Law Enforcement of Skimming as a Cyber Crime: Digital Forensic Challenges and Evidence in Court

Dian Eka Kusuma Wardani, Raodiah, Indrahayu M. Umar Gazali
Fakultas Hukum, Universitas Sawerigading, Makassar
dianunsa@gmail.com, hj_raodia@yahoo.com, yayukstiki@gmail.com

Article Info
Received: 2025-01-22
Revised: 2025-03-21
Accepted: 2025-03-30

Keywords:
Skimming; Cyber Crime; Law Enforcement; Digital Forensics

Abstract
Skimming is a form of cybercrime that continues to grow with the increasing use of digital banking technology. This method involves stealing customer card data through special devices installed on ATMs or payment terminals, resulting in significant financial losses. This article discusses law enforcement against skimming, focusing on two main aspects: digital forensic challenges and evidence in court. The research method used is a juridical-normative approach with a literature review, which includes analysis of laws and regulations, legal literature, and actual cases related to skimming. Furthermore, a case study approach is used to examine the application of digital evidence in the judicial process. The results show that investigators face difficulties in identifying electronic traces, analyzing evidence, and ensuring the authenticity of digital data that is vulnerable to manipulation. Another challenge lies in providing evidence in court, where judges and law enforcement officials often have limited technical understanding of digital forensics. However, judicial practice shows that digital evidence is admissible if obtained legally and supported by adequate forensic expertise. Thus, law enforcement against skimming requires synergy between regulations, technology, and the competence of law enforcement officials. Collaboration between digital forensic experts and law enforcement is key in addressing skimming as a cybercrime.

I. Introduction

The development of information and communication technology in the last two decades has brought significant changes to various aspects of human life, including the banking sector. The development of information technology has fundamentally revolutionized the banking world. If in the past customers had to come directly to branch offices or queue at tellers to conduct transactions, now most banking needs can be met simply through their fingertips. The transformation towards the digitalization of banking services offers ease of transactions through Automatic Teller Machines (ATMs), internet banking, mobile banking, and various other electronic payment system innovations (Khalaf Al Hattali et al., 2020).

The first convenience lies in accessibility. Customers can make fund transfers, bill payments, and even purchase financial products at any time without being bound by bank operating hours. The presence of 24/7 services makes banking more responsive to the fast-paced modern lifestyle. Secondly, the digitalization of banking also brings cost and time efficiency. Processes that once required additional administrative fees or trips to the bank office can now be completed in seconds through an application. This reduces the bank's operational costs while providing added value to customers (Gary Gagarin Akbar & Rahmatiar, 2025).

Thirdly, digitalization promotes financial inclusion. With just a smartphone and an internet connection, people in remote areas can open accounts, save, and transact. This innovation expands the reach of financial services to communities that were previously difficult for conventional banks to access. Furthermore, digitalization creates an integrated financial ecosystem. Collaboration between banking and fintech makes payment, investment, and lending services more affordable. Everyday transactions, from paying for online transportation to online shopping, are now inseparable from digital payment systems (Gary Gagarin Akbar & Rahmatiar, 2025).

Digitalization of banking not only provides transaction convenience but also shapes a new culture in managing finances, where speed, efficiency, and ease of access are the main values. However, this development not only brings benefits but also gives rise to new forms of crime that exploit technological loopholes. One of the most disturbing criminal modes is *skimming*.

Skimming is a form of cybercrime in the banking sector that is carried out by stealing customer's ATM card or credit card data using a special device. This mode is usually done by installing an additional tool (skimmer) on an ATM machine or Electronic Data Capture (EDC) machine at the transaction site. The tool is capable of recording information on the card's magnetic stripe, such as the card number and owner identity

data (Guers et al., 2022). In addition, perpetrators often include hidden mini cameras or fake keypads to record customer PINs. The data that is successfully stolen is then duplicated onto a blank card so that the perpetrator can withdraw money or make transactions as if they were the legitimate owner(Khalaf Al Hattali et al., 2020).

Skimming is a serious threat because it is carried out secretly, so victims often do not realize their data has been stolen until their account balance decreases. This crime is also often carried out by organized international networks, making it difficult to track. Skimming is often carried out by transnational organized crime networks with a high level of complexity. The stolen data is not only used to withdraw cash, but also to carry out illegal transactions that harm customers and banking institutions (Rakha, 2023).

This phenomenon causes huge financial losses and reduces public trust in the digital banking system. Because of its nature involving technological devices and electronic data, skimming is categorized as a cybercrime that requires a special legal approach, different from conventional crimes(Manthovani, 2023). Therefore, it requires special handling, including the involvement of digital forensics to uncover traces of electronic evidence.

