JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 2 Mei 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i2.10601/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Legal Proof of Cybercrime: A Case Study of the Hacking of Bank Syariah Indonesia (BSI)

Ramdhan Mahardika Nasyith[1], Marchello Putra Toding Palilli[2], Triswer[3], Russell Dante Wiranatakusumah[4], Telly Augustine[5]
Universitas Pelita Harapan

Article Info
Article history:
Received: 30 April 2026
Publish: 9 May 2026

Keywords:
Cybercrime;
Legal Evidence;
Digital Evidence;
IT IS;
BSI Hack.

Abstract
This research aims to analyze legal evidence for cybercrime through a case study of the hacking of Bank Syariah Indonesia (BSI). The method used is normative legal research with a statutory, case, and conceptual approach. The results show that evidence in cybercrime relies heavily on digital evidence such as system logs, electronic data, and malware analyzed through digital forensics. The validity of electronic evidence has been recognized in Article 5 paragraph (1) and Article 44 of the Electronic Information and Transactions Law (UU ITE), and is supported by Article 235 paragraph (1) of the new Criminal Procedure Code (KUHAP). However, the evidentiary process faces various obstacles such as the anonymity of the perpetrator, the cross-border nature, and the vulnerability of digital evidence to manipulation. Therefore, it is necessary to increase the capacity of law enforcement officers, strengthen cybersecurity systems, and collaborate across institutions and internationally to support effective law enforcement against cybercrime.

Corresponding Author:
Ramdhan Mahardika Nasyith
Universitas Pelita Harapan
Email: ramdhannasyith@gmail.com

1. INTRODUCTION

The development of information and communication technology in the digital era has brought significant changes to various aspects of life, including the financial and banking sectors. The digital transformation undertaken by financial institutions, including Islamic banks, has provided easier access to services for the public, such as online transactions, mobile banking, and cloud-based system integration. However, behind this progress, a serious threat has emerged in the form of increasingly complex and organized cybercrime (Sukesi et al., 2024). Cybercrime not only causes material losses but also impacts public trust in financial institutions. One case that has garnered public attention in Indonesia is the hacking of Bank Syariah Indonesia (BSI), which resulted in service disruptions and the potential for customer data leakage. This case serves as a clear example that digital security systems still have gaps that can be exploited by irresponsible parties.

From a legal perspective, cybercrime is a form of crime with unique characteristics compared to conventional crimes. This crime is borderless, utilizes advanced technology, and involves invisible digital evidence. This presents unique challenges in the legal evidence process, both for law enforcement officials and the judicial system. Proving in cybercrime cases relies not only on traditional evidence such as witness testimony or physical documents, but also involves electronic evidence, such as system logs, digital data, network activity recordings, and digital forensics (Aprilianti, 2024). Therefore, a

comprehensive understanding of the legal evidence mechanisms in the context of cybercrime is necessary to ensure effective and fair law enforcement.

Normatively, regulations regarding cybercrime in Indonesia have been accommodated in various laws and regulations, one of which is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law Number 19 of 2016. This law recognizes the existence of electronic information and/or electronic documents as valid legal evidence, as regulated in Article 5 paragraph (1) (Wirandicha et al., 2025). In addition, the Criminal Procedure Code (KUHAP) also forms the basis of the evidentiary system in Indonesia, which adheres to the principle of proof based on valid evidence and the conviction of the judge. In this context, the integration of conventional criminal procedure law with the development of digital technology is an unavoidable need, and we must learn.

The Bank Syariah Indonesia (BSI) hacking case is interesting to study because it reflects the complexity of proving the value of cybercrime. In this case, the perpetrators allegedly used cyberattack methods such as ransomware, which can encrypt data and disrupt banking system operations. Furthermore, there are indications of customer data leaks that could potentially be misused. In the process of proving the value, law enforcement officials must be able to identify the perpetrators, trace digital footprints, and secure valid and legally accountable electronic evidence (Ghozali et al., 2024). This requires specialized expertise in digital forensics and cross-agency coordination, including with information technology service providers.

