

# Web Forensic of Discord Services in Account Hijacking Cases using National Institute of Standards and Technology Method

Muhammad Difido  
Department of Informatics  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

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

## ABSTRACT

This study analyzes the security of social media accounts against Account Hijacking attacks *using* the National Institute of Standards and Technology (NIST) method, which consists of four stages: collection, examination, analysis, and reporting. Three tools were used in this research: FTK Imager, Discord Chat Exporter, and Chrome Cache Viewer. The results showed that Discord Chat Exporter produced 68% of the evidence in the form of text conversations, screenshot images, usernames, and profile pictures, while Chrome Cache Viewer contributed 16% from the Google Chrome browser cache. FTK Imager did not succeed in obtaining evidence from the Discord website, bringing the total collected evidence to 84%. The research findings confirm the effectiveness of Discord Chat Exporter and Chrome Cache Viewer in collecting digital evidence and recommend stricter digital forensic procedures and mitigation measures to enhance the security of social media accounts.

## Keyword

Account Hijacking; Discord; National Institute of Standards Technology; Hacking.

## 1. INTRODUCTION

The rapid development of digital technology has encouraged the use of social media platforms like Discord for interaction and transactions. However, this also increases the risk of cybercrimes, especially Account Hijacking. This research aims to analyze the security of Discord accounts from Account Hijacking attacks using the National Institute of Standards and Technology (NIST) method. By using tools such as FTK Imager, ChromeCacheViewer, and Discord Chat Exporter, this study aims to provide digital data that can be used as digital evidence of criminal activity. This research is expected to provide further understanding of Discord account security and provide recommendations for strengthening account security. [1]

Current technological developments are advancing rapidly, the many tools and applications for creating things bring not only positive but also negative impacts. This can be proven by the many cases of hacked accounts in Indonesia and worldwide. Account Hijacking is the act of taking control of another user's account after the "hijacker" has successfully obtained the authentication ID which is usually stored in local storage, cookies, or caches. [2] This study analyzes digital data obtained while investigating a criminal case on the Discord network. The objective of this project is to provide digital data, including the results of digital data analysis, that can be used to obtain digital evidence of criminal activity, such as Account Hijacking, to be presented in court. We hope that by using tools

like FTK Imager, ChromeCacheViewer, and Discord Chat Exporter, the examination of this digital evidence will become easier and more efficient. This is to educate readers on how to use the Discord site to research digital evidence.

A forensic workflow can implement one of several standard frameworks used in the forensic process. Among them are the National Institute of Standards and Technology (NIST), the National Institute of Justice (NIJ), the Integrated Digital Forensics Investigation Framework (IDFIF), the Digital Forensic Research Work Shop (DFRWS), the Association of Chief Police Officers (ACPO), or other forensic processes. In this study, the acquisition method used is the National Institute of Standards and Technology (NIST) method.

## 2. LITERATURE REVIEW

### 2.1 Digital Forensic

Digital forensics, or the forensic science used to conduct investigations of a case to find forensic information and content on digital devices, is essential for understanding cybercrime. In the field of digital forensic science, expertise in various areas is required, including legal studies. Depending on the type of digital device used, the technical aspect of the investigation is divided into several sub-branches, consisting of forensic data analysis, computer forensics, network forensics, and mobile device forensics as can be seen from Figure 1.

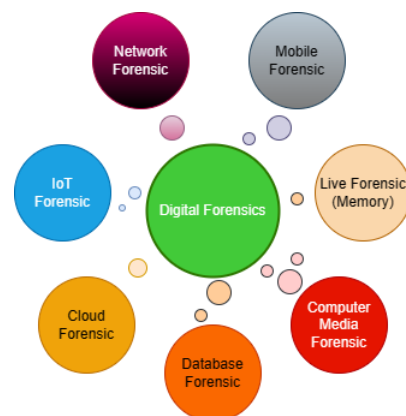


Figure 1: Overview of Digital Forensics

### 2.2 Digital Evidence

Digital forensics, or the forensic science used to conduct investigations of a case to find forensic information and content on digital devices, is essential for understanding cybercrime. In the field of digital forensic science, expertise in various areas is required, including legal studies. Depending on the type of

digital device used, the technical aspect of the investigation is divided into several sub-branches, consisting of forensic data analysis, computer forensics, network forensics, and mobile device forensics.

### 2.3 Data Recovery

Data Recovery is a crucial part of computer forensics, which can effectively acquire electronic evidence. Consequently, computer forensics technology has become a link between the prosecution and legal departments, which can help them solve, decide, and litigate cases more efficiently.

### 2.4 Account Hijacking

Account Hijacking is an illegal act involving the exploitation of a computer system or network to gain unauthorized access to data. This can be done through various methods, including phishing, brute force, and exploiting software vulnerabilities. Account Hijacking has many serious impacts, such as theft of personal data, financial loss, and reputational damage.

### 2.5 FTK Imager

FTK Imager is a software for analyzing and recovering data. FTK Imager can be used during the data collection process. To add evidence, one can select the file menu and click on the "add evidence Items" feature.

