Analysis of Phishing Attacks on Ecommerce Services using National Institute of Standards and Technology Method

Dio Andrean
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
The rapid growth of e-commerce has increased the risk of phishing attacks targeting users' sensitive information. This study aims to analyze phishing attacks on e-commerce services using the National Institute of Standards and Technology (NIST) digital forensic methodology. The investigation was conducted through the collection, examination, analysis, and reporting phases. A phishing attack scenario was simulated by sending phishing emails containing links to a fake login website. Network traffic was captured using Wireshark and analyzed using .pcapng files and sslkeylog.log to identify digital evidence from encrypted HTTPS communications. The investigation successfully identified the phishing domain (soppieeeee.free.nf), server IP address (185.27.134.228), TCP and TLS handshake activities, HTTP POST requests, and the victim's transmitted login credentials. The integrity of the collected evidence was verified using MD5 hash values. The results demonstrate that the NIST methodology, combined with Wireshark, provides a systematic and effective approach for collecting, examining, analyzing, and reporting digital evidence related to phishing attacks on e-commerce services.

Keywords
E-commerce, Digital Forensics, NIST, Phishing, Wireshark.

1. INTRODUCTION
The growth of e-commerce in Indonesia has surged alongside the rise in internet users and digital transactions. However, this growth has also been accompanied by an increase in cyberattacks, particularly web-based phishing aimed at stealing users' personal and financial data. According to the 2022 Honeynet Project BSSN report, there were over 370 million cyberattacks in Indonesia, with phishing being one of the most prevalent methods [1]. Web-based phishing poses a serious threat because it can mimic the appearance of legitimate websites, making it difficult for users to distinguish [2]. Previous research has shown that deep learning and XGBoost methods can detect phishing sites with an accuracy rate of over 95% [3],[4]. In addition to detection technologies, security frameworks such as the National Institute of Standards and Technology (NIST) are also needed to support the structured process of identifying and handling cyber threats [5]. The NIST method involves the stages of collection, examination, analysis, and reporting, which are used to systematically obtain and analyze digital evidence while maintaining data integrity throughout the investigation process [6]. Additionally, network forensic investigations are conducted by recording network traffic using PCAP files to identify network communication activities and data packets that are indicative of cyberattacks [7]. The NIST method has been applied in digital forensic research on phishing by utilizing Wireshark to capture and analyze suspicious network traffic [8]. Additionally, user security awareness is a critical factor in preventing phishing through education and increased understanding of cyber threats [9],[10]. Common types of phishing attacks include spear phishing, deceptive phishing, and web phishing, which are used to steal user credentials [11]. This study employs a digital forensic approach based on the NIST phases: collection, examination, analysis, and reporting [12]. The evidence collection process was conducted using Wireshark to record network activity and save data in .pcap format for further analysis[13]. Network traffic analysis enables investigators to identify communication patterns, reconstruct attack timelines, and recover digital artifacts such as IP addresses, domain names, protocol exchanges, and transmitted credentials. These capabilities play an important role in validating phishing incidents and strengthening the reliability of digital evidence obtained during forensic investigations. Therefore, protection against phishing requires collaboration between security technologies, user awareness, and strong regulatory support [14].

2. LITERATURE STUDY

2.1 Digital Forensics
Digital forensics is a field of study that applies scientific principles to obtain, analyze, and present digital evidence used in legal investigations. Digital evidence can originate from computers, smartphones, emails, network traffic, and system activity logs related to cybercrimes. In addition to supporting investigations, digital forensics is also used to maintain the security, integrity, and reliability of digital systems by identifying unauthorized activities and preserving important evidence. Mobile forensics, as part of digital forensics, is used to recover digital evidence from smartphones involved in cybercrime activities [15]. The digital forensics process generally involves several stages, including identification, collection, examination, analysis, and reporting of digital evidence to ensure that the investigation results are accurate and legally acceptable. Each stage has a specific role in preserving the integrity of digital evidence, minimizing the risk of data alteration, and ensuring that the collected evidence can be systematically analyzed throughout the investigation. A structured digital forensic process also improves the reliability and reproducibility of investigation results, particularly in cybersecurity incident investigations involving phishing attacks. Recent research shows that the use of digital forensics continues to increase alongside technological developments and the growing need for digital investigations in various sectors, including cybersecurity and law enforcement [16]. Based on this, the stages of the digital forensics process can be seen in Figure 1: Digital Forensics Diagram.

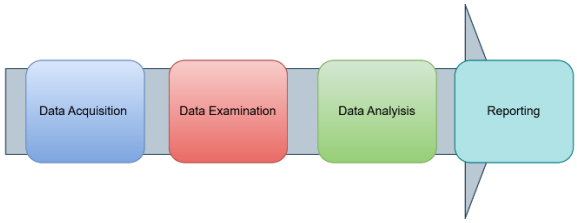

Figure 1 : Digital Forensics Diagram

2.2 Phishing

Phishing is a form of cybercrime that aims to obtain users' sensitive information, such as usernames, passwords, and financial data, through digital deception. In practice, perpetrators typically impersonate trusted entities, such as banks, government agencies, or specific companies, by employing social engineering and technical manipulation. Phishing attacks are generally carried out by spreading fake links via email, social media, or instant messaging that direct victims to websites that resemble official sites. The information entered by victims on these sites can then be used by perpetrators to commit identity theft, financial fraud, or other cybercrimes [17].

