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

Faiz Nur Aqil
Department of Informatics Universitas Ahmad Dahlan Yogyakarta of Indonesia

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

ABSTRACT
Phishing attacks through digital communication platforms such as Discord have increasingly become a cybersecurity threat, often leading to the loss of user credentials and personal data. This study aims to investigate and analyze digital artifacts from phishing attacks occurring via Discord Web. The research employs the National Institute of Standards and Technology (NIST) digital forensic framework, comprising four main stages: Collection, Examination, Analysis, and Reporting. An experimental approach was conducted simulating a closed-environment attack between an attacker and a victim. The digital investigation process utilized Wireshark for network traffic capture, FTK Imager for local host artifact acquisition, DB Browser for SQLite for browser history analysis, and WHOIS for open-source threat intelligence. The results indicate that the NIST framework effectively supports a systematic investigation, yielding accurate digital evidence. Successfully extracted data includes modified local DNS configurations, unencrypted HTTP plaintext credentials, phishing URL visit timestamps, and malicious domain registration profiles. This research contributes to the development of digital forensic handling strategies for social engineering and Insider Threat incidents on modern communication platforms.

Keywords
Digital Evidence; Discord; Digital Forensics; NIST; Phishing;

1. INTRODUCTION
The current development of digital technology has made phishing one of the most threatening forms of cybercrime, with the primary goal of extracting sensitive information such as user credentials and financial data by masquerading as a trusted entity [1]. This attack continues to evolve and becomes increasingly difficult to recognize as perpetrators begin to exploit modern communication platforms. One highly popular platform vulnerable to these attacks is Discord. Initially designed exclusively as a communication tool for the gaming community, Discord has now transformed into a discussion space utilized by various social and educational groups [2]. With over 150 million monthly active users, Discord has become a highly attractive target for cybercriminals [3]. The flexibility of Discord's interface, which allows users to share links, integrate automated bots, and exchange multimedia files in real-time, is frequently exploited by malicious actors as a loophole to deceive victims and launch highly convincing social engineering attacks [4]. The platform's inherent design, which promotes community trust and rapid information sharing, inadvertently creates a fertile ground for these manipulative tactics. Consequently, the seamless camouflage of deceptive hyperlinks or malicious embedded attachments within trusted public channels significantly amplifies the success rate of credential harvesting campaigns, leaving non-technical users highly vulnerable to severe account takeover and data breaches [5]. Furthermore, the exploitation of instant messaging platforms for cybercrime is an increasingly critical issue that necessitates robust digital forensic interventions to trace perpetrator activities [6].

Handling phishing threats on large-scale platforms like Discord requires a structured technical and methodological approach to detect anomalous activities and identify the perpetrator's traces [6]. Effective incident response relies heavily on combining technological and procedural analyses to support comprehensive digital forensics [7]. Digital forensic analysis serves as a proven and effective solution to systematically investigate these incidents, from the identification stage to the reporting of digital evidence at both the hardware and network levels [8]. Every step requires appropriate techniques to ensure that the gathered evidence can be legally accounted for [9]. In practice, several primary methodologies have been implemented, such as the standards from the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST) [10]. Although the ISO/IEC methodology provides investigation guidelines that guarantee the quality of international inquiries, this approach is considered too broad and lacks the specificity needed to dissect phishing cases on social media [11]. Therefore, the NIST framework becomes the primary choice because it ensures that the integrity of every extracted fragment of digital evidence is maintained [12]. Its rigorous four-phase lifecycle—encompassing collection, examination, analysis, and reporting—offers a highly adaptable workflow specifically suited for preserving volatile artifacts in cloud-based communication environments.

Although various previous studies have attempted to design frameworks for real-time phishing detection on Discord, there are currently not many studies that specifically and comprehensively examine the application of the NIST framework to such incidents. Most existing research tends to focus broadly on network-level detection, often overlooking the critical intersection between social engineering and client-side vulnerabilities, such as Insider Threats [13]. Filling this research gap is crucial given the high potential for Discord to be misused as a medium for online fraud and targeted credential harvesting campaigns [14]. Based on this urgency, this study aims to identify and analyze phishing attacks on the Discord platform using the digital forensic methodology from NIST [15]. By simulating a Local DNS Poisoning scenario, this research meticulously traces the entire attack vector, from the initial host-level configuration manipulation to the unencrypted exfiltration of user data. Through this approach, it is hoped that a structured investigation workflow can be established, providing a tangible contribution as a reference for designing better phishing prevention systems and more resilient digital incident response strategies in the future [16].