### 2.6 Discord

Discord is free software similar to WhatsApp or Skype that allows users to chat in real-time via text, voice, or video, like other voice chat applications. However, Discord is often misused. The program is very popular among gamers. This major chat platform was valued at over two billion in December after a successful fundraising round. It is the largest communication space available, used by millions of people.

### 2.7 Discord Chat Exporter

Discord Chat Exporter is an application that allows users to export chat history from various channels or servers on Discord into a file, which can be downloaded in HTML, TXT, and JSON formats. This application is compatible with direct messages, group messages, and server channels that can be seen in Figure 2.

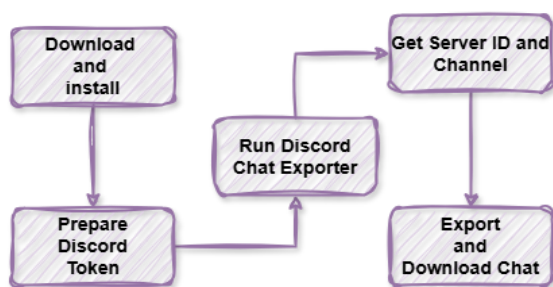


Figure 2: Discord Chat Exporter Usage Flow

### 2.8 Chrome Cache Viewer

ChromeCacheView is a small utility that reads the cache folder of the Google Chrome web browser and displays a list of all files currently stored in the cache. For each cache file, several pieces of information are displayed, such as URL, Content type, File size, Last accessed time, Expiration time, Server name, Server response, etc.

## 3. METHODOLOGY

The National Institute of Standards and Technology (NIST) framework serves as the foundation of this research, providing a structured approach to digital forensic investigations. This methodology comprises four primary stages: Collection, Examination, Analysis, and Reporting. The rationale for selecting NIST lies in its standardized and legally recognized structure, making it suitable for courtroom-ready evidence. Each stage is elaborated below, with detailed procedural and tool-specific insights to ensure forensic validity and replicability.

### 3.1 Research Tools and Materials

The selection of appropriate tools and materials is crucial in this research to ensure a smooth process and the validity of the results. This section presents a list of the hardware and software used. The following are the tools and materials used to support the investigation as shown in Table 1.

Table 1: Hardware used

No.	Hardware	Specifications
1.	Laptop	Intel® Core™ i5-10300H Processor 2.5 GHz (8M Cache, up to 4.5 GHz, 4 cores) 16337MB used, 8075MB available

Furthermore, various supporting tools and devices were prepared to support the investigation process as shown in Table 2.

Table 2: Software used

Software	Specifications
Chrome Caches View	ChromeCachesView v.2.47
Google Chrome	Version 114.0.5735.199 (Official Build) (64-bit)
FTK Imager	Version: 3.1.2 (x86)
Discord Chat Exporter	Version: v2.43.3

### 3.2 Research Stages

The stages of this research utilize the methodology shown in the figure. This methodology was investigated and structured to describe the steps taken in this research, with the aim of further studying and identifying a systematic process, and can be used as a guide in finding solutions to the challenges faced in this research.

#### 3.2.1 Collection

Collection is the process of gathering data with the aim of identifying, labeling, recording, and acquiring data from various sources that may contain relevant information, while adhering to guidelines and procedures that maintain data integrity. [6].

#### 3.2.2 Examination

Examination involves the forensic processing of large amounts of collected data using a combination of automated and manual methods to assess and extract data of interest, while preserving data integrity. [6].

#### 3.2.3 Analysis

Analysis involves the forensic examination of the various collected data using a mix of automated and manual methods to evaluate and extract relevant information, while maintaining data integrity. [13].

### 3.2.4 Reporting

Reporting the analysis results may include describing the actions taken, explaining the choice of tools and procedures, determining what actions need to be taken (such as performing forensic examination of additional data sources, ensuring discovered vulnerabilities are protected, improving existing security controls), and providing recommendations for improving policies, guidelines, procedures, tools, and other aspects of the forensic process. [11]

## 3.3. Case Scenario

This research illustrates a cybercrime case scenario, namely Account Hijacking, which begins with the perpetrator having financial problems. In the simulation scenario of this research, the focused cybercrime case is Account Hijacking.

### 3.3.1 Pre-Incident

The case scenario begins with a student who uses Discord to communicate with friends. They are members of a Discord server used by a gaming community, where they discuss and play games. Initially, the victim and the perpetrator were good friends who often played together and communicated using Discord. However, recently the perpetrator experienced financial problems and noticed that the victim frequently made purchases on the Discord application. The perpetrator intended to steal the victim's account to get money from them. The perpetrator created an application to hack the victim's account. This study aims to explore and analyze various related aspects as shown in Figure 3.