The main problem in proving cybercrime lies in the easily altered, deleted, or falsified nature of digital evidence. Therefore, strict procedures are required for the collection, storage, and analysis of electronic evidence to maintain its authenticity (integrity) and ensure its admissibility in court. Furthermore, jurisdictional issues pose a challenge, given that cybercriminals can operate from outside Indonesia's jurisdiction. This necessitates international cooperation in law enforcement and regulatory harmonization between countries. Furthermore, proving cybercrime requires increased human resource capacity, both among law enforcement officers and judges, in understanding information technology. Without adequate understanding, the evidentiary process can encounter obstacles, such as errors in interpreting digital evidence or an inability to assess the validity of electronic evidence (Laksito et al., 2024). Furthermore, rapid technological developments also require regular regulatory updates to remain relevant to current conditions.

Thus, this research is crucial to analyze the legal evidence mechanisms in cybercrime cases, particularly the Bank Syariah Indonesia (BSI) hacking case. This research is expected to provide a clear picture of the types of evidence used, the digital evidence analysis process, and the obstacles encountered in the evidentiary process. Furthermore, this research also aims to provide recommendations for the development of a legal system that is more adaptive to technological developments, thereby providing optimal legal protection for the public. Legal evidence in cybercrime is not merely a technical issue, but also concerns aspects of justice and legal certainty. In the increasingly advanced digital era, the legal system is required to be able to adapt and respond to existing challenges, without neglecting the basic principles of applicable law. Therefore, the study of legal evidence in cybercrime, particularly through the case study of the Bank Syariah Indonesia (BSI) hacking, is relevant and important as a contribution to the development of legal science, particularly in the field of cyber law in Indonesia.

2. RESEARCH METHODS

The research method used in this study is an empirical normative legal research method, namely, research that focuses on the study of applicable legal norms related to evidence in cybercrime (Muhammad, 2004). This method was chosen because the study aims to analyze in depth how the legal regulations and application of evidence in cybercrime, particularly in the case of the hacking of Bank Syariah Indonesia (BSI). The approaches used include a statute approach, a case approach, and a conceptual approach. The statutory approach is carried out by examining various relevant regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Criminal Procedure Code (KUHAP). The case approach is used to concretely examine the BSI hacking incident, particularly in the aspects of evidence and analysis of digital evidence. Meanwhile, the conceptual approach is used to understand legal theories related to electronic evidence and digital forensics.

The types of legal materials used consist of primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations, secondary legal materials include books, scientific journals, and previous research results, while tertiary legal materials include legal dictionaries and other supporting sources. The legal materials were collected through library research. Furthermore, the data obtained were analyzed using qualitative methods by reviewing, interpreting, and connecting legal norms with the facts. Through this method, it is hoped that a comprehensive understanding of legal evidence in cybercrime and the obstacles encountered in practice can be achieved.

3. RESULTS AND DISCUSSION

Chronology of the Bank Syariah Indonesia (BSI) Hacking Case

The chronology of the Bank Syariah Indonesia (BSI) hacking case began in early May 2023, when several customers began complaining about disruptions to digital banking services, such as mobile banking and ATMs, which were inaccessible. This disruption was widespread and lasted for several days, raising public concern. Initially, BSI stated that the disruption was caused by system maintenance (Putri & Yusuf, 2025). However, as time went on, indications emerged that the disruption was not merely a technical issue, but rather related to a cyberattack.

Information regarding the alleged hacking has grown stronger following the circulation of claims from a hacker group known as LockBit, claiming responsibility for the attack on BSI's systems. This group is known for carrying out ransomware attacks, a type of cybercrime that encrypts victims' data and demands a ransom to recover it. In this case, LockBit claimed to have successfully accessed BSI's internal systems and stolen a large amount of critical data, including customer data and internal company documents. Furthermore, the hacker group allegedly published some of the stolen data on the dark web to pressure BSI into complying with the ransom demands. The purportedly leaked data includes sensitive information such as customer identities, account numbers, and confidential internal documents (BBC Indonesia, 2023). This undoubtedly poses the potential for significant financial and reputational losses for BSI, a financial institution that maintains public trust.

In response to this situation, BSI, along with relevant authorities, such as the National Cyber and Crypto Agency (BSSN) and the Financial Services Authority (OJK), immediately took action. These efforts included gradually restoring the service system, investigating the source of the attack, and enhancing the information technology security system. Furthermore, a search was conducted for possible data leaks and their impact on customers. During the investigation, an analysis of the perpetrator's digital footprint was conducted. This included examining system logs, network activity, and the methods used

to penetrate the system. Based on this analysis, it is suspected that the perpetrator exploited a security vulnerability in BSI's information technology system to gain unauthorized access. After successfully gaining access (Kristianti, 2026), the perpetrator then further exploited the system by accessing, copying, and encrypting data within the system.