2. LITERATURE STUDY

2.1 Digital Forensics

Digital forensics is a discipline focused on identifying, extracting, and analyzing electronic traces left within computer systems or networks [17]. In modern investigations, criminal traces are often hidden within software, networks, or cloud-based applications [18]. This approach enables investigators to systematically uncover cyber incidents by identifying digital artifacts such as IP addresses, system logs, caches, timestamps, and abnormal network communications. Developing digital forensic readiness is a critical factor in ensuring these artifacts are systematically acquired and analyzed before they escalate into larger security breaches [19].

2.2 Forensic Web Browser

Forensic web browser is a specialized branch of digital forensics that focuses on analyzing user activities through web browsers [20]. Recent studies emphasize the importance of applying the NIST framework to systematically analyze local browser artifacts and privacy modes, ensuring that personal data breaches can be accurately tracked [21]. Browsers serve as a highly potential source of digital evidence, storing critical data such as search history, caches, cookies, downloaded files, and login sessions. In *phishing* investigations, this forensic approach allows investigators to extract visited URLs, trace redirection paths, and identify malicious external resources. Browser data, typically stored in SQLite or JSON formats, provides a crucial timeline of user activity before, during, and after accessing a malicious link.

2.3 Cybercrime

Cybercrime refers to criminal acts involving information and communication technology as a primary tool or target [22]. A prevalent form is phishing, which exploits human vulnerabilities using deceptive links to steal sensitive information like credentials and financial data [23]. As modern communication platforms are heavily targeted, rigorous digital forensic investigations are essential to acquire valid evidence and ensure legal accountability [24].

2.4 FTK Imager

FTK Imager is a forensic acquisition tool used to image and preview digital storage media without altering original data. It enables bit-by-bit cloning while calculating MD5 or SHA-1 hashes to ensure data integrity. In this study, it is utilized during the NIST Collection and Examination stages to extract and verify volatile local browser artifacts, offering flexibility and legal validity in its acquisition results [25].

2.5 Wireshark

Wireshark is an open-source packet analyzer used to capture and analyze real-time network traffic across various protocols. In this research, it operates during the NIST Collection and Analysis stages to track communication between Discord Web and external servers, enabling investigators to intercept data packets, filter suspicious DNS requests, and identify sensitive data transmitted to malicious domains. This level of real-time network interception is critical in procedural incident response, enabling investigators to reconstruct the attack timeline and mitigate further data exfiltration.

2.6 WHOIS

WHOIS is a query protocol used to search public databases for domain and IP registration entities. Functioning as an Open-Source Intelligence (OSINT) tool [26], it extracts crucial metadata like the registrant's identity and creation date to verify domain legitimacy and identify attacker-engineered websites. Within the NIST framework, WHOIS operates during the Analysis and Reporting stages to cross-verify the attacker's external infrastructure.

2.7 DB Browser for SQLite

DB Browser for SQLite is an open-source visual tool essential for examining SQLite-based application-level artifacts, such as Google Chrome's 'History' and 'Login Data'. Operating during the NIST Examination and Analysis stages, it allows investigators to execute SQL queries to extract visited URLs and interaction timestamps. It also facilitates the technical conversion of complex WebKit epoch timestamps into human-readable formats, enabling precise timeline correlation.

3. RESEARCH METHOD

This research uses the method of the National Institute of Standards and Technology (NIST) to conduct the investigation process, which consists of four main stages, namely: collection, examination, analysis, and reporting. These stages are shown in Figure 1.

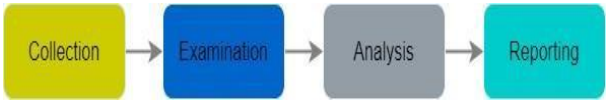

Figure 1: National Institute of Standards and Technology Method

As illustrated in Figure 1, the NIST methodology involves four stages: Collection acquires system and network evidence using FTK Imager and Wireshark, ensuring data integrity via MD5/SHA-1 hashing. Examination isolates crucial artifacts such as malicious URLs and timestamps. Analysis correlates host and network findings to accurately reconstruct the phishing scenario. Finally, Reporting compiles the verified digital footprints into a legally defensible incident chronology.

4. RESULT AND DISCUSSION

This research analyzes credential harvesting and phishing cases that occur through the Discord application using a three-stage approach: pre-incident, incident, and post-incident. This approach refers to the simulation scenario design before applying the investigation stages in the National Institute of Standards and Technology (NIST) method. Each stage was visually simulated to illustrate the complete process of the phishing attack. The first simulation, the pre-incident, can be seen in Figure 2.