In the context of criminal law, the biggest challenge is how digital evidence from investigations can be processed, analyzed, and then convincingly presented in court. Handling skimming cases requires the involvement of digital forensics. Digital forensics is a branch of forensic science that plays an important role in uncovering skimming cases because this crime leaves traces of electronic evidence. Through digital forensics, investigators can identify and analyze data from devices used by perpetrators, such as ATM machines that have been fitted with skimmers, hidden camera recordings, or bank transaction log files(Manthovani, 2023).

This digital forensic process includes the collection, examination, analysis, and reporting of digital evidence using scientific methods that maintain the authenticity of the data. For example, investigators use imaging techniques to copy data without damaging the original, then trace usage patterns of devices or the flow of stolen data. With the support of digital forensics, electronic evidence can be verified for authenticity and then presented in court as valid evidence. This is very important because without scientific evidence, skimming crimes are difficult to prove given that the modus operandi is carried out secretly and is technology-based. However, this process is not simple. Digital data is vulnerable to being altered, deleted, or falsified, so the integrity of the evidence is often questioned. Judges, prosecutors, and investigators are also required to have technical understanding in assessing electronic evidence so that the resulting decisions are not only fair but also legal according to

criminal procedure law.

This research offers novelty about cybercrime in Indonesia. So far, studies on cybercrime in Indonesia are generally still general, discussing cybercrime as a broad phenomenon without highlighting specific forms such as skimming in depth. This research is here to fill that gap by providing a primary focus on skimming, namely the mode of stealing banking card data that is widespread and causes huge losses.

This research uses an interdisciplinary approach that combines criminal law, digital forensics, and judicial practice. This approach is important because skimming crimes cannot be understood only from the legal aspect, but also require a technical understanding of how skimmer devices work and the digital forensic process. Another novelty is the emphasis on the direct relationship between technical challenges in digital forensics and the acceptance of evidence in court, something that is still rarely discussed in Indonesian legal literature. Thus, this research provides new contributions that are relevant both theoretically and practically.

The urgency of this research is also very high. Skimming crimes in Indonesia still occur frequently, even causing losses of billions of rupiah every year. On the other hand, the government is encouraging the digitalization of banking and financial inclusion, which makes more and more people vulnerable to the threat of this crime. Challenges arise because law enforcement officials often do not have adequate technical understanding related to digital forensics, so the evidence in court becomes weak. Therefore, this research is urgent to provide solutions so that the legal system is able to adapt to the dynamics of cybercrime that continue to develop.

This research also has urgency in the context of consumer protection and maintaining public trust in the digital banking system. Without serious efforts in law enforcement, public trust could decline, which ultimately impacts the stability of the national financial system. Therefore, this research is not only important academically but also strategic for national interests. Based on this, this paper is designed to answer several key questions that are the focus of the study:

1. What are the characteristics of skimming as a form of cybercrime, and how is law enforcement carried out against skimming perpetrators in Indonesia?

2. What are the challenges faced in using digital forensics as a tool for proving skimming cases in court?

This research aims to analyze skimming as a cybercrime and to examine law enforcement against perpetrators in Indonesia. It also aims to identify and explain the challenges of digital forensics in proving skimming cases in court, while offering

relevant solutions.

2. Research Method

This research uses a normative-juridical method with descriptive-analytical characteristics. The normative-juridical type of research was chosen because the focus of the study lies on the positive legal norms that regulate the crime of skimming as a cybercrime, as well as the application of digital evidence in the judicial process. The descriptive-analytical nature is used to systematically describe how the law applies in practice, then analyzed to find answers to the formulated problems.

The research approach used is the statute approach, the conceptual approach, and the case approach. The statute approach is used to examine related regulations, such as the Law on Information and Electronic Transactions (UU ITE), the Criminal Code (KUHP), and the Criminal Procedure Code (KUHAP). The conceptual approach is used to review the theory of criminal law, cybercrime, and digital forensics. Meanwhile, the case approach is used to analyze the real practice of handling skimming cases in Indonesia.

The main data source in this research is secondary data, which consists of primary, secondary, and tertiary legal materials. Primary legal materials include laws and regulations and court decisions related to skimming cases. Secondary legal materials are obtained from academic literature, legal journals, research results, and scientific articles on cybercrime and digital forensics. The tertiary legal materials include legal dictionaries, encyclopedias, and other supporting sources that help explain the concept.