The service disruption that lasted for several days indicated that this attack was not only intended to steal data but also disrupted the overall system's operations. This is a common characteristic of ransomware attacks, which aim not only to acquire data but also to paralyze the system, putting victims under pressure. In such situations, companies are faced with the difficult choice of paying the ransom or bearing the losses resulting from operational disruptions and data leaks. Over time, BSI's services began to gradually recover, and the bank stated that customer funds remained secure. However, this case remains a serious concern because it highlights weaknesses in the cybersecurity system that could be exploited by irresponsible parties (Larasati & Firdaus, 2024). Furthermore, this case also serves as an important lesson for the Indonesian banking industry regarding the importance of strengthening digital security systems and being prepared to face cyber threats.

Identification and Analysis of Digital Evidence in the BSI Case

Identification and analysis of digital evidence in the Bank Syariah Indonesia (BSI) hacking case is a crucial aspect of the legal evidence process, considering that cybercrime generally leaves no physical traces, but rather electronic ones that require special methods to uncover. In the 2023 BSI case, the identified digital evidence came from various sources, including the bank's internal systems, communication networks, and data published by hacker groups in cyberspace, such as the dark web. In fact, the LockBit 3.0 ransomware group claimed to have stolen approximately 1.5 terabytes of data from BSI's systems, including the data of more than 15 million customers and employees. This data consisted of various types of sensitive information, such as names, addresses, telephone numbers, account information, transaction history, and internal company documents. In fact, several reports stated that the stolen data also included legal documents, non-disclosure agreements (NDAs), and system credentials in the form of internal and external service passwords. All of this data can be categorized as digital evidence with high evidentiary value in uncovering the perpetrators' modus operandi (CSIRT, 2023).

In the context of identification, the digital evidence in this case can be grouped into several types. First, system logs, which are records of server and network activity that can indicate the time, source of access, and attack patterns carried out by the perpetrator. Second, exfiltrated data, which is customer data and internal documents successfully taken by the perpetrator. Third, the malware or ransomware used, in this case LockBit 3.0, which was the primary tool for encrypting data and disabling the system. Fourth, digital communication traces, such as threatening messages, ransom negotiations, and data publications on the dark web. All of these components are integral parts of electronic evidence that must be forensically analyzed.

Analysis of digital evidence is conducted using a digital forensics approach, a scientific process for identifying, collecting, examining, and analyzing electronic data to obtain legal evidence. In the BSI case, the analysis focused on how the perpetrator gained initial access to the system, allegedly through exploiting a security vulnerability or compromised credentials. The perpetrator then escalated access rights, copied data, and encrypted the system to disrupt operations. This process typically leaves a digital trail that can be traced through activity logs and system artifacts.

From a legal perspective, the existence and use of digital evidence in Indonesia have been legally recognized. This is regulated in Article 5 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law Number 19 of 2016, which states that electronic information and/or electronic documents and their printouts constitute valid legal evidence. In addition, Article 44 of the ITE Law also emphasizes that evidence in investigations, prosecutions, and examinations in court may be in the form of evidence as regulated in criminal procedural law, as well as other evidence in the form of electronic information.

Furthermore, in the new Criminal Procedure Code (KUHAP), the evidentiary system refers to Article 235 paragraph (1), which mentions five valid pieces of evidence, namely witness statements, expert statements, letters, defendant statements, evidence, electronic evidence, judge observations, and everything that can be used for evidentiary purposes during court hearings as long as it is obtained legally. In the context of cybercrime, digital evidence is often classified as written evidence that is strengthened by expert testimony in the field of digital forensics (Pradipa, 2025). Therefore, the results of forensic analysis of stolen data, system logs, and malware are very important to strengthen evidence in court.

However, the main challenge in digital evidence analysis is maintaining the integrity and authenticity of the data. Digital evidence is highly vulnerable to alteration, deletion, or manipulation, so the collection process must adhere to the chain of custody principle, a procedure that ensures that evidence remains unchanged from the time it is first discovered until it is presented in court. In the case of BSI, the complexity increases because some of the data has been made public by the perpetrator, requiring additional verification to ensure its authenticity and linkage to the BSI system.