2.3 Wireshark

Wireshark is open-source software used to analyze data packets in computer networks. This application can capture and display network traffic in detail, allowing each data packet to be examined based on the information it contains. Wireshark is widely used to identify network problems, monitor communication activities, and evaluate data transmission performance within a system. In addition, Wireshark is often utilized in Quality of Service (QoS) analysis because it can accurately measure parameters such as throughput, packet loss, delay, and jitter. The application also supports various network protocols, making it easier for users to analyze communication processes occurring within a network environment. In the field of digital forensics, Wireshark is frequently used to capture and analyze suspicious network traffic in order to identify communication patterns, packet activities, and data transmission related to cyberattacks. Due to its ability to analyze network traffic comprehensively, Wireshark has become one of the important tools in network monitoring, troubleshooting, and digital forensic investigations[18].

2.4 National Institute of Standards And Technology

The National Institute of Standards and Technology (NIST) is an organization that develops standards and guidelines related to information technology, cybersecurity, and digital forensics. In cybersecurity investigations, the NIST framework is widely used because it provides systematic procedures for handling digital evidence and analyzing cyber incidents. The NIST method consists of four main stages: collection, examination, analysis, and reporting. The collection stage is carried out to collect digital evidence, while the examination stage focuses on extracting and examining data using forensic tools. Furthermore, the analysis stage is used to identify and analyze findings obtained during the investigation process, and the reporting stage is conducted to document the investigation results systematically [19], [20]. The workflow of the NIST method is shown in Figure 2: NIST Process Diagram.

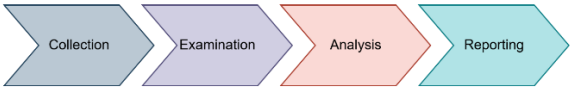

Figure 2 : NIST Process Diagram

2.5 E-commerce

E-commerce is a digital trading system that utilizes the internet to support online transactions, marketing, and business operations. Advances in information technology have made e-commerce more efficient and flexible because it can be accessed anytime and anywhere through internet-connected devices. In addition, digital payment systems and online services have contributed to the rapid growth of the digital economy and expanded market reach at both local and international levels[21].

2.6 Digital Evidence

Digital evidence consists of data or information from electronic devices related to cybercrimes, such as digital documents, communication records, and user activity within network systems[22]. Digital evidence is not physically tangible and is easily modified, thus requiring special handling during digital forensic investigations. In digital forensics, evidence is obtained through the stages of identification, acquisition, and data extraction using specialized software. Such evidence can take the form of images, videos, messages, activity logs, or other digital artifacts that help uncover the perpetrator's activities before and after a cyberattack[23]. Furthermore, digital evidence plays a crucial role in law enforcement as it can be used to trace the perpetrator's identity, determine the chronology of events, and serve as admissible evidence in court in accordance with applicable regulations[24].

2.7 Cybersecurity

Cybersecurity refers to efforts to protect information systems, networks, and data from various threats arising from the use of internet technology. The development of interconnected information technology has made cyberspace a vital component of digital activities, thereby requiring continuous protection. One widely used framework is that of the National Institute of Standards and Technology (NIST), which outlines five key functions: Identify, Protect, Detect, Respond, and Recover to support comprehensive cybersecurity management and incident response.

2.8 Social Engineering

Social engineering is a manipulation technique that involves deceiving victims through social interaction to obtain sensitive information. These attacks exploit human weaknesses such as trust and a lack of vigilance, making them difficult to prevent with security technology alone [25]. Generally, social engineering is divided into two types: human-based methods, such as face-to-face conversations or phone calls, and computer-based methods, such as emails and fake websites. These methods are commonly used by attackers to persuade victims to disclose sensitive information or access malicious websites without realizing the potential risks. This demonstrates that human factors represent a primary vulnerability in cybersecurity. The stages of social engineering are illustrated in Figure 3: Stages of Social Engineering.

Figure 3 : Stages of Social Engineering

The stages of a social engineering attack consist of several processes carried out systematically by the attacker. The first stage is investigation, which involves gathering information about the target, such as personal data, habits, and social media activity, to support attack planning. Next, during the hook stage, the attacker begins establishing communication with the victim to gain their trust via email, instant messaging, or other channels. The next stage is the "play" stage, where the attacker begins manipulating the victim to obtain sensitive information such as passwords, financial data, or access to specific systems. Once the objective is achieved, the attacker moves to the "exit" stage, which involves leaving the target and attempting to erase digital traces to make tracking difficult. Social engineering itself is a form of cyber threat that exploits human vulnerabilities to obtain sensitive information without resorting to technical system hacking [26].