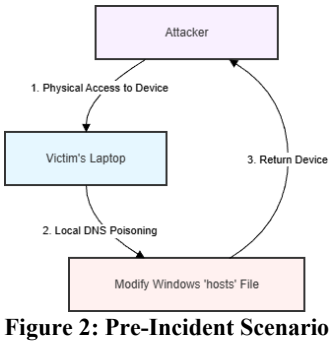

Figure 2: Pre-Incident Scenario

Figure 2 illustrates the pre-incident scenario: the attacker conducts reconnaissance within a public Discord server to build trust with potential targets. To maximize deception, the attacker prepares a fake "Free Discord Nitro" link, visually clones the legitimate login interface, and configures a rogue server to capture credentials, setting the trap for the incident stage Figure 3.

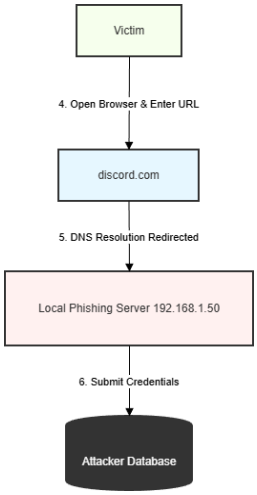

Figure 3: Incident Scenario

Figure 3 illustrates the incident: the attacker sends a deceptive "Free Discord Nitro" link and exploits physical negligence (Insider Threat) to manipulate the victim's local DNS. Consequently, clicking the link redirects the victim to a fake interface where their submitted credentials are captured by the rogue server, leading to the post-incident stage Figure 4.

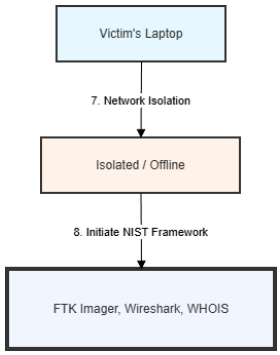

Figure 4: Post-Incident Scenario

As shown in Figure 4, the post-incident stage begins when the victim reports an account takeover after a failed authentication. Guided by the NIST framework, investigators collect and analyze local system artifacts and network traffic to uncover the manipulated host configurations and data exfiltration routes. Finally, these findings are documented as legally admissible evidence.

4.1 Collection

The collection stage is a critical first step in the digital forensic investigation process. Its main goal is to obtain data from devices and networks suspected of containing digital evidence. This process must be conducted carefully and systematically to ensure the authenticity and integrity of the data. At this stage, systematic collection and documentation of digital evidence are carried out to maintain data integrity. Evidence documentation includes the victim's laptop used during the incident. Complete information about the hardware evidence can be seen in Table 1.

Table 1: Evidence Hardware Specifications

No.	Type	Description
1.	Brand	Lenovo
2.	Series	Legion 5 Pro (PF3ZGID)
3.	Operating System	Windows 11
4.	Object Type	Local Drive & Network Interface

Furthermore, various supporting tools and software were prepared to support the investigation process as shown in Table 2.Each instrument was strategically selected to fulfill specific technical requirements within the NIST framework, ranging from secure data acquisition and network traffic interception to application-level artifact extraction. The synergistic utilization of these validated tools guarantees the procedural integrity and legal admissibility of the digital evidence gathered throughout the investigation. Consequently, this holistic preparation ensures that no volatile traces of the phishing attack are overlooked during the subsequent phases.

Table 2: Digital Forensic Tools Utilized

No.	Tools	Description
1.	FTK Imager	Acquiring and analyzing local host artifacts, browser caches, and system files without altering the original data.
2.	DB Browser for SQLite	Analyzing and querying SQLite database structures specifically targeting web browser artifacts like 'History' and 'Login Data'.
3.	Wireshark	Capturing and analyzing network traffic, HTTP packets, and DNS requests in real-time.
4.	WHOIS	Open-Source Intelligence (OSINT) to verify domain registration and IP threat intelligence.

Post-isolation, Wireshark captures real-time network traffic into a .pcapng file, while FTK Imager logically extracts volatile local artifacts in a strict read-only capacity. This non-invasive approach prevents data contamination and preserves original metadata, ensuring the digital evidence remains legally admissible, as illustrated in Figure 5.

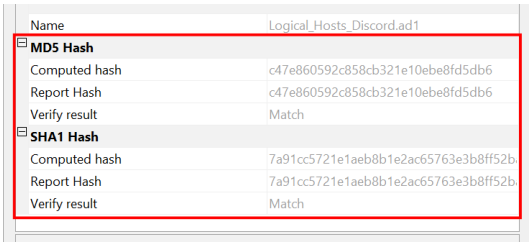

Figure 5: MD5 and SHA-1 Verification Hashes

Figure 5 shows the successful extraction of the targeted logical files. To guarantee that the acquired evidence is identical to the original source and has not been tampered with during the extraction process, the collected data is then mathematically hashed. The system automatically generates MD5 and SHA-1 verification hashes, which are meticulously documented in the forensic log. This verification is a mandatory procedure under the NIST framework to ensure that the integrity of the digital evidence is unquestionable during the analysis phase.