The analysis method used is qualitative analysis, namely by interpreting laws and regulations, reviewing literature, and comparing them with existing case facts. The analysis mechanism is carried out in three stages, the first is the identification of legal norms relevant to skimming and digital evidence; second, the synchronization and interpretation of legal norms with digital forensic practices in the field; and third, a critical evaluation of the extent to which positive law is able to answer the challenges in skimming law enforcement. With this method, the research is expected to provide a comprehensive picture of the relationship between regulations, digital forensic practices, and proof mechanisms in court, as well as offer solutions for strengthening the legal system in the face of cyber skimming crimes.

3. Results and Discussion

Characteristics of Skimming as a Cyber Crime

Skimming is a form of cybercrime that has characteristics different from conventional crimes. Skimming is defined as the act of stealing bank customer data through the process of copying information from ATM cards or credit cards using a special device called a skimmer. This device is usually installed secretly on ATM machines or Electronic Data Capture (EDC) machines at transaction sites(Guers et al., 2022).

Skimming perpetrators not only record the data stored on the card's magnetic stripe but also try to obtain the customer's Personal Identification Number (PIN) in various ways, such as installing hidden mini cameras or creating fake keypads (*keypad overlays*)(Fok et al., 2023). The data that has been successfully collected is then transferred to a blank card, so the perpetrator can duplicate the original card and use it to withdraw money or make transactions as if they were the legitimate owner.

The characteristics of *skimming* as *cybercrime* consist of four important points that distinguish it from conventional criminal acts. First, the modus operandi is highly dependent on digital technology. Perpetrators do not use physical violence but utilize electronic devices designed to record and store customer data. Skimming cannot be done in a conventional way because the entire process involves electronic devices, from skimmer devices installed on ATM machines to record card data, to hidden cameras or keypad overlays to record customer PINs. The data obtained is then transferred and processed through a computer or certain software, and then duplicated on a blank card(Guers et al., 2022).

This shows that digital technology is not just a tool but is a key element that enables this crime to occur. Without electronic devices and digital banking systems, skimming could not be carried out. This is what distinguishes skimming from conventional theft, because its digital nature makes this crime more difficult to detect, more complex to handle, and requires digital forensics to uncover it.

Second, skimming is generally carried out by organized transnational groups. This crime is rarely committed individually but involves a network of perpetrators with a clear division of roles. There are those who are responsible for producing and installing skimmer devices, some collect and process data, and some are responsible for withdrawing cash or carrying out illegal transactions using duplicate cards(Dessy Natalia DEF et al., 2020). This can be seen from several cases in Indonesia involving foreign perpetrators with global networks, which shows that skimming is no longer local but is a transnational crime. The financial transactions resulting from the crime are often channeled through several countries to make tracking difficult.

The involvement of transnational networks reinforces the fact that skimming is a global cybercrime. Handling it not only requires technical digital forensic capabilities but also cooperation between countries through mutual legal assistance mechanisms, Interpol, and international banking cooperation. Without cross-border coordination, law enforcement against skimming crimes will be difficult to carry out completely(Dewi & Septiwidiantari, 2021).

The third important characteristic of skimming is that this crime always leaves a trail of electronic evidence. Unlike conventional theft, which usually leaves physical evidence such as fingerprints or tangible evidence, skimming produces digital data records that can only be identified through specific technological devices. Electronic evidence in skimming cases can be in the form of data stored on the skimmer device, such as customer card information that has been successfully copied. Other evidence includes digital files on the perpetrator's computer or storage device containing thousands of stolen card data. Furthermore, evidence is in the form of traces of illegal transactions, both cash

withdrawals and online payments recorded in the banking system. Finally, evidence is in the form of recordings from hidden cameras installed by the perpetrators to record customer PINs(Dewi & Septiwidiantari, 2021).

The digital traces that exist are very important, but they are also fragile and easily manipulated. Data can be deleted, changed, or moved quickly, making it difficult to prove if it is not secured immediately. This is where the role of digital forensics becomes crucial, namely to ensure that electronic evidence can be extracted, analyzed, and validated according to legal standards so that it can be legally used in court(Rakha, 2023). Thus, the trail of electronic evidence is not only a characteristic of skimming but also a major challenge in the law enforcement process, because the success of uncovering this case greatly depends on the ability of law enforcement to manage digital evidence professionally.

The last important characteristic of skimming is that its impact not only harms individual victims but also poses a systemic risk to public trust in digital banking. For individuals, the direct loss can be in the form of lost savings balances or transaction bills that were never made. Although some banks usually provide a fund replacement mechanism, this claim process takes time and causes psychological stress for the victim. The customer's sense of security in using ATM services or credit cards is also disrupted.