3. RESEARCH METHOD

This study applies the National Institute of Standards and Technology (NIST) digital forensic method, which consists of four stages: collection, examination, analysis, and reporting. Network traffic data was captured using Wireshark and stored in .pcapng format during the collection stage. The captured data was then examined and analyzed to identify phishing domains, IP addresses, TLS communication, and login credentials sent to the phishing website. Finally, all investigation results were documented as digital evidence in the reporting stage, as shown in Figure 4: Stages of the National Institute of Standards and Technology Method.

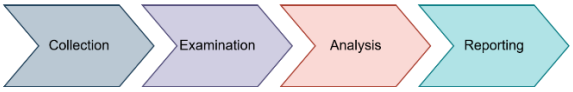

Figure 4 : Stages of the National Institute of Standards and Technology Method

Figure 4 illustrates the stages of the National Institute of Standards and Technology (NIST) digital forensic methodology applied in this study. The collection stage focuses on acquiring digital evidence by capturing network traffic generated during the phishing attack simulation using Wireshark and storing the captured data in .pcapng format. The examination stage involves inspecting the captured network traffic, importing the sslkeylog.log file, and filtering relevant packets to identify communication activities associated with the phishing website. The analysis stage is conducted to interpret the extracted digital evidence, including the identification of the phishing domain, server IP address, TCP and TLS handshake processes, HTTP POST requests, and victim credentials transmitted to the phishing server. Finally, the reporting stage summarizes and documents all digital evidence in a systematic manner to ensure that the investigation results are reliable, verifiable, and suitable for supporting digital forensic investigations of phishing attacks.

4. RESULT AND DISCUSSION

This study analyzes phishing attacks targeting e-commerce services using a three-stage scenario consisting of pre-incident, incident, and post-incident. These stages represent the sequence of events before, during, and after the phishing attack and provide a structured simulation for conducting a digital forensic investigation based on the National Institute of Standards and Technology (NIST) methodology. Each stage was designed to illustrate the phishing process systematically, from the preparation of the attack to the collection and analysis of digital evidence. The first stage, namely the pre-incident, is illustrated in Figure 5.

Figure 5 : Pre-Incident of Phishing Attack Scenario

Figure 5 illustrates the preparation phase of the phishing attack. In this stage, the attacker creates a phishing website that mimics the appearance of the legitimate Shopee login page and prepares a phishing email containing a malicious link. The email is then sent to the victim as part of a social engineering strategy. After receiving the email, the victim is persuaded to access the phishing website without realizing that it is a fraudulent page controlled by the attacker. This stage represents the initial interaction that triggers the phishing attack and prepares the conditions for credential theft.

The second stage, the incident, is illustrated in Figure 6.

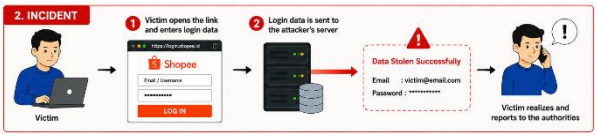

Figure 6 : Post-Incident of Phishing Attack Scenario

Figure 6 depicts the execution phase of the phishing attack. After accessing the phishing website, the victim enters login credentials into the fake login form. The submitted information is immediately transmitted to the attacker's server through an HTTP POST request, allowing the attacker to obtain the victim's email address and password. Once the credentials are successfully captured, the victim realizes the fraudulent activity and reports the incident to the relevant authorities. This stage represents the primary objective of the phishing attack, namely the unauthorized acquisition of sensitive user credentials.

The final stage of the simulation is the post-incident, as presented in Figure 7.

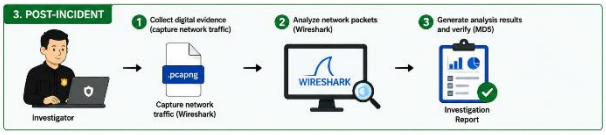

Figure 7 : Post-Incident of Phishing Attack Scenario

Figure 7 illustrates the digital forensic investigation conducted after the phishing incident. Investigators collect digital

evidence by capturing network traffic using Wireshark and storing the captured packets in .pcapng format. The collected evidence is subsequently examined and analyzed to identify communication between the victim and the phishing server, including TCP and TLS handshakes, server IP addresses, phishing domains, and HTTP POST requests containing transmitted credentials. Finally, the investigation results are documented and verified using hash values to ensure the integrity and reliability of the digital evidence before being included in the forensic report.

4.1 Collection

The collection phase involves gathering digital evidence related to phishing activities. In this study, data collection was performed by recording network traffic using the Wireshark application when victims accessed links and logged in to phishing websites. All network communication activities were successfully recorded in .pcapng files, which included TCP, TLS, and HTTP protocols, as well as the IP addresses involved. The capture process was performed in real-time so that the data could be used as digital evidence in subsequent investigation stages. The Wireshark interface during the data collection process is shown in Figure 8: Wireshark Interface.