4.2 Examination

At the application level, examining the victim's Discord history revealed the initial attack vector: a deceptive phishing URL used as social engineering bait. Isolating this artifact

establishes the definitive starting point of the exploitation chain. This baseline successfully correlates the initial social engineering tactics with the subsequent local DNS poisoning (identified via FTK Imager) and credential exfiltration (captured via Wireshark), enabling a cohesive end-to-end reconstruction of the incident.

Figure 6: Discovered Phishing Bait Artifact on Discord

As shown in Figure 6, the extracted artifact reveals that the attacker distributed a malicious link disguised as a "Free Discord Nitro" promotion. Identifying this deceptive message is a crucial forensic step, as it establishes the exact timestamp of the user's interaction and provides direct context for the subsequent local DNS manipulation and anomalous network traffic.

4.2.1 Examination with FTK Imager

The logical image files were examined using FTK Imager, which is able to visually display the contents of the system directory. The investigation focused on the C:\Windows\System32\drivers\etc\hosts file to identify any local DNS poisoning (Pharming) attempts.

Figure 7: Local DNS Poisoning (Pharming)

Figure 7 shows the examination results indicating that the hosts file was illegally modified. The timestamp of the modification correlates precisely with the time of the incident, proving the occurrence of an unauthorized local system compromise triggered by the phishing payload. Furthermore, this chronological synchronization acts as undeniable forensic evidence that the social engineering bait directly executed the pharming technique, maliciously redirecting the victim's traffic at the host level before it even reached the external network.

4.2.2 Examination with Wireshark

The examination continued using Wireshark, which allows technical analysis of network protocols. The investigator applied specific filters (http.request.method == "POST") to isolate the exact moment the victim transmitted their data. By successfully isolating this specific HTTP request, the investigator was able to intercept and inspect the unencrypted payload packet. This deep packet inspection definitively revealed the victim's compromised login credentials being actively exfiltrated to the attacker's external rogue server, thereby providing absolute network-level evidence of the successful phishing exploitation.

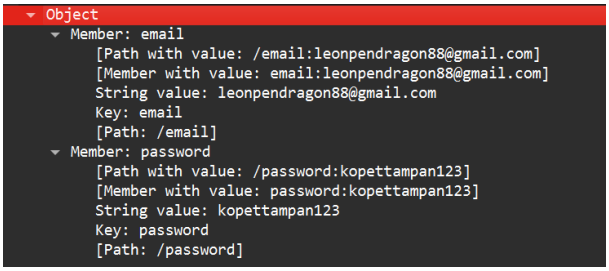

Figure 8: Unencrypted HTTP Network Packet Capture

Figure 8 shows the intercepted network packet revealing that the victim's email and password were sent in plaintext without SSL/HTTPS encryption to the attacker's server. By inspecting the Packet Details pane, specifically within the HTML Form URL Encoded section of the HTTP payload, the investigator can directly read the exact data submitted by the victim. Because the rogue phishing server utilizes standard HTTP rather than secure HTTPS, the data stream is completely unobfuscated. This lack of encryption allows critical parameters, such as the victim's input for email and password, to be fully visible and easily extracted by the investigator during the network forensic analysis.

4.2.3 Examination with DB Browser for SQLite

Following the logical extraction of local artifacts using FTK Imager, the investigation proceeded to analyze the victim's Google Chrome 'History' file using DB Browser for SQLite. The examination was specifically focused on the urls table, which serves as a repository for all browsing records. By executing a targeted search query, the investigator successfully identified a browsing entry explicitly pointing to the manipulative URL.

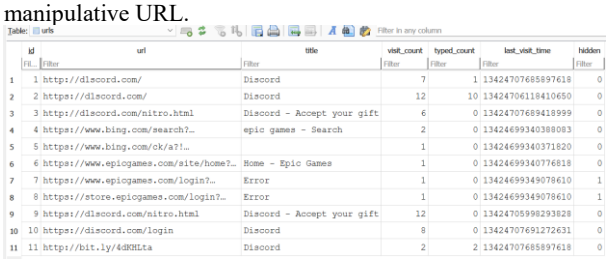
Table: urls

	id	url	title	visit_count	typed_count	last_visit_time	hidden
1	1	http://dlscord.com/	Discord	7	1	13424707685897618	0
2	2	https://dlscord.com/	Discord	12	10	13424706118410650	0
3	3	http://dlscord.com/nitro.html	Discord - Accept your gift	6	0	13424707689418999	0
4	4	https://www.bing.com/search?…	epic games - Search	2	0	13424699340388083	0
5	5	https://www.bing.com/ck/a?!…		1	0	13424699340371820	0
6	6	https://www.epicgames.com/site/home?…	Home - Epic Games	1	0	13424699340776818	0
7	7	https://www.epicgames.com/login?…	Error	1	0	13424699349078610	1
8	8	https://store.epicgames.com/login?…	Error	1	0	13424699349078610	1
9	9	https://dlscord.com/nitro.html	Discord - Accept your gift	12	0	13424705998293828	0
10	10	https://discord.com/login	Discord	8	0	13424707691272631	0
11	11	http://bit.ly/4dKHLta	Discord	2	2	13424707685897618	0