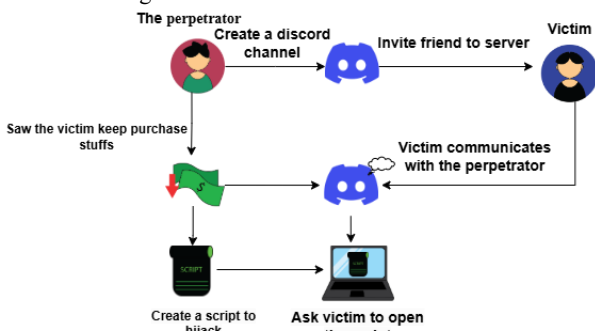


Figure 3: Pre-Incident

As shown in Figure 3, the perpetrator created an application containing a script designed to extract the victim's data and used social engineering techniques to persuade the victim to open the application. The victim and the perpetrator had known each other online and frequently played games and communicated via Discord. On December 4, 2025, at 09:20 AM (WIB), the perpetrator contacted the victim through Discord direct message and sent an executable file named HelperQuest.exe.

The perpetrator included the message:

"I made a cool game, want to try it?"

One minute later, the victim responded that the application did not work when run. The perpetrator then replied:

"Did you turn off your antivirus?"

This statement indicates that the perpetrator was aware the file could be detected as a threat by the computer's security system.

### 3.3.2 Incident

The perpetrator sent the application to the victim using another account. The victim asked the perpetrator if the application sent

from the second account was safe. The victim executed the application, and it was automatically deleted. After executing the application, the victim's token was sent to the perpetrator via a Webhook without the victim's knowledge. Ultimately, the perpetrator successfully hacked the victim's account and used it, which was linked to a credit card, to buy items on Discord to resell. The perpetrator also sent the application to the victim's friends. The victim realized their account was hacked when they saw their credit card balance had decreased and that the perpetrator had sent the malicious application to their friends. The victim then changed their Discord account password as shown in Figure 4.

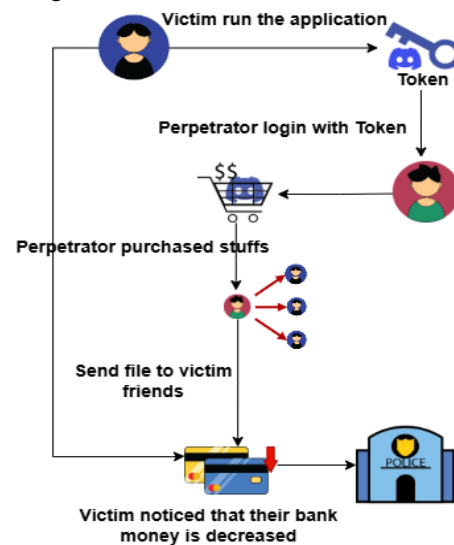


Figure 4: Incident

### 3.3.3 Post-Incident

After the victim reported the incident, an evidence-gathering process was initiated. An investigation was conducted on the relevant Discord server and the Direct Messages between the victim and the perpetrator. Electronic evidence related to the Account Hijacking activity was collected from the victim's laptop using the digital forensic procedures of the National Institute of Standard and Technology method. This involved recovering the conversation between the victim and the perpetrator as well as the hacking application, which would later be used as evidence as can be seen in Figure 5. This evidence will then be thoroughly analyzed and will proceed to the next stage where all collected evidence will be presented.

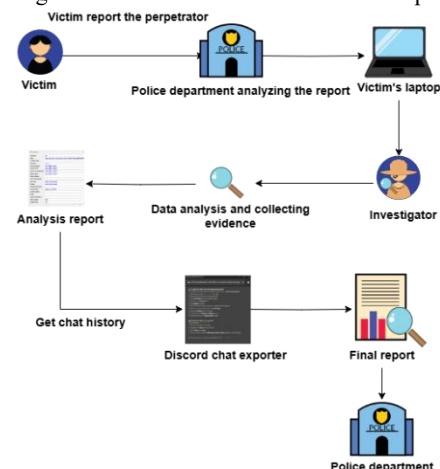


Figure 5: Post-Incident

## 4. RESULTS AND DISCUSSION

This section will present the results and discussion of the research using the National Institute of Justice method for digital forensic analysis on the Discord application. The findings include the misuse of Discord as a medium for Account Hijacking, confirming the urgency of this research in uncovering the misuse of digital platforms for crime.

### 4.1 Implementation

This research used the National Institute of Justice (NIJ) method to obtain digital evidence from the Discord Mobile application containing chats between the victim and the perpetrator. The NIJ method was chosen for its efficiency in systematically explaining the research steps: preparation, data collection, examination, analysis, and reporting.

#### 4.1.1 Collection

This stage is the initial step in the data collection process, where data was successfully gathered by capturing images and messages related to the account hijacking. The data includes conversations between the perpetrator and the victim, as well as the recovered application created by the perpetrator to hack the account. The data obtained from the chat was collected through the collection process. The ASUS TUF Gaming F15 laptop and its system specifications are important for the forensic process as it is the piece of evidence. It is crucial to know the system and all specifications of the ASUS TUF Gaming Laptop to plan and record all necessary information to maintain the integrity and authenticity of the digital evidence during the investigation. Specification can be seen in Table 3.