A more serious impact is the systemic risk to the banking industry. Skimming creates the image that digital banking services are not completely secure. If this case occurs repeatedly, the public may lose confidence in the electronic transaction system, so they prefer to return to cash methods. This condition certainly contradicts the national and global agendas that encourage digital transformation and a cashless society. In addition, the bank's reputation can also be threatened. Customers tend to blame banking institutions when skimming occurs, even though legal responsibility does not entirely lie with the bank.(Yusnita et al., 2025). As a result, the bank's credibility could decline, triggering a potential massive withdrawal of funds, and even disrupting the stability of the financial system.

Based on the last characteristic, skimming cannot be seen only as a crime against individuals but as a threat to the entire digital banking ecosystem, which demands serious handling through strict regulations, more advanced security technology, and increased digital literacy of the public. From this discussion, it can be concluded that skimming as a cybercrime has characteristics, namely, technology-based, transnational, leaves digital evidence, and has broad implications for the banking system. These characteristics are an important basis for placing skimming as a cybercrime that requires a different legal and evidentiary approach than ordinary crimes.

Digital Forensics Challenges in Skimming Disclosure

Digital forensics plays a central role in uncovering skimming cases, as almost all traces of this crime are in the form of electronic evidence. Without the involvement of digital forensic experts, the investigation and evidentiary process in court would face significant obstacles(Amsori et al., 2024). However, research results indicate that there are significant

challenges in the implementation of digital forensics in Indonesia, particularly in handling skimming cases.

Digital evidence, including that found in skimming cases, is highly vulnerable. Unlike physical evidence, digital data can be easily deleted, modified, moved, or even hidden with a single simple command. For example, information from skimmer recordings can be permanently erased, or illegal transactions can be concealed with specific software.

Digital evidence also depends on storage media such as memory cards, hard disks, or servers, which are prone to physical and technical damage. This poses a significant challenge for law enforcement, as even a slight error in the securing process can render the evidence invalid or unaccountable in court. Therefore, strict digital forensic procedures, including maintaining the chain of custody and using scientific methods, are essential to ensure that electronic evidence remains intact, authentic, and legally valid as evidence(Rakha, 2023).

One of the main challenges in handling skimming cases is the limited expertise of law enforcement officials. Investigators, prosecutors, and judges often lack a technical background in digital forensics. As a result, the process of identifying, analyzing, and interpreting electronic evidence is not optimal. This lack of understanding creates two problems: first, investigators have difficulty collecting and securing digital evidence according to international standards; second, judges are often hesitant to accept electronic evidence because they do not understand the technical mechanisms of its authenticity. This situation opens opportunities for skimming perpetrators to escape legal sanctions, even though their digital traces could actually be revealed(Chen & Dong, 2023). Therefore, increasing the capacity of law enforcement through specialized training in cybercrime and digital forensics is an urgent need, so that the law enforcement process can run more effectively and in accordance with the development of crime technology.

The next obstacle in uncovering skimming cases is the lack of digital forensic infrastructure and technology. Not all regions in Indonesia have digital forensic laboratories or specialized equipment capable of analyzing electronic evidence quickly and accurately. As a result, investigations are often centralized in large cities or certain institutions, which slows down the investigation process. In addition, the increasingly sophisticated development of skimming modes demands state-of-the-art analysis tools, while the facilities owned by law enforcement officials are often lagging behind(Rahman Najwa, 2024). For example, when perpetrators use malware-based skimming, conventional investigation tools have difficulty detecting its traces. This limitation has a direct impact on the effectiveness of evidence in court, because digital evidence that is not properly analyzed can weaken the position of prosecutors and investigators. Therefore, investing in modern forensic technology is an urgent matter to improve law enforcement capacity in the era of cybercrime.

Evidence in skimming cases in the form of digital data must go through strict legal procedures in order to be legally used in court. This procedure is known as the chain of custody, which is the chain of possession of evidence that documents who accessed, moved, or examined the evidence from the first time it was found until it was presented at trial. The problem is that digital evidence is far more vulnerable than physical evidence.

If there is no clear record, the authenticity of the evidence can be debated. For example, data from skimmer recordings could be considered to have been altered if there is no official documentation of the seizure process. As a result, the judge may reject the evidence because it does not meet evidentiary standards. Thus, chain of custody issues often become an obstacle in skimming cases, and can only be overcome with procedural discipline, the use of standardized forensic methods, and the involvement of competent experts (Gary Gagarin Akbar & Rahmatiar, 2025).