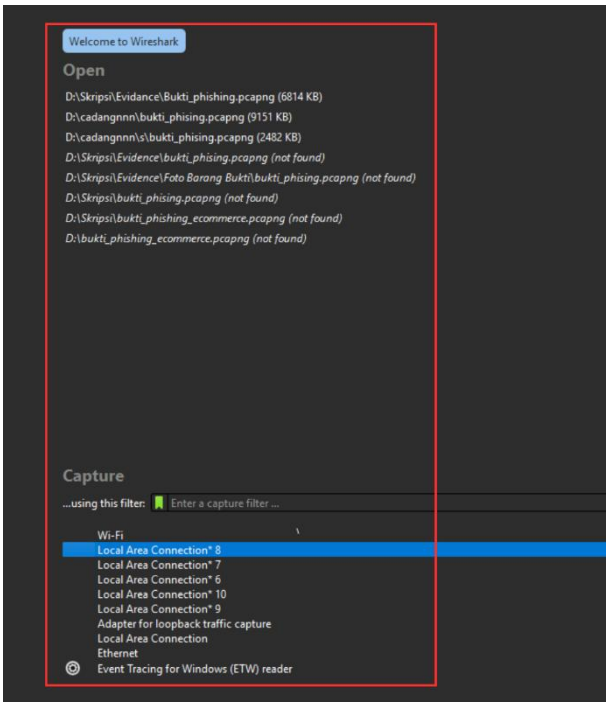

Figure 8 : Wireshark Interface

Before the capture process begins, the system is first configured using the SSLKEYLOGFILE environment variable. This configuration is intended to record session keys from HTTPS communications so that encrypted traffic can be decrypted during the investigation process using the Wireshark application. The generated session keys are then stored in the sslkeylog.log file and used as supporting evidence to assist in the decryption of HTTPS communications secured using the TLS protocol. With this file, investigators can display portions of HTTPS traffic in HTTP format, making the process of analyzing data packets easier. The SSL keylog configuration is shown in Figure 9, SSLKeylog Configuration.

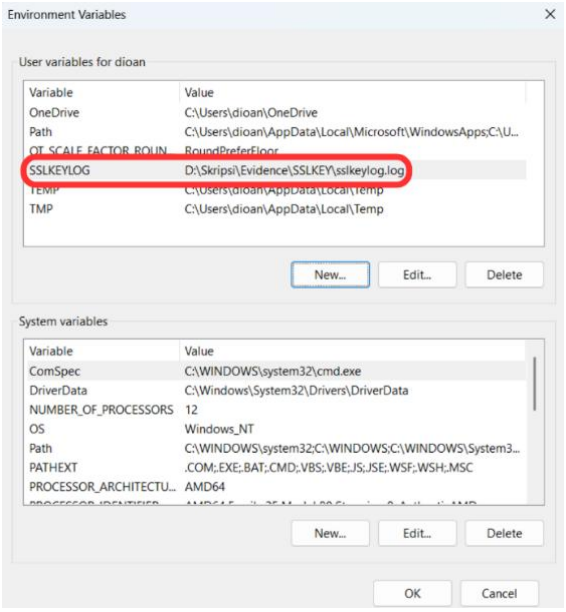

Figure 9 : SSLKEYLOG Configuration

All digital evidence successfully obtained, including network capture files, the sslkeylog.log file, and documentation of phishing activities, is stored in the evidence folder. This process is carried out to preserve the integrity and authenticity of digital evidence throughout the investigation. In addition, organized evidence storage enables investigators to conduct examination, analysis, and reporting systematically and efficiently during subsequent stages of the digital forensic investigation. As shown in Figure 10, Evidence Folder

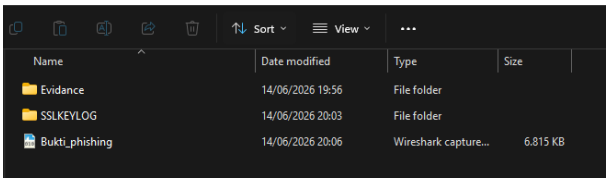

Figure 10 : Evidence Folder

4.2 Examination

The examination phase involves analyzing digital evidence captured from the network using the Wireshark application. The captured .pcapng files are opened and examined to identify network communication activities related to the phishing attack. During this phase, each packet is inspected to observe the communication patterns between the victim's device and the phishing server. An initial analysis of the captured network packets is conducted to determine the protocols used during the communication process, including the source and destination IP addresses, communication ports, transmission timing, and packet exchange sequence. This examination provides an overview of the network traffic generated during the phishing simulation and serves as the basis for the subsequent analysis phase. The network traffic packets captured during the examination process can be seen in Figure 11: Examination of Network Traffic Packets Using Wireshark.

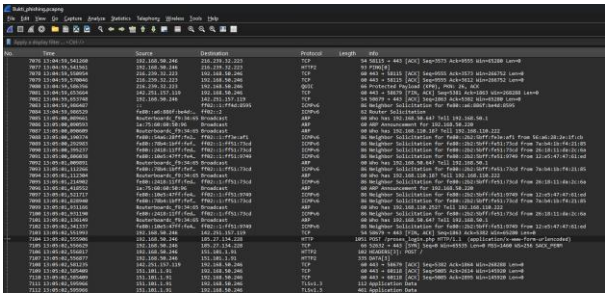

Figure 11 : Examination of Network Traffic Packets Using Wireshark

To assist with HTTPS analysis, the sslkeylog.log file was imported into the TLS configuration in Wireshark so that HTTPS communications could be decrypted. This process enables Wireshark to read the session keys stored in the log file and use them to decrypt encrypted TLS traffic captured during the investigation. After decryption, some of the HTTPS traffic was successfully displayed as HTTP, making it easier to identify the communication flow, inspect transmitted packets, and analyze the victim's login data sent to the phishing server. The decrypted traffic also allowed investigators to observe the interaction between the victim and the phishing website in more detail. The SSL keylog import process is shown in Figure 12: Process of importing an SSLkeylog file into Wireshark to decrypt HTTPS traffic.