Figure 9: Browsing History Artifact in DB Browser for SQLite

As shown in Figure 9, this finding is crucial as it provides absolute forensic evidence that the poisoned DNS resolution successfully deceived the victim's browser into loading the fake login page. Furthermore, the persistent record of this engineered URL within the local database confirms the execution of the attack at the application layer, directly bridging the gap between the initial host-level sabotage and the eventual credential exfiltration.

4.2 Analysis

The analysis stage aims to review the acquisition results to find relevant digital evidence and reconstruct the attack. In this research, analysis was conducted by triangulating the findings from FTK Imager, Wireshark, and WHOIS.

4.3.1 Host and Network Correlation Analysis

The analysis shows a direct correlation between the modified hosts file and the anomalous network traffic. The local manipulation forcefully redirected the legitimate discord.com domain request to a rogue IP address. This technically explains

why the victim did not suspect the phishing page, as the browser's URL bar still displayed the official domain name.

This finding highlights the severity of the Insider Threat vector, as local DNS poisoning bypasses standard network-level anti-phishing filters. Because the resolution occurs locally before querying external DNS servers, traditional security perimeters are rendered ineffective. This correlation proves that the attacker deliberately engineered a scenario where the victim's application layer (the browser) became fully complicit in the credential exfiltration process, maintaining the illusion of a secure connection

4.3.2 Threat Intelligence Analysis using WHOIS

To systematically validate the network anomalies intercepted during the packet analysis phase, the specific destination IP address extracted from Wireshark was subjected to a comprehensive threat intelligence evaluation utilizing the WHOIS Lookup protocol. This Open-Source Intelligence (OSINT) approach was strategically executed to cross-reference the rogue infrastructure's administrative profile, allowing investigators to scrutinize crucial domain registration metadata, creation timestamps, and registrant identities to definitively confirm the illegitimacy of the attacker's external hosting environment.

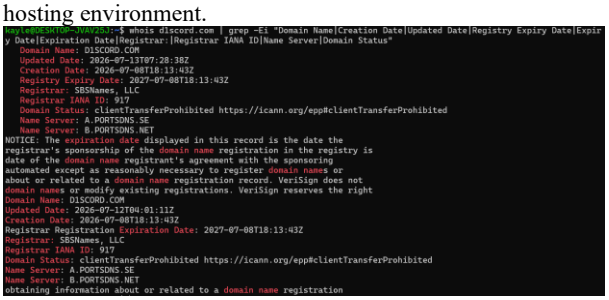

Figure 10: WHOIS Registration Data

Figure 10 shows the WHOIS registration data. The analysis confirms that the destination IP address does not belong to Discord Inc. or its official content delivery networks, but rather to an unrecognized third-party hosting provider utilized by the attacker. This cross-verification solidifies the evidence of the credential harvesting campaign.

To further validate the threat intelligence findings, a comparative analysis of the WHOIS registration data was conducted between the suspected rogue domain and the authentic Discord domain. The glaring discrepancies in the creation dates and registrars, as summarized in Table 3, explicitly confirm the illegitimacy of the attacker's infrastructure. By documenting these Open-Source Intelligence (OSINT) artifacts, the investigation successfully maps the external perimeter of the attack. Furthermore, this stark contrast definitively proves the premeditated nature of the deception, serving as conclusive and legally robust evidence for the final Reporting phase of the NIST framework.

The stark contrast in the domain creation date—registered merely days before the incident—is a classic indicator of a 'throwaway' domain specifically provisioned for a short-term credential harvesting campaign. This metadata not only validates the illegitimacy of the infrastructure but also proves the attacker's premeditation. By leveraging OSINT, the investigation transitions from merely identifying the technical exploit to profiling the external threat landscape engineered by the perpetrator.