Table 3: Laptop Evidence Specifications

Specification Type	Description
Brand	ASUS TUF Gaming F15
Model Number	FX506LHB
Operating System	Windows 11
Processor	Intel(R) Core(TM) i5-10300H CPU @ 2.50GHz (8 CPUs), ~2.5GHz
BIOS	FX506LHB.311 (type: UEFI)

When collecting evidence, it is highly likely that deleted data and evidence will be recovered using forensic tools. Evidence that has been deleted is collected using FTK Imager, Chrome Cache Viewer, and Discord Chat Exporter software.

#### 4.1.1.1 Data Collection Using FTK Imager

After identifying the evidence, the next step is to collect digital evidence using the FTK Imager tool. This tool can recover lost or deleted data. Evidence acquisition with FTK Imager is done by recovering the downloaded file. In FTK Imager, to recover a downloaded file, a Disk Image of the victim's Local Disk C is created for further analysis as can be seen from Figure 6.

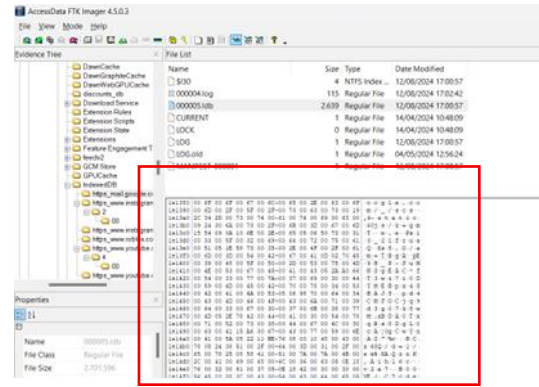


Figure 6: FTK Imager showcase

#### 4.1.1.2 Data Collection Using Discord Chat Exporter

The next step is to collect digital evidence with Discord Chat Exporter. This tool is used because Discord does not store data in a database or local device storage, but on their servers. Discord Chat Exporter works by using the authentic token stored by Discord, allowing access and export of chat data directly from the server, thereby ensuring the accuracy and authenticity of the obtained evidence. The application can be seen in Figure 7.

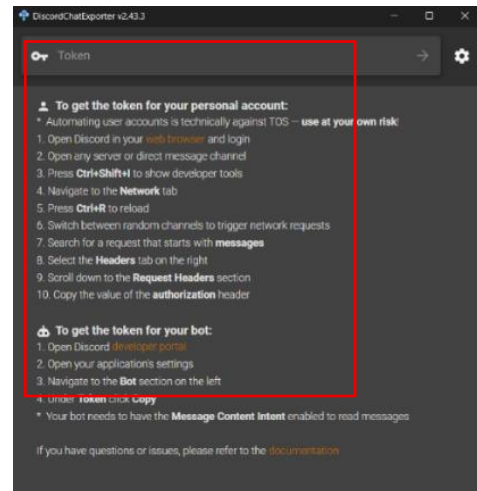


Figure 7: Image of Discord Chat Exporter

After the login process is complete, Ctrl+Shift+I is pressed to display the developer tools. Then, navigate to the Application tab and type "token". If the Key tab does not display a numerical value or the token, press Ctrl+R to reload, and the token will appear automatically. Once the token appears, copy it and paste it into the provided column on the first page of the Discord Chat Exporter tool as can be seen from Figure 8.

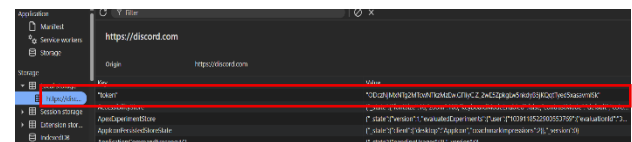


Figure 8: Discord Website inspect

After pasting the token code into the provided column and pressing Enter, the tool will display the Discord application interface, as shown as Figure 9.



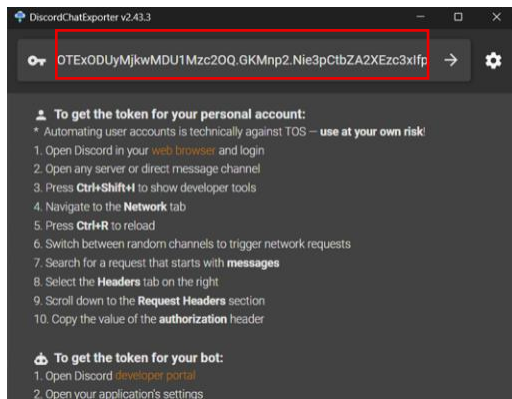


Figure 9: Inputting the token

Next, click on the channel/server that is the subject of the investigation that can be seen in Figure 10. The exported data from the discord server will appear in the previously selected file folder. This downloaded file contains the full digital evidence of the chat history between the perpetrator and the victim; further examination of this exported file will be done in the next stage.