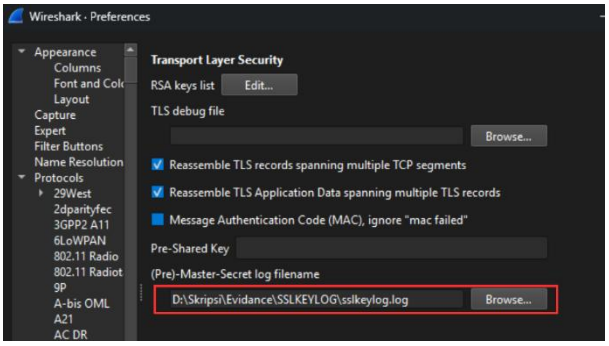

Figure 12 : Process of importing an SSLkeylog file into Wireshark to decrypt HTTPS traffic

The next step involves filtering the captured network packets using several Wireshark display filters, including tls.handshake, tcp, and http. The purpose of this filtering process is to help investigators identify communication packets related to phishing activities so that the examination can be conducted more quickly and effectively. By reducing irrelevant traffic, the analysis can focus on the communication between the victim's device and the phishing server. Through this process, important information such as communication sessions, encrypted traffic, source and destination IP addresses, communication ports, and credential transmission activities can be identified more clearly. The filtering process also assists in organizing the captured network traffic, making it easier to trace suspicious communication patterns and locate digital evidence associated with the phishing attack. Figure 13 shows the process of filtering data packets in Wireshark using several display filters.

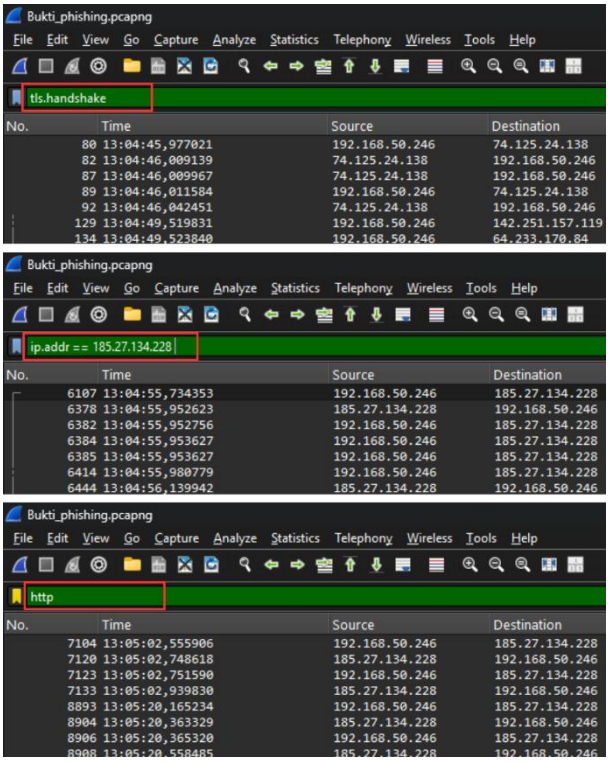

Figure 13 : The Process of filtering data packets in Wireshark uses several filters

4.3 Analysis

In this study, .pcapng files were analyzed using Wireshark to obtain phishing attack evidence. The sslkeylog.log file was used to decrypt TLS communication, allowing HTTPS traffic to be displayed as HTTP. Analysis was conducted using the tls.handshake, IP address 185.27.134.228, and HTTP filters to identify the phishing domain, server communication, and victim login data sent through the HTTP POST method to process_login.php. The filtering process is shown in Table 1: Summary of Wireshark display filters and the data structure used for phishing analysis.

Table 1 : **Summary of Wireshark display filters and the data structure used for phishing analysis**

Data plan	Filtering	Description
Data Plans 6385	tls.handshake	Shows the TLS handshake process between the client and the server
Packages 4548, 4549, and 4550	Ip.addr == 185.27.134.228	Shows communication traffic with the phishing server
Data Plan 4563	http	Displays HTTP request packets (GET and POST)

Based on the filtering results in the Wireshark application, as shown in Table 1, several data packets related to network activity during the phishing attack simulation were successfully identified. These packets contain important information regarding the communication process between the client and

the phishing server, including connection establishment, data transmission, and user credential delivery. The captured packets were then analyzed to identify communication patterns and the transmission of the victim's data to the phishing server. The analysis results are discussed as follows:

1. Data Plans 6385

Based on the results of filtering for "tls.handshake" in Wireshark, packets 6385 show the TLS handshake process between the client and the phishing server during the establishment of an HTTPS connection. Packet 4551 contains a Client Hello message from IP 12.168.50.246 to IP 185.27.134.228 and identifies the phishing domain soppieeeee.free.nf through the SNI value. Meanwhile, packet 6445 shows a Server Hello message indicating that the secure connection was successfully established. The handshake process also demonstrates the exchange of cryptographic parameters used to secure communication between the client and the server. This analysis confirms communication activity between the victim and the phishing server and provides digital evidence that an HTTPS session was initiated successfully. The TLS handshake process is shown in Figure 14: TLS Handshake Process in a File Capture Using Wireshark.