Skimming is not only carried out locally, but often involves transnational crime networks. Many cases in Indonesia have found that the perpetrators come from abroad, collaborating with local networks to install skimmer devices, process data, and withdraw money from the crime. Stolen customer data can even be transferred to servers in other countries to be used globally(Guers et al., 2022)l.

This complexity poses a major obstacle to law enforcement, as the investigation process must involve international cooperation through mechanisms such as mutual legal assistance or Interpol. Without cross-border coordination, perpetrators who are outside Indonesia's jurisdiction are difficult to prosecute. In addition, the flow of funds from the crime usually passes through various countries, making it difficult to trace. Thus, the transnational nature of skimming confirms that this crime is not just an individual threat, but also a global challenge that requires cross-border collaboration, both in the aspects of law enforcement and the security of digital banking systems.

The biggest challenge in uncovering skimming is the very rapid development of its criminal methods. If initially perpetrators only used simple physical devices installed on ATMs to copy card data, now skimming methods have evolved to use malicious software (malware) that can infiltrate directly into ATM machine systems or banking networks(Khalaf Al Hattali et al., 2020).

Modern skimmer devices are increasingly small and difficult to detect, some even resemble genuine parts of the ATM machine, making them appear unsuspicious to customers. New modes also involve phishing or social engineering techniques to obtain PINs and additional data from victims. These dynamic changes in modus operandi require law enforcement officials and digital forensic experts to constantly update their skills and investigation technology(Sikos, 2021). Without rapid adaptation, law enforcement will lag behind the sophistication of perpetrators, making it increasingly difficult to solve skimming cases.

Based on the various challenges above, it is clear that the role of digital forensics is not only limited to investigation tools, but also part of the legal evidence mechanism. The success of uncovering skimming cases depends heavily on three main things: speed in securing digital evidence, the competence of law enforcement officials in understanding and using the results of digital forensic analysis, and strong legal legitimacy to ensure that digital evidence can be legally used in court. If these three aspects are not strengthened, then even if digital evidence is successfully found, the proof in court will most likely face serious obstacles.

Proving *Skimming* in Court

The evidentiary aspect in the criminal system plays a very vital role in determining whether a defendant can be found guilty or not. This also applies to skimming cases, which are categorized as cybercrimes. Unlike conventional crimes that generally leave physical evidence, skimming leaves more electronic evidence that is complex, easily modified, and difficult for law enforcement officials to understand without a technical background (Guers et al., 2022).

The Electronic Information and Transactions Law (UU ITE) has recognized electronic documents and digital information as legitimate evidence, but practices in the field show that there are still many challenges in presenting them in court. Judges are often hesitant to place digital evidence as primary evidence without the testimony of digital forensic experts who can explain the validity and integrity of the data. Therefore, proving skimming in court not only concerns the application of criminal procedure law normatively, but also demands synchronization between legal aspects, technology, and digital forensic expertise. This sub-chapter will review various obstacles, dynamics, and the important role of digital forensics in ensuring that skimming evidence can be accepted as the basis for a fair verdict(Dewi & Septiwidiantari, 2021).

Evidence is the most crucial aspect in every criminal case, including skimming as a cybercrime. In the Indonesian legal system, the existence of electronic evidence has been recognized through Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments. The UU ITE affirms that electronic information and/or electronic documents can be used as legitimate evidence as with other evidence in the Criminal Procedure Code (KUHAP). However, this normative recognition has not fully run smoothly in practice. Judges often still prioritize conventional evidence (witnesses, written documents, physical evidence) over digital evidence, especially if it is not accompanied by technical explanations from digital forensic experts(Rahman Najwa, 2024). In other words, electronic evidence is often seen only as a complement, not as primary evidence.

Based on the results of the analysis, there are several major obstacles in presenting skimming evidence in court, namely, first, the difficulty in guaranteeing the integrity of digital evidence; data seized from skimmer devices or the perpetrator's computer can be debated for its authenticity. The defense often argues that the data has been manipulated or is not authentic. Second, the limitations of the judge's understanding, namely that not all judges have the technical competence to assess digital forensic procedures (Khalaf Al Hattali et al., 2020). This results in hesitation in deciding whether electronic evidence is valid and convincing. Third, limitations in criminal procedure law, namely that the Criminal Procedure Code (KUHAP) has not comprehensively regulated the mechanism of proof based on digital evidence. As a result, there is overlap between the Criminal Procedure Code and the ITE Law, which causes debate in the courtroom. And fourth, the absence of a standard digital forensic standard. Until now, there is no detailed national procedural standard regarding the methods of acquisition, analysis, and presentation of electronic evidence(Gary Gagarin Akbar & Rahmatiar, 2025). This condition opens up gaps for inconsistencies between cases.