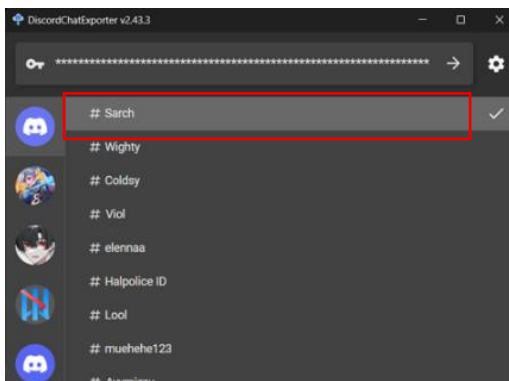


Figure 10: Image after inputting the Token

#### 4.1.2 Examination

In this phase, the collected data was processed using both automated and manual techniques. FTK Imager was used to examine system artifacts and recover deleted files. Discord Chat Exporter outputs were reviewed to validate chat history and media authenticity. Each file format was analyzed to identify communication patterns and media usage. Chrome Cache Viewer provided insight into cached images and user profiles, supporting cross-verification with Discord artifacts, can be seen in Figure 11.

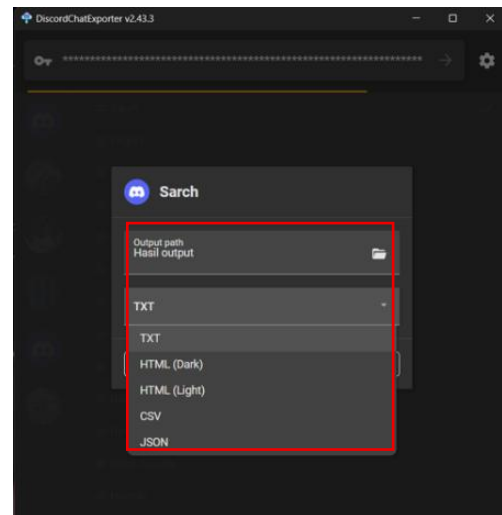


Figure 11: Export choice of Discord chat exporter

#### 4.1.2.1 Cache file checking from FTK Imager

The attempt to acquire digital evidence using FTK Imager proved unsuccessful. Despite performing a memory capture and creating a comprehensive disk image, FTK Imager failed to locate the specific file reportedly downloaded by the victim. This inability to find the crucial evidence renders the current acquisition effort inconclusive for the investigation. This outcome could stem from various factors, including the file being intentionally hidden or securely deleted, the victim utilizing encryption, or potential limitations of FTK Imager itself in identifying files under certain conditions or file systems. Further forensic analysis with more specialized tools may be necessary to uncover the missing digital evidence. Evidence can be seen in Figure 12.

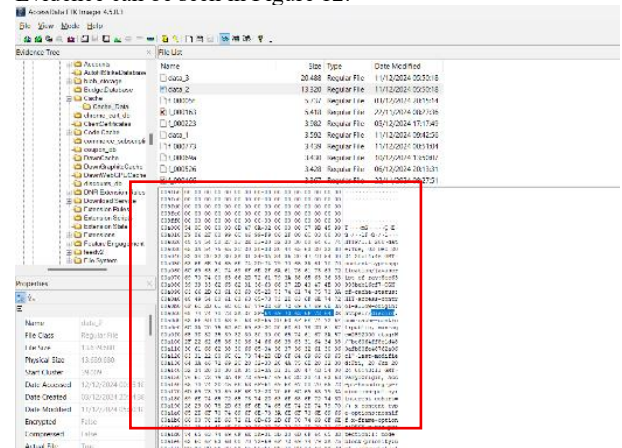


Figure 12: FTK Imager Page

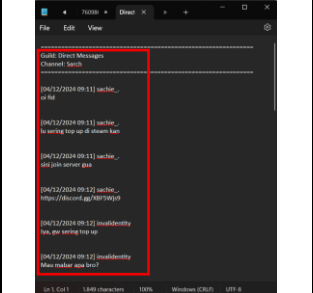
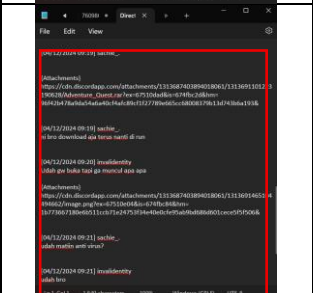
#### 4.1.2.2 TXT dan HTML File checking from Discord Chat Exporter

The data acquisition process, which utilized the Discord Chat Exporter, yielded two distinct file formats: TXT and HTML. Our initial focus is on the TXT file, as it contains the critical chat history between the victim and the perpetrator surrounding the time the incriminating file was transmitted.

Upon examination, the content of this TXT file has been confirmed to be identical to the digital evidence uncovered in the preceding investigative steps. This consistency is crucial, as it reinforces the integrity and reliability of the acquired data. This file offers a direct, verbatim record of the conversation,