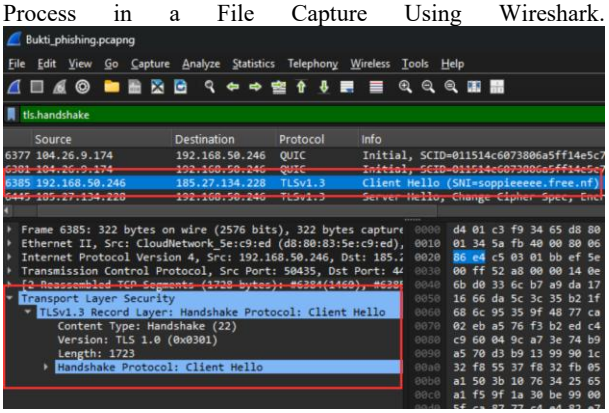

Figure 14 : TLS handshake process in a file capture using Wireshark

2. Data Plans 6414, 6444, and 6445

Based on the results of filtering using ip.addr == 185.27.134.228 in the Wireshark application, packets 6414, 6444, and 6445 show the TCP three-way handshake process between the client and the phishing server through port 443. This process consists of SYN, SYN-ACK, and ACK packets, indicating that the TCP connection was successfully established before encrypted HTTPS communication took place. The successful completion of the three-way handshake confirms that the client device initiated communication with the phishing server and that both devices were ready to exchange application-layer data. Establishing this connection is an essential prerequisite for the subsequent TLS handshake and secure HTTPS communication. The presence of these packets also serves as digital evidence that a network session was successfully created between the victim's device and the phishing server before any credential or web-related data was transmitted. This communication process is illustrated in Figure 15, which presents the TCP three-way handshake process between the client and the phishing server as captured using Wireshark.

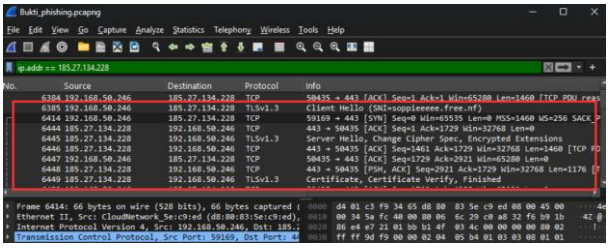

Figure 15 : Three-way handshake process with a phishing server using Wireshark.

3. Data Plan 7104

Based on the HTTP filtering results in Wireshark, packet 7104 shows the transmission of the victim's login data to the phishing server through an HTTP POST request directed to process_login.php. The analysis identified the victim's email and password parameters within the transmitted data, confirming that the phishing website successfully captured sensitive user credentials. This indicates that the phishing page was functioning as intended by harvesting user authentication data and forwarding it directly to the attacker-controlled server for processing. The HTTP POST request also demonstrates that the submitted credentials were transmitted from the victim's device after the login form was completed, providing clear digital evidence of credential theft during the phishing simulation. These findings confirm the effectiveness of network traffic analysis in identifying phishing activities and tracing the transmission of sensitive information. The process is illustrated in Figure 16, which shows the HTTP POST request containing the victim's login data on the phishing website.

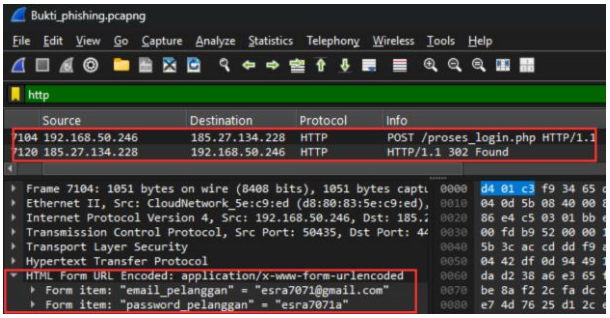

Figure 16 : HTTP POST login data on the phishing website

4.4 Reporting

The reporting phase is the final stage in the National Institute of Standards and Technology (NIST) digital forensics methodology, which aims to systematically present the results of the investigation as digital evidence. In this phase, all findings obtained from the collection, examination, and analysis of the captured network files are compiled, organized, and documented to ensure that the identified digital evidence can be clearly understood, verified, and used as supporting evidence in the investigation process. The reporting process also provides a structured summary of the forensic investigation, enabling investigators to reconstruct the sequence of events and explain how the phishing attack was carried out. Important findings related to phishing activities targeting e-commerce services, including network traffic data, phishing domains, server IP addresses, login credentials, communication protocols, packet analysis results, and communication activities identified from the captured packets, are summarized to provide a comprehensive overview of the

investigation. These findings are presented in Table 2, which summarizes the digital evidence identified throughout the phishing investigation.