In many skimming cases, the presence of a digital forensic expert becomes a determining factor. The expert functions to explain to the judge how the digital evidence was obtained,

how its integrity was maintained, and why the evidence is valid to link the perpetrator to the crime. Without the presence of an expert, digital evidence is vulnerable to being considered weak or invalid(Shetty & Murthy, 2023). In addition, experts also help bridge the gap in understanding between digital technical language and legal language, so that judges can understand the context of the evidence more clearly. This role makes digital forensic experts often referred to as an "epistemic bridge" in cybercrime trials.

Based on the discussion, proving skimming in court faces a paradox. On the one hand, digital evidence is the most important element to ensnare perpetrators. However, on the other hand, this evidence is the most frequently debated for its validity. This paradox occurs because of the gap between the increasingly rapid development of crime technology, the capacity of criminal procedure law which is still conventional, and the readiness of judicial officials who are not yet uniform in understanding digital evidence. To overcome these obstacles, harmonization between the Criminal Procedure Code and the ITE Law is needed, strengthening special regulations regarding electronic evidence, and increasing the capacity of officials and judges through cybercrime training. Thus, proving skimming in court can be more effective and able to provide a sense of justice for victims.

Critical Analysis

The enforcement of skimming laws demonstrates a significant gap between the development of digital crime methods and the readiness of the legal system and law enforcement officials to respond. Skimming, rooted in the use of digital technology, presents new complexities that cannot be addressed solely with conventional legal instruments(Iswani & Nur, 2024). There are several aspects that influence the complexity of skimming cases, including regulatory aspects, technical and human resource aspects, infrastructure aspects, evidentiary aspects in court, and global and transnational aspects.

The regulatory aspect of handling skimming crimes in Indonesia already has a basis through the Criminal Code (KUHP), the Criminal Procedure Code (KUHAP), and the Electronic Information and Transactions Law (UU ITE). However, implementation in the field still faces a number of problems. There is a disharmony in criminal procedure law as the Criminal Procedure Code does not fully regulate evidentiary procedures with electronic evidence, while the ITE Law already recognizes it (Gary Gagarin Akbar & Rahmatiar, 2025). This situation causes confusion, namely that judges are often hesitant as to whether digital evidence can be used as primary evidence or only as supporting evidence. Another problem relates to rigid legal norms; positive law in Indonesia still tends to be based on conventional physical evidence. This is inversely proportional to the nature of skimming crimes, which are entirely based on digital technology. As a result, there is a mismatch between legal norms and the characteristics of the crime.

Another problem from the regulatory aspect is the lack of technical regulations. Until now, Indonesia does not have detailed national operational standards regarding the management of digital evidence, starting from the process of seizure, security, analysis, to presentation in court. This gap creates differences in procedures between law enforcers and risks weakening the power of proof. And another problem relates to cross-border jurisdictional challenges, in this case, skimming is often carried out by transnational

networks, requiring international legal rules and mechanisms for cooperation between countries. Unfortunately, Indonesia's national regulations are still weak in reaching cross-jurisdictional crimes(Rahman Najwa, 2024).

This condition shows that the existing regulations are still partial and reactive, and have not been able to comprehensively answer the needs of cybercrime law enforcement (Gary Gagarin Akbar & Rahmatiar, 2025). Therefore, updating criminal procedure law by including special regulations for digital evidence is a necessity. In addition, harmonization between the ITE Law, the Criminal Procedure Code, and international legal instruments is needed so that Indonesia has a strong and adaptive legal umbrella for the dynamics of cybercrime.

The next aspect is the technical and human resource aspect, which is one of the biggest obstacles in skimming law enforcement due to limitations within it. This crime is highly dependent on sophisticated digital technology, so handling it also requires law enforcement officials to have technical competence in the field of digital forensics. The first limitation that is often found is the limited expertise of officials. Many investigators, prosecutors, and judges still lack understanding of the characteristics of electronic evidence. As a result, the investigation and trial process is highly dependent on digital forensic experts. This dependence creates vulnerability if the number of experts available is limited or their interpretations differ.

Competency gaps between institutions are the second limitation in investigating skimming cases in Indonesia. Not all law enforcement agencies have the same capacity in handling digital evidence. For example, the police at the regional level often have difficulty handling skimming cases due to minimal facilities and experts, so they have to wait for central assistance. The third is the limited of continuous training(Rahman Najwa, 2024). The development of cybercrime modes, including skimming, is progressing very rapidly. However, the training of law enforcement officials does not always keep up with this development. As a result, there is a gap between the mode of crime and the capacity of officials to handle it. In addition, dependence on foreign technology is a further limitation of the investigation. Some of the digital forensic software or hardware used in Indonesia still relies on foreign products. In addition to high costs, this also raises issues of independence and confidentiality in the evidentiary process(Manthovani, 2023).