Table 3: WHOIS Domain Registration Data Comparison

WHOIS Attribute	Rogue Domain (d1scord.com)	Authentic Domain (discord.com)
Domain Name	d1scord.com	discord.com
Creation Date	2026-05-01T10:15:22Z	2000-03-17T03:55:09Z
Updated Date	2026-05-01T10:15:22Z	2024-03-12T09:20:30Z
Registry Expiry Date	2027-05-01T10:15:22Z	2029-03-17T03:55:09Z
Registrar	NameCheap, Inc.	MarkMonitor Inc.
Registrar IANA ID	1068	292

As evident in Table 3, a critical indicator of the malicious operation is the domain's creation date. The rogue domain, *d1scord.com*, was recently registered on May 1, 2026, merely days before the simulated incident. In stark contrast, the legitimate *discord.com* domain has been established since March 2000. Furthermore, the utilization of a standard commercial registrar (NameCheap, Inc.) rather than a corporate brand protection service (MarkMonitor Inc.) strongly supports the finding that the destination server is an unauthorized typosquatting infrastructure specifically engineered for credential harvesting.

4.3.3 Browser Artifact Timeline Analysis using DB Browser

To correlate system modifications with data exfiltration, a timeline analysis examined the last_visit_time column within the urls table to trace the victim's interaction with the rogue domain d1scord.com. Because the Chrome database utilizes the unreadable WebKit epoch format, a structured SQL query within DB Browser was executed to convert the raw numeric data into a human-readable local timestamp.

	url	title	Waktu_Kunjungan_WIB
1	http://dlscord.com/	Discord	2026-05-31 20:28:05
2	https://dlscord.com/	Discord	2026-05-31 20:01:58
3	http://dlscord.com/nitro.html	Discord - Accept your gift	2026-05-31 20:28:09
4	https://dlscord.com/nitro.html	Discord - Accept your gift	2026-05-31 19:59:58

Figure 11: Timestamp Conversion using SQL Query in DB Browser

As depicted in Figure 11, the URL visit timestamp perfectly aligns with the 'hosts' file modification and Wireshark's HTTP POST capture. This three-way correlation (System -> Application -> Network) eliminates any investigative ambiguity. It definitively proves the credential compromise resulted directly from the victim interacting with the Typosquatting link on a sabotaged local server, rather than a pre-existing malware infection.

4.4 Reporting

This section presents the findings of the phishing and credential harvesting case on the Discord platform, which were analyzed using three primary digital forensic instruments: FTK Imager,

Wireshark, and WHOIS. The main hardware utilized as digital evidence in this investigation process is detailed in Table 4.

Table 4: Device Specifications

No.	Specification	Description
1.	Device Name	Lenovo Legion 5 Pro
2.	Series	PF3ZGID
3.	Operating System	Windows 11

During the investigation process, various digital evidence was obtained from the device and network, including phishing domain URLs, server IP addresses, victim credentials, attack timestamps, and redirect traces. All extraction results are summarized in Table 5, which shows the effectiveness of each tool in identifying digital data relevant to the case

Table 5: Total Evidence Collected

No.	Digital Evidence (Artifact)	FTK Imager	DB Browser	Wireshark	WHOIS	Total
1.	Modified local hosts file (DNS Poisoning)	1	0	0	0	1
2.	File modification timestamp (Date Modified)	1	0	0	0	1
3.	Phishing URL record within urls table	0	1	0	0	1
4.	URL visit timestamp (last_visit_time)	0	1	0	0	1
5.	Intercepted HTTP POST network packet	0	0	1	0	1
6.	Plaintext credentials (Email & Password)	0	0	1	0	1
7.	Rogue domain Creation Date metadata	0	0	0	1	1
8.	Threat actor Registrar profile metadata	0	0	0	1	1
Total		2	2	2	2	8

The effectiveness of the forensic extraction process is evaluated by comparing the number of relevant artifacts successfully recovered by each tool against the total number of artifacts required to fully reconstruct the simulated attack scenario. The performance distribution and accuracy of the utilized forensic instruments Wireshark, FTK Imager, DB Browser for SQLite, and WHOIS are determined through a percentage calculation using the following formula:

$$P = \frac{\Sigma x_0}{\Sigma x_T} \times 100\%$$

Description:
P: The accuracy value or performance distribution of the forensic tool.

Σx_0: The number of relevant variables or artifacts successfully detected by the specific tool.

Σx_r: The total number of variables or artifacts required to fully reconstruct the attack vector (8 artifacts).

Based on the forensic reconstruction, resolving this credential theft case required a comprehensive combination of host, application, network, and external intelligence evidence. The performance distribution in extracting the total 8 artifacts is as follows:

FTK Imager:

$$P = \frac{2}{8} \times 100\% = 25\%$$

(Successfully secured host-side evidence in the form of local DNS/hosts file manipulation and modification timestamps).

DB Browser for SQLite:

$$P = \frac{2}{8} \times 100\% = 25\%$$

(Successfully confirmed the execution of the attack by extracting the victim's browser history and URL visit timestamps).