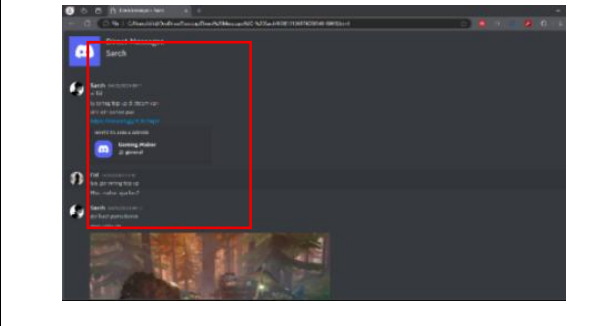
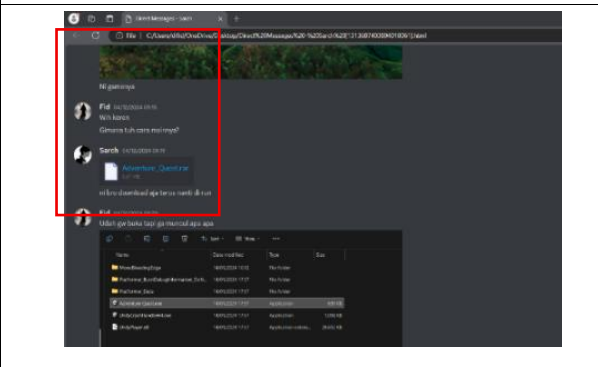
including timestamps and messages. The results of the TXT file examination are detailed in Table 4.

**Table 4: Chat Evidence from TXT file**

	<p>The perpetrator invites the victim</p>
	<p>The victim downloads the file given by the perpetrator</p>

From the examination of the TXT file, it can be seen that the screenshot image file sent by the victim cannot be displayed; instead, the image file is converted into a link. If one of the links is copied and pasted into a web browser, the browser will display the screenshot that can be seen in Table 5.

**Table 5: Chat Evidence from HTML file**

	<p>https://cdn.discordapp.com/attachments/1313687403894018061/1313689992312127488/best-multiplayer-games-valheim.png?ex=67510ca5&amp;is=674fbb25&amp;hm=7f4b83cd72089d574f4ae39e7f9c6c88a6e6f494c5b7af3e8a961aab23007975&amp;</p>
	<p>https://cdn.discordapp.com/attachments/1313687403894018061/1313691101223190628/Adventure_Quest.rar?ex=67510dad&amp;is=674fbc2d&amp;hm=96f42b478a9da54a6a40cf4afc89cf1f27789e665cc68008379b13d743b6a193&amp;</p>

Next, when the downloaded file in HTML format is clicked, the digital evidence is displayed via a web page. The display will be exactly like the website version of Discord. Unlike the TXT file, the HTML file can display images or screenshots directly in the chat room. The digital evidence from the HTML file is presented in Table 5.

### 4.1.3 Analysis

The analysis stage is carried out to examine in detail and thoroughly the results obtained from the collection and examination phases using tools such as FTK Imager and Discord Chat Exporter. At this stage, the primary objective is to interpret the digital artifacts that have been extracted and identify patterns, anomalies, and correlations that can provide insight into the incident being investigated.

#### 4.1.3.1. Analysis with FTK Imager

From the process of examining the memory capture from Local Disk C, it was found that the file downloaded and executed by the victim could not be located. This indicates that the malicious file, HelperQuest.exe, had been permanently deleted from the system after execution, leaving minimal to no trace in the file system. As a result, FTK Imager was unable to recover the executable file during the forensic imaging and analysis process.

#### 4.1.3.2. Analysis with Discord Chat Exporter

From the examination of the Discord chat export using the token, the TXT and HTML files show a chat room display that is identical to the original. The screenshot image evidence sent by the victim to the chat room also serves as valid proof of the export's authenticity. This is proven by the link obtained from the TXT file being the same as the screenshot link in the HTML file and the original chat room. The result of evidence can be seen in Table 6.

**Table 6: The differences of TXT, HTML and Application**

<p>https://cdn.discordapp.com/attachments/1313687403894018061/1313689992312127488/best-multiplayer-games-valheim.png?ex=67510ca5&amp;is=674fbb25&amp;hm=7f4b83cd72089d574f4ae39e7f9c6c88a6e6f494c5b7af3e8a961aab23007975&amp;</p>	<p>File TXT</p>
<p>https://cdn.discordapp.com/attachments/1313687403894018061/1313691101223190628/Adventure_Quest.rar?ex=67510dad&amp;is=674fbc2d&amp;hm=96f42b478a9da54a6a40cf4afc89cf1f27789e665cc68008379b13d743b6a193&amp;</p>	<p>File HTML</p>
<p>https://cdn.discordapp.com/attachments/1313687403894018061/1313691465104494662/image.png?ex=67510e04&amp;is=674fbc84&amp;hm=1b773667180e6b511ccb71e24753f34e40e0cfe95ab9bd686d601cece5f5f506&amp;</p>	<p>Discord Application</p>

After accessing the links extracted from the TXT file, each URL led to a specific image hosted on Discord's CDN, confirming that the exported chat data included valid media files. These images serve as supporting evidence, showing files or messages shared during the interaction. The corresponding images are presented in Table 7, each matched with its respective link to ensure traceability.

### Table 7: Evidence Differences

The image displays a 3x3 grid of screenshots from a digital investigation. The columns represent different types of evidence: Chat Evidence from a TXT file, Chat Evidence from an HTML file, and a Page of a Direct Message. The rows show a progression of chat messages. The middle row's central screenshot (HTML file) and the bottom row's central screenshot (Direct Message page) both feature a red rectangular box highlighting a specific message that mentions a 'Direct Messages Search' button. The other screenshots show various chat messages, including timestamps, usernames, and links, providing context for the highlighted evidence.