Regarding the technical and human resource aspects, it is clear that the weak capacity of law enforcement can reduce the effectiveness of handling cases *skimming*(Shetty & Murthy, 2023). In fact, digital evidence is very sensitive and requires professional handling in order to maintain its integrity in court. Without increasing the technical capacity of officials and equitable distribution of digital forensic facilities, the law enforcement process will continue to face significant obstacles.

Law enforcement in skimming cases is also strongly influenced by the availability of digital forensic infrastructure. This infrastructure includes hardware, software, laboratories, and support systems for identifying, securing, and analyzing digital evidence. Infrastructure limitations include limited digital forensic laboratories, outdated or limited analysis tools, a lack of data storage and security systems, and unequal access between regions(Rahman Najwa, 2024).

Regarding the limited number of digital forensic laboratories, it can be seen that not all regions in Indonesia have adequate digital forensic laboratories. Many skimming cases at the local level have to be sent to the central level for analysis, which results in the investigation process being slow (Rahman Najwa, 2024). This inequality creates gaps in the speed and quality of case handling. In addition, outdated or limited analysis tools in Indonesia are certainly an obstacle in tracing cases amidst the rapidly developing skimming technology, while the forensic tools used by law enforcement often lag behind the technology of the perpetrators. This reduces the effectiveness in finding electronic evidence.

The last limitation is the lack of data storage and security systems. Digital evidence is very vulnerable to damage, manipulation, or loss. However, there are still limitations in secure storage facilities and encryption systems, so the integrity of the evidence is at risk of being compromised. Infrastructure limitations show that skimming law enforcement still faces unequal access to technology (Iswani & Nur, 2024). In fact, without the support of adequate forensic infrastructure, even the expertise of officials will not be optimal. Therefore, state investment in building modern digital forensic laboratories and distributing them evenly is an urgent need.

The next aspect related to evidence in court in skimming cases is a crucial point that determines whether the perpetrator can be legally ensnared. Unlike conventional crimes that leave physical evidence, skimming produces more electronic evidence in the form of digital data from skimmer devices, transaction records, to network activity logs. The evidentiary aspect in court shows a legal paradox, namely that skimming crimes can only be proven through electronic evidence, but this evidence is the most frequently debated. This shows that there is still a gap between the development of crime technology and the adaptation of criminal procedure law(Dewi & Septiwidiantari, 2021).

To bridge the gap between technological developments and the adaptation of criminal procedure law, it is necessary to strengthen regulations so that digital evidence has a position equal to conventional evidence. In addition, it is necessary to increase the capacity of judges and prosecutors in understanding digital forensics. And it requires standardization of forensic procedures to ensure that digital evidence remains valid until the trial stage.

Skimming is included in the category of cybercrime that is often carried out by organized transnational networks. This mode is rarely carried out by a single individual, but involves international syndicates that have a division of roles ranging from skimmer device manufacturers, distributors of devices in various countries, to controllers of financial networks to withdraw and launder the proceeds of crime(Dewi & Septiwidiantari, 2021). Regarding the last aspect, the global and transnational aspects show that handling skimming cannot be done nationally alone.

Skimming crimes demand international legal harmonization, especially in the recognition of digital evidence. Furthermore, there needs to be faster and more effective cross-country cooperation through Interpol or other international forums. And it is important for Indonesia to play an active role in drafting international standards regarding digital forensics and banking security. With this transnational approach, skimming can be

handled more effectively, so that the law does not lag behind the evolving modes of crime.

4. Conclusion

Skimming, as a form of cybercrime, has evolved into a serious threat to digital banking systems in Indonesia and the world. Its characteristics, which are based on digital technology, carried out by transnational syndicates, leave electronic evidence, and have a systemic impact on public trust, make skimming a crime with high complexity. Law enforcement against skimming still faces a number of fundamental obstacles. From the regulatory side, there is disharmony between the Criminal Procedure Code and the ITE Law in terms of recognition and use of electronic evidence. From the technical and human resource aspects, the limited expertise of officials and dependence on digital forensic experts make the evidentiary process often dependent on the capacity of certain individuals. Meanwhile, the infrastructure aspect shows a lack of digital forensic laboratories, outdated analysis tools, and unequal distribution of facilities between regions.