Legal Proof Process for BSI Hackers

The legal process of establishing evidence against the perpetrators in the Bank Syariah Indonesia (BSI) hacking case is complex because it involves technology-based crimes with cross-system characteristics and potentially cross-border. In practice, the evidence base relies not only on conventional evidence but also heavily on electronic evidence and digital forensic analysis. Therefore, the evidentiary process in this case must integrate provisions of criminal procedure law with specific regulations in the field of information technology.

The initial stage in the evidence-gathering process begins with an investigation and inquiry conducted by law enforcement officials, such as the Indonesian National Police, with support from technical institutions such as the National Cyber and Crypto Agency (BSSN). In the BSI case that occurred in May 2023, the investigation began following a service system disruption and claims from the LockBit ransomware group that they had stolen and encrypted bank data. At this stage, investigators collected digital evidence, such as system logs, network activity recordings, suspected leaked data, and samples of the malware used in the attack.

In the context of Indonesian law, the basis of evidence for cybercrime is regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 (ITE Law). Article 5, paragraph (1) of the ITE Law emphasizes that electronic information and/or electronic documents and their printouts constitute valid legal evidence. This legitimizes the use of digital evidence in criminal justice processes. In addition, Article 44 of the ITE Law also states that evidence in cases related to information technology can be in the form of evidence as regulated in criminal procedural law, as well as other evidence in the form of electronic information (Ilham et al., 2024).

Furthermore, in the new Criminal Procedure Code (KUHAP), specifically Article 235 paragraph (1), it is regulated that valid evidence includes witness statements, expert statements, letters, defendant statements, evidence, electronic evidence, judge observations, and anything that can be used for evidentiary purposes in court proceedings, as long as it is obtained lawfully. In the BSI hacking case, electronic evidence such as system logs and digital data is generally qualified as written evidence, which is then strengthened by the testimony of a digital forensic expert (Banjarnahor, 2023). Expert testimony is very important to explain technically how the attack was carried out, how data was accessed or stolen, and how the perpetrator is related to the digital evidence found.

The evidence-gathering process also involves digital forensic analysis aimed at uncovering the perpetrator's digital footprint. In the BSI case, the analysis was conducted on the LockBit 3.0 ransomware attack pattern, which is known to use data encryption and information exfiltration techniques before crippling the system. According to circulating reports, this group claimed to have accessed and stolen approximately 1.5 terabytes of data, including millions of customer records and internal documents (CSIRT, 2023). This claim served as an initial clue that was later verified through forensic analysis of BSI's internal systems.

During the evidentiary stage of the trial, the judge will assess the strength of the evidence based on Indonesia's system of proof, namely the negative legal system (negatief wettelijk bewijsstelsel). This means that the judge's decision must be based on at least two valid pieces of evidence and the judge's conviction. In cybercrime cases such as the BSI hack, the combination of electronic evidence, expert testimony, and witness testimony is key to building a strong legal framework to prove the perpetrator's guilt.

However, there are various obstacles in the evidence-gathering process, one of which is the anonymity of perpetrators, who often use hidden networks (the dark web) and encryption technology to conceal their identities. Furthermore, the perpetrators' locations, which can be outside of Indonesian jurisdiction, also present a challenge to law enforcement. Therefore, international cooperation through mechanisms is necessary for *mutual legal assistance* (MLA) or international cooperation in handling cybercrime. Furthermore, the authenticity and integrity of digital evidence are also important concerns. To ensure that evidence remains intact, investigators must apply the chain of custody principle at every stage of evidence handling. This is crucial to ensure that evidence presented in court is admissible and has valid probative force (Cahyono et al., 2025).

4. CONCLUSION

Based on the discussion, it can be concluded that legal proof of cybercrime in the Bank Syariah Indonesia (BSI) hacking case is highly complex because it involves digital evidence that is invisible and vulnerable to manipulation. This case demonstrates that cyberattacks not only disrupt banking system operations but also have the potential to cause massive data leaks that impact public trust. Digital evidence, such as system logs, stolen data, malware, and communication traces are crucial element in the evidentiary process. This evidence must be analyzed through digital forensics, and its authenticity must be maintained according to the principles of the digital forensics *Chain of custody. From* a legal perspective, Article 5 paragraph (1) and Article 44 of the ITE Law, as well as Article 235 paragraph (1) of the new Criminal Procedure Code, provide a strong basis for the use of electronic evidence in the judicial process. The evidentiary process also emphasizes the important role of digital forensic experts in explaining technical aspects in court. However, there are obstacles such as the anonymity of the perpetrator, the use of advanced

technology, and the possibility of cross-jurisdictional disputes that hamper law enforcement.