#### 4.1.3.3 Analysis with Chrome Cache Viewer

The examination process with Chrome Cache Viewer, by retrieving the cache from the Chrome browser, found several caches from Discord that displayed the URLs of the victim's and perpetrator's profile pictures, as well as images that had been sent in the chat between them. The results obtained from Chrome Cache Viewer can be seen in Table 8.

**Table 8: Digital Evidence from Chrome Cache Viewer**

The image displays two side-by-side Windows File Explorer windows. Both windows show the contents of a folder named 'https://discord.com/assets/70c4e-nr5u3channel\_id'. The left window shows a file named 'File Name' with a size of 340,370 bytes, last accessed on 04/12/2024 at 09:20:40, and a server name of 'Server Name'. The right window shows a file named 'File Name' with a size of 1,478 bytes, last accessed on 04/12/2024 at 09:13:34, and a server name of 'Server Name'. Both windows have a red box highlighting the 'File Name' field.

#### 4.1.4 Reporting

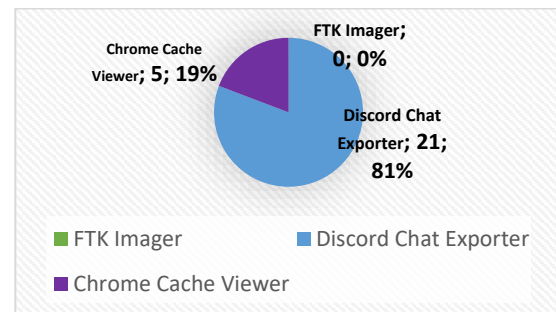
This report presents the examination results and digital evidence related to the hijacking case on the Discord Mobile platform. The evidence was collected using forensic tools such as FTK Imager, Discord Chat Exporter, and Chrome Cache Viewer. The analysis was conducted in accordance with the method established by the National Institute of Standards and

Technology (NIST). Details of the identified digital evidence are presented in Table 9.

### Table 9: Summary of Findings

Findings	FTK Image r	Discord Chat Exporter	Chrome Cache Viewer	Total
Server members' usernames (including perpetrator and victim)	-	✓	-	3
Text conversation between victim and perpetrator	-	✓	-	18
Profile Pictures of server members (including perpetrator and victim)	-	✓	✓	2
Screenshots sent by the Victim	-	✓	✓	4
File downloaded by the Victim		✓	-	1
Total Application Findings	0	21	5	27

Table 9 presents the digital evidence successfully identified in the hijacking case through the Discord platform, using three different forensic tools. Discord Chat Exporter successfully identified digital evidence in the form of username information, text conversations, and screenshot evidence sent by the victim on the Discord Website. Chrome Cache Viewer was able to collect digital evidence from the Discord Website application such as Profile Pictures and images that had been sent. The percentage of evidences can be seen in Figure 13.



**Figure 13: Evidence percentage Diagram**

Based on the number of items, the text conversations reported against the perpetrator were most numerous found with Discord Chat Exporter, at 88.4%. The examination using Chrome Cache Viewer also found evidence in the form of profile pictures and screenshots sent by the victim, with a finding percentage of 11.5%. FTK Imager did not find any evidence, thus having a finding percentage of 0%. This report is structured with detailed explanations and discussions in accordance with the rules and stages of the National Institute of Standards and Technology (NIST), which include collection, examination, analysis, and reporting.

## 5. CONCLUSION

The research titled "Web Forensics on Discord Services in an Account Hijacking Case Using the National Institute of Standards and Technology Method" successfully applied the NIST method in a forensic case of Account Hijacking on Discord. The entire process, including collection, examination,

analysis, and reporting of digital evidence, was successfully carried out according to the NIST method. The collection and analysis process, assisted by the forensic tool Discord Chat Exporter, yielded 68% of digital evidence in the form of text conversations, screenshot images, usernames, and profile pictures used by the perpetrator. The use of Chrome Cache Viewer only succeeded in producing 16% of the evidence. However, FTK Imager did not succeed in obtaining digital evidence from the Discord website. Thus, only Discord Chat Exporter and Chrome Cache Viewer could prove the Account Hijacking case as per the received report. In general, Discord is a secure platform; however, its vulnerabilities lie on the user-end. The primary weakness is the lack of validation or sandboxing for applications sent via direct messages (DMs), as well as the ease with which tokens can be stolen from the browser's local storage. The forensic approach applied here can be expanded to cover multiple messaging platforms and real-world cybercrime datasets to validate robustness. Additionally, integrating automated classification techniques may enhance the efficiency and accuracy of digital investigations.