In court, digital evidence is often debated for its validity even though it has been normatively recognized. This shows a paradox: the crime can only be proven through electronic traces, but this evidence is the most often doubted. Furthermore, the global and transnational aspects show that skimming cannot be handled nationally alone, but requires more adaptive and rapid international legal cooperation. Therefore, strategic steps are needed in the form of regulatory harmonization, increasing the capacity of officials through cybercrime education and training, strengthening digital forensic infrastructure, and transnational cooperation. With these efforts, skimming law enforcement is expected to be more effective, provide legal certainty, protect the interests of the community, and maintain public trust in the digital banking system.

References

Amsori, A., Awaluddin, akhri, & Mulyana, M. (2024). Tantangan dan Peran Digital Forensik dalam Penegakan Hukum terhadap Kejahatan di Ranah Digital. *Journal Humaniora: Jurnal Hukum Dan Ilmu Sosial*, *02*.

Chen, C., & Dong, B. (2023). Digital forensics analysis based on cybercrime and the study of the rule of law in space governance. *Open Computer Science*, *13*(1). https://doi.org/10.1515/comp-2022-0266

Dessy Natalia DEF, C., Sagung Laksmi Dewi, A., & Made Minggu Widyantara, I. (2020). *SANKSI PIDANA TERHADAP WARGA NEGARA ASING YANG MELAKUKAN TINDAKAN PEMBOBOLAN ANJUNGAN TUNAI MANDIRI (ATM) DENGAN TEKNIK SKIMMING*. *1*(2), 37–41. https://doi.org/10.22225/jph.v1i2.2340.37-41

Dewi, P. E. T., & Septiwidiantari, N. M. (2021). EFFORTS TO OVERCOME CRIMINAL ACTS OF SKIMMING COMMITTED THROUGH ATMS IN THE PERSPECTIVE OF LAW NUMBER 19 OF 2016 CONCERNING EIT. *NOTARIIL Jurnal Kenotariatan*, *6*(2), 106–111. https://doi.org/10.22225/jn.6.2.2021.106-111

Fok, R., Kambhamettu, H., Soldaini, L., Bragg, J., Lo, K., Hearst, M., Head, A., & Weld, D. S. (2023). Scim: Intelligent Skimming Support for Scientific Papers. *International Conference on Intelligent User Interfaces, Proceedings IUI*, 476–490. https://doi.org/10.1145/3581641.3584034

Gary Gagarin Akbar, M., & Rahmatiar, Y. (2025). Law Enforcement of Transnational Cybercrime: Case Study in Indonesia. *Delegalata: Jurnal Ilmu Hukum*, *10*, 279–286. https://doi.org/10.30596/dll.v10i2.24627

Guers, K., Chowdhury, M. M., & Rifat, N. (2022). Card skimming: A cybercrime by hackers. *IEEE International Conference on Electro-Information Technology*. https://ieeexplore.ieee.org/abstract/document/9813890/

Iswani, N. K., & Nur, M. (2024). THE ROLE OF FORENSIC TECHNOLOGY IN CYBER CRIME INVESTIGATION AND PROSECUTION. *Legal Studies and Social Science (MICoLLS), 2024*, 2985–3613.

Khalaf Al Hattali, S. S., Hussain, S. M., & Frank, A. (2020). Design and development for detection and prevention of ATM skimming frauds. *Indonesian Journal of Electrical Engineering and Computer Science*, *17*(3), 1224–1231. https://doi.org/10.11591/ijeecs.v17.i3.pp1224-1231

Manthovani, R. (2023). Indonesian Cybercrime Assessment and Prosecution: Implications for Criminal Law. *International Journal of Criminal Justice Sciences*, *18*. https://doi.org/10.5281/zenodo.4756224/IJCJS

Rahman Najwa, F. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *Al-Bahst Jurnal Ilmu Sosial, Politik, Dan Hukum*, *2*(1).

Rakha, N. A. (2023). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review*.

Shetty, A. A., & Murthy, K. V. (2023). Investigation of Card Skimming Cases: An Indian Perspective. *Journal of Applied Security Research*, *18*(3), 519–532. https://doi.org/10.1080/19361610.2021.2024049

Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations. *Wires Forensic Sci*, *3*(3). https://doi.org/10.1002/WFS2.1394

Yusnita, R., Aprilia Pratiwi, L., & Citra, H. (2025). *Perlindungan Konsumen Terhadap Kerugian Akibat Skimming dan Kebocoran Data di Bank*. *1*(4), 380–383. https://jurnal.kopusindo.com/index.php/jkhkb