Table 2 : Summary of Digital Evidence Findings in the Phishing Case

Elements of Evidence	Value of the Artifact	Status
Network Files	Bukti_phising.pcapng	Main file of traffic data records
File Hash Value	ed1e3419420250e2f6d9b5468e2b0bf5	Ensuring file integrity (Valid)
Server IP Address	185.27.134.228	Location of the perpetrator's phishing server
Phishing Domain	soppieeeee.free.nf	Fake login website address (SNI detected)
Protocols & Script Files	HTTP POST / proses_login.php	Fake login website address (SNI detected)
Encryption Key File	sskeylog.log	TLS secure traffic decryption tool
Victim's Account Leaked	Email: esra7071@gmail.com Password: esra7071a	Sensitive data that was successfully stolen

Table 2 shows that the digital evidence was successfully verified using an MD5 hash to maintain data integrity. The decryption process using the sslkeylog.log file successfully identified the phishing server IP address 185.27.134.228 and the phishing domain soppieeeee.free.nf through the Server Name Indication (SNI) value. In addition, the victim's email and password were found to have been transmitted through an HTTP POST request to process_login.php. The traffic analysis also indicates that HTTP, TLS, and TCP protocols dominated the communication process during the phishing attack simulation. These findings demonstrate that network traffic analysis can provide important digital evidence related to phishing activities, as illustrated in Figure 18: Percentage of Phishing Network Traffic Protocols.

5. CONCLUSIONS

This study investigated phishing attacks on e-commerce services using the National Institute of Standards and Technology (NIST) digital forensic methodology. The investigation successfully identified various digital artifacts, including the phishing domain, server IP address, TCP and TLS communications, HTTP POST requests, and victim credentials transmitted to the phishing server. The findings demonstrate that the NIST methodology, combined with Wireshark and SSL/TLS key logging, provides a systematic and effective approach for collecting, examining, analyzing, and reporting digital evidence related to phishing attacks.

Although this study was conducted using a single phishing simulation, the proposed approach provides a practical framework for investigating similar phishing incidents. Future research should perform a more comprehensive evaluation by applying the methodology to multiple phishing scenarios, different e-commerce platforms, and various web browsers to further validate its effectiveness and generalizability. In addition, comparative studies with other digital forensic frameworks and the integration of automated phishing detection techniques may improve the efficiency and accuracy of future digital forensic investigations.

6. REFERENCES

[1] H. Irawan, A. H. Muhammad, and A. Nasiri, "Design of Cybersecurity Maturity Assessment Framework Using NIST CSF v1.1 and CIS Controls v8," vol. 9, no. 1, p. 2024.

[2] Isaac Dawandakpoye Ohwosoro, "A Filter-Based Feature Selection for Robust Phishing Attack Detection using XGBoost," International Journal of Advanced Research in Science, Communication and Technology, pp. 558–571, Aug. 2024, doi: 10.48175/ijarsct-19372.

[3] P. H. Hussan and S. M. Mangj, "BERTPHIURL: A Teacher-Student Learning Approach Using DistilRoBERTa and RoBERTa for Detecting Phishing Cyber URLs," Journal of Future Artificial Intelligence and Technologies, vol. 1, no. 4, pp. 417–428, Feb. 2025, doi: 10.62411/faith.3048-3719-71.

[4] T. R. Karin, R. R. Sani, F. Alzami, and A. Rohmani, "Enhancing Bank Customer Protection Against Phishing Attacks Through Xgboost-Based Feature Analysis," Transmisi: Jurnal Ilmiah Teknik Elektro, vol. 26, no. 3, pp. 114–121, Jul. 2024, doi: 10.14710/transmisi.26.3.114-121.

[5] F. Ferdynandus, J. Natu Prihanto, and W. Winarno, "Implementing NIST Framework and the People, Process, Technology approach in Indonesian Financial Services," International Journal of Engineering Continuity, vol. 3, no. 1, pp. 172–182, Jul. 2024, doi: 10.58291/ijec.v3i1.265.

[6] I. Riadi, R. Umar, and M. I. Syahib, "Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)," Jurnal RESTI, vol. 5, no. 1, pp. 45–54, Feb. 2021, doi: 10.29207/resti.v5i1.2626.

[7] A. Wijayanto, I. Riadi, and Y. Prayudi, "TAARA Method to Processing on the Network Forensics in the Event of an ARP Spoofing Attack," Jurnal RESTI, vol. 7, no. 2, pp. 208–217, Apr. 2023, doi: 10.29207/resti.v7i2.4589.

[8] R. Hidayat and N. Anwar, "Forensic Analysis Of Web Phishing And Social Engineering Using The National Institute Of Standards And Technology Method Case Study Of Facebook Account Data Theft," Journal of Digital Security and Forensics, vol. 1, no. 1, Jul. 2024, doi:

10.29121/digisecforensics.v1.i1.2024.14.