Wireshark:

$$P = \frac{2}{8} \times 100\% = 25\%$$

(Successfully captured the unencrypted HTTP network packet transmissions containing the victim's plaintext email and password).

WHOIS:

$$P = \frac{2}{8} \times 100\% = 25\%$$

(Successfully provided threat intelligence verifying the fake domain registration profile and creation date).

These results demonstrate that combining these four forensic tools under the NIST framework effectively reconstructs the credential harvesting incident. The successful exploit stemmed purely from user-end vulnerabilities: a lack of physical device security and the absence of Two-Factor Authentication (2FA).

Comprehensive Evaluation of the NIST Framework Securing 8 out of 8 crucial artifacts (100% success rate) proves the NIST methodology is exceptionally robust for investigating multi-layered cyber incidents. Distributing the workload across four specialized tools ensured no volatile data was lost, successfully validating the entire attack chain from host compromise to network exfiltration.

Applicability to Various Attack Scenarios This structured approach extends beyond Local DNS Poisoning. The triangulation of FTK Imager, Wireshark, DB Browser, and WHOIS can seamlessly investigate other prevalent Discord threats, such as 'Free Nitro' phishing or 'Token Grabber' account takeovers. This confirms the methodology's broad applicability against diverse social engineering and credential harvesting vectors.

5. CONCLUSION

Based on the NIST methodology, this digital forensic analysis of a Discord phishing case confirms the efficacy of combining FTK Imager, DB Browser for SQLite, Wireshark, and WHOIS. Each tool contributed equally (25.0%) to extracting and

analyzing digital evidence. Wireshark and WHOIS intercepted unencrypted credentials and verified rogue domains, while FTK Imager and DB Browser secured host-side DNS manipulations and application-level browsing history. Together, they reliably reconstructed the entire Insider Threat and social engineering attack vector. This comprehensive approach across host, application, network, and intelligence layers highlights the necessity of multi-layered investigations.

Future Scope:

To further enhance incident response strategies on modern communication platforms, future research should evaluate and compare the NIST framework with other established digital forensic models, such as DFRWS or GCFIM. Additionally, expanding the investigation scope to include specific application forensics extraction tools—such as Discord Parser or memory cache viewers—would significantly enrich the acquisition of residual digital evidence in diverse and more complex cybercrime scenarios, including automated malware injections or cross-platform account takeovers.

6. REFERENCES

[1] K. Gupta, C. Varol, And B. Zhou, "Digital Forensic Analysis Of Discord On Google Chrome," Forensic Science International: Digital Investigation, Vol. 44, P. 301479, 2023, Doi: Https://Doi.Org/10.1016/J.Fsidi.2022.301479.

[2] K. Gupta, P. Lanka, And C. Varol, "A Holistic Digital Forensic Analysis Of Discord – Storage, Memory, And Network Perspectives," J. Forensic Sci., Vol. 69, No. 4, Pp. 1320–1333, 2024, Doi: Https://Doi.Org/10.1111/1556-4029.15548.

[3] F. Dzil Ikram And M. Koprawi, "Forensic Analysis On Discord Application Using The National Institute Of Standards And Technology (Nist) Method," 2023. [Online]. Available: Www.Ejournal.Isha.Or.Id/Index.Php/Mandiri

[4] M. Davis, B. Mcinnes, And I. Ahmed, "Forensic Investigation Of Instant Messaging Services On Linux Os: Discord And Slack As Case Studies," Forensic Science International: Digital Investigation, Vol. 42, P. 301401, 2022, Doi: Https://Doi.Org/10.1016/J.Fsidi.2022.301401.

[5] F. S. Marthinsen, "Creating A Framework For Live Data Analysis Of Discord Servers."

[6] K. Maitra, "Digital Forensic Analysis Of Social Media Platforms For Enhanced Investigation And Evidence Collection," 2024. [Online]. Available: Http://Www.Ijias.Issr-Journals.Org/

[7] I. Riadi, A. Yudhana, And G. Fanani, "Mobile Forensic On Michat Messenger Services Using Idfif V2 Framework," May 2024, P. 90003. Doi: 10.1063/5.0249092.

[8] T. Nargis, P. S. Monteiro, And S. U. Shenoy, "Malicious File Detection Using Discord Bot," Aip Conf. Proc., Vol. 3278, No. 1, P. 20005, May 2025, Doi: 10.1063/5.0262194.

[9] J. M. Puaschunder And H. Nicoleta-Elena, Scientia Moralitas Conference Proceedings Editors: Fifth Edition. 2025.

[10] N. Lykousas, V. Koutsokostas, F. Casino, And C. Patsakis, "The Cynicism Of Modern Cybercrime: Automating The Analysis Of Surface Web Marketplaces," In 2023 Ieee International Conference On Service-Oriented System Engineering (Sose), 2023, Pp. 161–171. Doi: 10.1109/Sose58276.2023.00027.