## 6. REFERENCES

- [1] Discord, "Transparency Report: January - June 2024," 2024. [Online]. Available: <https://discord.com/safety-transparency-reports/2024-h1>
- [2] WithBlaze, "Discord Statistics and Demographics," WithBlaze, 2023. [Online]. Available: <https://www.withblaze.app/blog/discord-statistics-and-demographics>
- [3] F. Paligu and C. Varol, "Browser Forensic Investigations of WhatsApp Web Utilizing IndexedDB Persistent Storage," *Future Internet*, vol. 12, no. 11, p. 184, Oct. 2020
- [4] T. Pandela and I. Riadi, "Browser Forensics on Web-based Tiktok Applications," *Int J Comput Appl*, vol. 175, pp. 47–52, Dec. 2020
- [5] S. D. Utami, C. Carudin, and A. A. Ridha, "Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Security dan Forensik Digital*, vol. 4, no. 1, pp. 24–32, Jun. 2021
- [6] E. Ariyanti, "Identifikasi Bukti Digital Instagram Web Dengan Live Forensic Pada Kasus Penipuan Online Shop," *Cyber Security dan Forensik Digital*, vol. 4, no. 2, pp. 58–62, Apr. 2022
- [7] G. S. Suma, S. Dija, A. T. Pillai, "Forensic Analysis of Google Chrome Cache Files," *ICCIC*, Coimbatore, India, 2017, pp. 1-5
- [8] T. F. Efendi, "The Management of Physical Evidence and Chain of Custody (CoC) in Digital Forensic Laboratory Storage," *International Journal of Seocology*, pp. 001–010, Sep. 2019
- [9] R. Duan and X. Zhang, "Research on Computer Forensics Technology Based on Data Recovery," *J Phys Conf Ser*, vol. 1648, no. 3, p. 032025, Oct. 2020
- [10] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indonesian Journal of Business Intelligence (IJUBI)*, vol. 1, no. 1, p. 32, Feb. 2019
- [11] R. A. Kinasih, A. Wirawan Muhammad, and W. Adi Prabowo, "Analisis Live Forensics Pada Keamanan Browser Untuk Mencegah Pencurian Akun (Studi Kasus: Facebook dan Instagram)," *Digital Zone: Jurnal Teknologi Informasi dan Komunikasi*, vol. 11, no. 2, pp. 174–185, Nov. 2020
- [12] Nur Maghfirah Aesthetika and M. S. Rizal, "Efektifitas Penggunaan Aplikasi Discord Dalam Meningkatkan Komunikasi Interpersonal Di Kalangan Pecinta Film," *Medium*, vol. 10, no. 1, pp. 19–27, Apr. 2022
- [13] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 5, pp. 820–828, Oct. 2020
- [14] M. Fitriana, "Penerapan Metode *National Institute of Standards and Technology* (NIST) Dalam Analisis Forensic Digital Untuk Penanganan *Cyber Crime* Ditinjau Dari Aspek Hukum Yang Berlaku," Skripsi, UIN AR-RANIRY, 2020.
- [15] S. S. Tirumala, H. Sathu, V. Naidu, "Analysis and Prevention of Account Hijacking Based INCIDENTS in Cloud Environment," 2015 International Conference on Information Technology (ICIT), Bhubaneswar, India, 2015, pp. 124-129
- [16] Unicef, "Cyberbullying: Apa itu dan bagaimana menghentikannya," Unicef. Diakses: 8 Maret 2024. [Daring]. Tersedia pada: <https://www.unicef.org/indonesia/id/child-protection/apa-itu-cyberbullying>
- [17] "FTK Imager - Exterro." [Online]. Available: <https://www.exterro.com/ftk-imager>
- [18] A. M. Afdal, Y. Salim, and A. R. Manga, "Analisis Bukti Digital Forensik Pada Discord Menggunakan Metode *National Institute Of Standards Technology*," *Buletin Sistem Informasi dan Teknologi Islam*, vol. 3, no. 4, pp. 293–300, Nov. 2022
- [19] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital dalam Mengungkap *Cybercrime*," *csecurity*, vol. 3, no. 2, pp. 12–21, Dec. 2022
- [20] S. S. Tirumala, H. Sathu and V. Naidu, "Analysis and Prevention of Account Hijacking Based INCIDENTS in Cloud Environment," 2015 International Conference on Information Technology (ICIT), Bhubaneswar, India, 2015, pp. 124-129
- [21] Tyrrrz. DiscordChatExporter. [Online]. Available: <https://github.com/Tyrrrz/DiscordChatExporter>.
- [22] K. N. Isnaini, H. Ashari, and A. P. Kuncoro, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode Nist," *JURNAL RESISTOR*, vol. Vol. 3, pp. 72–81, 2020, [Online]. Available: <https://s.id/jurnalresistor>
- [23] G. Mishardila, "Analisa Dan Pencarian Bukti Forensik Digital Pada Aplikasi Media Sosial Facebook Dan Twitter Menggunakan Metode Statik Forensik," 2020.
- [24] Andria and S. Nita, "Forensik Digital Sistem Informasi Berbasis Web," *JAMI: Jurnal Ahli Muda Indonesia*, vol. 2, no. 2, Dec. 2021.
- [25] D. Rathod, "Web Browser Forensics: Google Chrome," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 7, pp. 4433, Jul.-Aug. 2017.