[9] A. Wibowo Noor Fikri et al., "Analisis Keamanan Sistem Operasi dalam Menghadapi Ancaman Phishing dalam Layanan Online Banking," Jurnal Ilmu Multidisplin, vol. 2, no. 1, pp. 84–91, Jun. 2023, doi: 10.38035/jim.v2i1.228.

[10] M. A. H Nasution and J. D. Santoso, "Analysis of Community Awareness Against Threats to Personal Data Security Through Phishing Websites," The IJICS (International Journal of Informatics and Computer Science), vol. 5, no. 2, p. 102, Aug. 2021, doi: 10.30865/ijics.v5i2.3053.

[11] D. Wina et al., "The Importance of Security Awareness in Combating Phishing Attacks: A Case Study of Bank Rakyat Indonesia Article Info ABSTRACT," Journal of Social Sciences and Humanities, vol. 14, no. 3, 2024.

[12] R. Hanipah and H. Dhika, "Analisa Pencegahan Aktivitas Ilegal Didalam Jaringan Dengan Wireshark," Journal of Computer and Information Technology, vol. 4, no. 1, 2020, [Online]. Available: http://e-journal.unipma.ac.id/index.php/doubleclickTelepon:

[13] A. Nofiyan, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology," CYBERNETICS, vol. 4, no. 02, pp. 79–92, 2020, [Online]. Available: https://centralops.net

[14] G. Nurmansyah, G. Arya, B. Wiranata, A. I. Fardiansyah, and S. V. Mladenov, "Preventing AI-based phishing crimes across national borders through the reconstruction of personal data protection laws," Nurmansyah, vol. 15, no. 2, pp. 286–311, 2024, [Online]. Available: http://www.apwg.org.

[15] I. Ainur Rafiq, I. Riadi, F. Teknologi Industri, and U. Ahmad Dahlan, "Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST," MEI, 2022.

[16] R. Andhika Surya, F. Ridho, and D. T. Yuwono, "Analisis Bibliometrik Menggunakan Vosviewer Terhadap Trend Digital Forensik Pada Saat Pemilu Indonesia The Bibliometric Analysis Using VOSviewer on Digital Forensics Trends During the Indonesian Election," 2024. [Online]. Available: http://journal.umpalangkaraya.ac.id/index.php/pencerah

[17] M. Nadhif Hermanto, "Analisis Forensic Berbasis Web Phising Menggunakan Metode National Institute Of Standards And Technology," Cipta Cendikia Kotabumi Jurnal informasi dan Komputer, vol. 11, no. 1, p. 2023, 2023.

[18] R. Adiputera Tangahu, A. Bode, M. Kom, and S. Taliki, "Analisa Kualitas Layanan Jaringan Internet Pada Wireless Lan Menggunakan Metode Qos (Quality Of Service) (Studi kasus : Kedai Mako)," Jurnal Ilmiah Ilmu Komputer Banthayo Lo Komputer, vol. 3, no. 1, 2024.

[19] S. Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti, I. Riadi, N. Hamida Siregar, P. Studi Sistem Informasi, F. Sains dan Teknologi Terapan, and U. Ahmad Dahlan, "Terakreditasi SINTA Peringkat 4 Forensik Mobile Pada Kasus Cyber Fraud Layanan Signal Messenger Menggunakan Metode NIST," 2018.

[20] I. Riadi, F. Tella, S. Informasi, F. Sains dan Teknologi Terapan, and U. Ahmad Dahlan, "Analisis Forensik pada Email Menggunakan Metode National Institute of Standards Technology," MEI, 2022.

[21] R. Nur, R. Pusdiklat, B. Siber, and S. Negara, "Cendekia Niaga Journal of Trade Development and Studies Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia," 2022.

[22] A. E. Saragih, N. Christian, and P. Khoirunisa, "Media Hukum Indonesia (MHI) Analisis Penggunaan Barang Bukti Digital di Dalam Sistem Hukum di Indonesia (Studi Kasus Putusan Nomor 3 K/PID.SUS/2019)," vol. 2, no. 2, p. 504, 2024, doi: 10.5281/zenodo.12082755.

[23] I. Ainur Rafiq, I. Riadi, F. Teknologi Industri, and U. Ahmad Dahlan, "Perbandingan Forensic Tools pada Instagram Menggunakan Metode NIST," MEI, 2022.

[24] Shinta Widhaningroem and Yeni Widowaty, "Digital Evidence Tracing in the Investigation of Identity Theft in the E-Commerce Era," Formosa Journal of Social Sciences (FJSS), vol. 3, no. 2, pp. 287–300, Jun. 2024, doi: 10.55927/fjss.v3i2.9797.

[25] K. Sarpong Adu-Manu, R. Kwasi Ahiable, J. Kwame Appati, and E. Essel Mensah, "Phishing Attacks in Social Engineering: A Review," Journal of Cyber Security, vol. 4, no. 4, pp. 239–267, 2022, doi: 10.32604/jcs.2023.041095.

[26] E. W. Tyas Darmaningrat et al., "Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi," Sewagati, vol. 6, no. 2, Feb. 2022, doi: 10.12962/j26139960.v6i2.92.