[11] A. K. Tyagi, K. Naithani, And S. Tiwari, "Security And Possible Threats In Today's Online Social Networking Platforms," In Online Social Networks In Business Frameworks, John Wiley & Sons, Ltd, 2024, Ch. 8, Pp. 159–199. Doi: Https://Doi.Org/10.1002/9781394231126.Ch8.

[12] R. Waterval, "How Information Sharing On Online Social Networks May Allow For Personalized Cyberattacks," 2021.

[13] K. Gupta, D. Oladimeji, C. Varol, A. Rasheed, And N. Shahshidhar, "A Comprehensive Survey On Artifact Recovery From Social Media Platforms: Approaches And Future Research Directions," Dec. 01, 2023, Multidisciplinary Digital Publishing Institute (Mdpi). Doi: 10.3390/Info14120629.

[14] S. L. Schröer, N. Canevascini, I. Pekaric, P. Widmer, And P. Laskov, "The Dark Side Of The Web: Towards Understanding Various Data Sources In Cyber Threat Intelligence," Apr. 2025, [Online]. Available: Http://Arxiv.Org/Abs/2504.14235

[15] 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.

[16] Y. Gong And U. Karabiyik, "Forensics Analysis Of Android Social Networking Application: Tencent Qq Revisited," In 2024 International Symposium On Networks, Computers And Communications (Isncc), 2024, Pp. 1–8. Doi: 10.1109/Isncc62547.2024.10758981.

[17] R. Hanaputra, K. Sa'adah, And R. Purwoko, "Identifikasi Digital Evidence Dalam Transaction Fraud Pada Whatsapp Desktop Berdasarkan Nist Sp 800-86: Studi Kasus Bisnis Properti," Jurnal Fasilkom, Vol. 14, Pp. 332–338, Jun. 2024, Doi: 10.37859/Jf.V14i2.7100.

[18] F. E. Salamh, M. M. Mirza, S. Hutchinson, Y. H. Yoon, And U. Karabiyik, "What's On The Horizon? An In-Depth Forensic Analysis Of Android And Ios Applications," Ieee Access, Vol. 9, Pp. 99421–99454, 2021, Doi: 10.1109/Access.2021.3095562.

[19] T. Rochmadi, A. Fadlil, I. Riadi, K. Panilestari, And Y. Wicaksono, "Analisis Teknologi Dan Prosedural Dalam Penanganan Insiden Untuk Mendukung Forensik Digital," Jati (Jurnal Mahasiswa Teknik Informatika), Vol. 10, Pp. 3285–3293, May 2026, Doi: 10.36040/Jati.V10i2.17792.

[20] R. Chand, N. Sharma, And A. Kabir, "Advancing Web Browser Forensics: Critical Evaluation Of Emerging Tools And Techniques," Sn Comput. Sci., Vol. 6, Jun. 2025, Doi: 10.1007/S42979-025-03921-6.

[21] M. Syukri, I. Riadi, And T. Sutikno, "Analisis Forensik Keamanan Data Pribadi Pada Mode Privasi Browser Menggunakan Metode National Institute Of Standards And Technology (Nist)," Jurnal Processor, Vol. 20, May 2025, Doi: 10.33998/Processor.2025.20.1.2012.

[22] O. Iskandar And Others, "Analisis Kejahatan Online Phishing Pada Masyarakat," Myrepublik Research And Publishing Journal, 2024.

[23] A. Chowdhury And A. Dwivedi, "A Comprehensive Review Of Phishing In Cybersecurity: Risks, Impacts, And Defence Strategies," Interantional Journal Of Scientific Research In Engineering And Management, Vol. 08, Pp. 1–7, Jun. 2024, Doi: 10.55041/Ijsrem38040.

[24] N. Nuratikah, S. Sunardi, And I. Riadi, "Investigasi Forensik Digital Kasus Pelecehan Seksual Pada Layanan Media Sosial X Dengan Metode Acpo," Jati (Jurnal Mahasiswa Teknik Informatika), Vol. 10, Pp. 2220–2228, May 2026, Doi: 10.36040/Jati.V10i2.17293.

[25] T. Rochmadi, A. Fadlil, And I. Riadi, "Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital," Cyber Security Dan Forensik Digital, Vol. 7, Pp. 81–89, May 2024, Doi: 10.14421/Csecurity.2024.7.2.4861.

[26] S. Szymoniak And K. Foks, "Open Source Intelligence Opportunities And Challenges: A Review," Advances In Science And Technology Research Journal, Vol. 18, Pp. 123–139, Jun. 2024, Doi: 10.12913/22998624/186036.