5. BIBLIOGRAPHY

Aprilianti, A. (2024). Efektivitas dan Implementasi Undang-Undang Informasi dan Transaksi Elektronik sebagai Hukum Siber di Indonesia: Tantangan dan Solusi. *Begawan Abioso*, *15*(1).

Banjarnahor, D. (2023). *Diduga Kena Cyber Attack, Bos BSI: Perlu Audit & Digital Forensik*. Bloomberg Technoz. https://www.bloombergtechnoz.com/detail-news/6104/diduga-kena-cyber-attack-bos-bsi-perlu-audit-digital-forensik

BBC Indonesia. (2023). *BSI diduga kena serangan siber, pengamat sebut sistem pertahanan bank "tidak kuat."* BBC Indonesia. https://www.bbc.com/indonesia/articles/cn01gdr7eero

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). RIKONSTRUKSI HUKUM PIDANA TERHADAP KEJAHATAN SIBER (CYBER CRIME) DALAM SISTEM PERADILAN PIDANA INDONESIA. *DJH Dame Journal Hukum*, *1*(1), 111–133.

CSIRT. (2023). *Mengenal LockBit 3.0, Ransomware yang membuat layanan BSI lumpuh*. CSIRT.

Ghozali, M., Liana, N., Afra, C., Siregar, Z., Nurfahni, Malahayati, & Hatta, M. (2024). Kejahatan Siber (Cyber Crime) dan Implikasi Hukumnya : Studi Kasus Peretasan Bank Syariah Indonesia (BSI). *CENDEKIA: Jurnal Hukum, Sosial & Humaniora*, *2*(4), 797–809.

Ilham, A. I., Shuhufi, M., & Rauf, A. A. M. (2024). Kedudukan Alat Bukti Elektronik Dalam Pembuktian Tindak Pidana. *Media Hukum Indonesia (MHI)*, *2*(2), 555–559.

Kristianti, L. (2026). *BSI koordinasikan serangan siber pada OJK, BI, dan BSSN*. Antara News. http://kalteng.antaranews.com/berita/635334/bsi-koordinasikan-serangan-siber-pada-ojk-bi-dan-bssn

Laksito, J., Idris, M. F., & Waryanto, A. (2024). Hak dan Kewajiban Negara dalam Mengatasi Kejahatan Lintas Batas di Era Digital: Pendekatan Analisis Normatif. *HAKIM – Jurnal Ilmu Hukum Dan Sosial*, *2*(4), 774–790. https://doi.org/10.51903/hakim.v2i04.2154

Larasati, N. M., & Firdaus, R. (2024). Analisis Bahaya Serangan Ransomeware Terhadap Layanan Perbankan. *Merkurius : Jurnal Riset Sistem Informasi Dan Teknik Informatika*, *2*(4), 102–109.

Muhammad, A. (2004). *Hukum dan Penelitian Hukum*. *8*(1), 134.

Pradipa, A. (2025). Analisis terhadap Kedudukan Alat Bukti Elektronik dalam Pembuktian Perkara Perdata Pasca UU ITE dan Perkembangan E-Court. *Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, *2*(3).

Putri, A. A., & Yusuf, H. (2025). RANSOMWARE DI SEKTOR KEUANGAN : STUDI KASUS SERANGAN TERHADAP BSI PADA TAHUN 2023 RANSOMWARE IN THE FINANCIAL SECTOR : A CASE STUDY OF ATTACKS ON BSI IN 2023. *JIIC: JURNAL INTELEK INSAN CENDIKIA*, *2*(8), 15649–15656.

Sukesi, E., Astuti, R. P., Wijayanti, L., & Wicaksono, R. B. (2024). Peran Dan Tantangan Jasa Perbankan Di Era Digital. *Gudang Jurnal Multidisiplin Ilmu*, *2*(12), 548–551.

Wirandicha, Y., Jayakusuma, Z., & Diana, L. (2025). Ratifikasi Convention on Cybercrime Oleh Indonesia Sebagai Bentuk Pencegahan Carding Dalam Perspektif Hukum Internasional. *Milthree Law Journal*, *1*(1), 58–90.