronic evidence to qualify as valid evidence in court. In addition, law enforcement against online gambling also still faces juridical and technical obstacles, so it is necessary to strengthen the capabilities of the apparatus, digital forensic facilities, and cross-sector cooperation so that it is handled more effectively.

It is recommended that law enforcement officials, especially cyber-crime investigators, improve their capabilities in the field of digital forensics and cyber investigation. In addition, it is necessary to strengthen facilities, procedures for handling electronic evidence, and cooperation with various parties, both domestic and foreign, to support the effectiveness of law enforcement against online gambling crimes.

ADVANCED RESEARCH

Further research is recommended to more deeply examine the effectiveness of applying digital forensic techniques in the investigation and prosecution of online gambling cases, using a comparative approach across regions or countries to identify best practices. Furthermore, future research could explore the integration of artificial intelligence and digital forensics in detecting and tracking increasingly complex online gambling activities.

REFERENCES

Ariyanto, Y. W. B., & Ibrahim, B. H. (2024). Penegakan hukum kasus judi online di Indonesia. Kultura: Jurnal Ilmu Hukum, Sosial, dan Humaniora, 2(9).

Budiman, A., Rusmiati, E., & Rukmini, M. (2025). Alat bukti mata uang elektronik pada proses penyidikan dalam rangka pembaharuan hukum terhadap tindak pidana pencucian uang. Jurnal Ilmiah Penegakan Hukum, 12(1).

Casino, F., dkk. (2022). SoK: Cross-border criminal investigations and digital evidence.

Du, X., & Scanlon, M. (2019). Methodology for the automated metadata-based classification of incriminating digital forensic artefacts.

Efendi, T. F., Rahmadi, R., & Prayudi, Y. (2020). Rancang bangun sistem untuk manajemen barang bukti fisik dan chain of custody (CoC) pada penyimpanan laboratorium forensika digital. Jurnal Teknologi dan Manajemen Informatika, 6(2).

Fernando, D., Heniarti, D. D., & Zakaria, C. A. F. (2025). Transformasi alat bukti elektronik menggunakan digital forensik dalam pembaharuan hukum acara pidana. Journal Justiciabelen (JJ), 5(1).

Maryam, T. A., dkk. (2024). Peran digital forensik dalam pengumpulan bukti pada kasus judi online di Kabupaten Demak. Konsensus.

Marzuki, P. M. (2016). Penelitian hukum. Kencana.

Mawei, O. P. Y., Bawole, H. Y. A., & Kasenda, V. D. (2025). Penegakan hukum judi online berdasarkan Pasal 27 Ayat (2) Undang-Undang Informasi dan Transaksi Elektronik. Lex Administratum, 13(1).

Mursyid, Putera, A., & Jannah, M. (2025). Rekonstruksi peran digital forensik dalam penyidikan tindak pidana siber: Analisis kritis terhadap konstruksi hukum pidana di Indonesia. Jurnal Tana Mana, 21.

Mustika, J., Djumhadi, Abdillah, M. F., & Utomo, D. S. I. (2025). Urgensi digital forensik untuk pembuktian tindak pidana siber dalam konteks merusak data dan sistem elektronik. JAITS: Journal of Applied Information Technology Solution.

Nathalia, B. (2021). Urgensi digital forensik dalam pembuktian tindak pidana siber (cyber crime). Brawijaya Law Student Journal.

Rahayu, S. T. W. (2022). Penegakan hukum perjudian online menurut Undang-Undang ITE. Rechtsregel: Jurnal Ilmu Hukum, 5(2).

Rahmad, N., Arifah, K. N., Setiyawan, D., Ramli, M., & Daud, B. S. (2022). Efektivitas bukti elektronik dalam UU ITE sebagai perluasan sistem pembuktian dalam KUHAP. Prosiding University Research Colloquium, 51.

Ramdani, M. A. R. F., Hadiana, A. I., & Ilyas, R. (2025). Pemanfaatan open-source intelligence untuk deteksi dan penanganan cybercrime judi online berbasis forensik digital. Jurnal Algoritma.

Soekanto, S. (2014). Pengantar penelitian hukum. UI Press.