Mobile Forensic Analysis of Discord Services Cyberbullying Case using National Institute of Justice Method

Hafizhah Dyanty Putri
Department Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
The development of information technology has brought significant impacts, including on social media such as Discord, which although useful, has also increased cases of cyberbullying. This research aims to find digital evidence in cyberbullying cases on Discord using the National Institute of Justice (NIJ) method. The NIJ methodology consists of five stages: preparation, collection, examination, analysis, and reporting. Digital forensic tools used include MOBILEdit Forensic Express, Discord Chat Exporter, and SysTools SQLite Viewer. The collection stage involved collecting evidence from the victim's smartphone, and the examination and analysis stage involved evaluating the digital evidence. The results showed that Discord Chat Exporter found 92 items (88%) of digital evidence, including usernames, conversation texts, and screenshots, while MOBILEdit Forensic Express found 12 items (12%). SysTools SQLite Viewer found nothing. This research confirms the importance of the NIJ method in ensuring the integrity and accuracy of digital evidence in forensic investigations of cyberbullying cases.

Keywords
Cyberbullying, Digital Forensics, National Institute of Justice, Discord, Digital Evidence.

1. INTRODUCTION
Social media users continue to grow rapidly, bringing many benefits and positives. One such service is Discord, a digital platform for playing games with friends. Users can use many features such as sharing information, messages, pictures, videos, voice chat, and video calls [1].

The development of social media has brought negative impacts such as the rise of cyberbullying in Indonesia and the world. Cyberbullying is the malicious use of information and communication technology to intimidate, humiliate, or degrade someone. It includes angry messages, harassment, defamation, impersonation, dissemination, deception, exclusion, and stalking [2].

According to Influencer Marketing Hub, Discord users increased from 45 million in 2017 to 350 million in 2021 [3]. Discord, as a digital distribution platform, is experiencing an increase in users that brings both positive and negative impacts. Discord has secured 2,000 servers suspected of containing violent and extreme content, and closed 30,000 servers due to various offenses, especially online crimes [4].

This research uses the National Institute of Justice (NIJ) methodology to analyze and solve cyberbullying cases through digital forensics. The NIJ method includes five stages: preparation, collection, examination, analysis, and reporting. This method was chosen because it provides a systematic analysis and makes it easier to obtain the necessary digital evidence [5].

This research analyzes digital data as evidence of cyberbullying cases on Discord using the National Institute of Justice method. Tools such as FTK Imager, MOBILEdit Forensic Software, DB Browser for SQLite Software, Autopsy, SysTools SQLite Viewer, and Discord Chat Exporter are used to facilitate the analysis and investigation process.

2. RELATED WORKS
Andi Muh Afdal, Yulita Salim, Abdul Rachman Manga (2022) on "Forensic Digital Evidence Analysis on Discord Using the National Institute of Standards Technology Method", which discusses the analysis of digital evidence on Discord services using the National Institute of Standards Technology (NIST) technique, which includes collection, examination, analysis, and reporting. FTK Imager is used as a tool in this analysis process [1].

Gede Pawitradi, I Ketut Gede Suhartana (2019) on "Acquisition of LINE Digital Social Media Evidence Using the National Institute of Justice (NIJ) Method", which discusses the acquisition of digital evidence on LINE social media using the National Institute of Justice (NIJ) method, which includes preparation, collection, examination, analysis, and reporting. The tools used are MOBILEdit and DB Browser [5].

Hijrah Nuraini, Imam Riadi (2019) on "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method", this research discusses the analysis of cellphones in root conditions to find evidence on the Twitter application using DB Browser for SQLite, SQLite Manager, and Root Explorer. The method used is the National Institute of Justice [6].

Kadek Dwi Oka Mahendra, I Komang Ari Mogi (2021) on "Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases" This study involves five stages: preparation, collection, examination, analysis, and reporting. Data was obtained from the perpetrator's Vivo 1606 Y53 smartphone, where MiChat was used for prostitution promotion and transactions. Examination used MOBILEdit Forensic Express for data such as IMEI and IMSI numbers, and analysis of MiChat contacts and conversations. The results served as digital evidence in court, emphasizing the importance of digital forensics in tackling online prostitution on social media [7].

Herman, Anton Yudhana, Fitri Anggraini (2023) on "Android-Based TikTok Digital Evidence Acquisition Using the National Institute of Justice Method". This research uses the National Institute of Justice method to obtain digital evidence from TikTok on Android devices. The preparation stage involves Thinkpad laptops and Samsung Galaxy Tab A8 SM-P355. Evidence was collected using MOBILedit Forensic Express. Testing and analyzing TikTok data included app information, user accounts, messages, images, videos, and event times. A report was generated based on the acquired data, with results showing a higher success rate of evidence acquisition on rooted smartphones [8].

3. METHODOLOGY

The National Institute of Justice (NIJ) functions to explain the stages of the research being conducted so as a reference in solving problems. This method recommends the basic stages in the forensic process, namely preparation, collection, examination, analysis, and reporting [7].

The methodologies used in this research aim to help the investigation process, obtain digital evidence, and uncover digital forensic cases.

3.1 Research Tools and Materials

The selection of appropriate tools and materials is crucial in this research to ensure the smoothness of the process and the validity of the results. This section presents a list of hardware and software used. Here are the tools and materials used, Table 1 lists the hardware, and Table 2 lists the software.

Table 1. Hardware used in Research

Hardware	Spesification
Laptop	VivoBook K413F Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz
Smartphone	Samsung Galaxy E7 Android 5 (Lollipop)
Reversible Connector or USB Cable	USB Micro-USB

Table 2. Software used in Research

Software	Spesification
MOBILEdit Forensic Express	MOBILEdit Forensic Express for Windows Versi 7.2.0.17975 (64-bit)
Discord Chat Exporter	DiscordChatExporter v2.43.3
SysTools SQLite Viewer	SysTools SQLite Viewer Version 3.0 (x86)

3.2 Research Phase

The stages used in this research are taken from the National Institute of Justice method. These stages have been proven in law enforcement attempts.

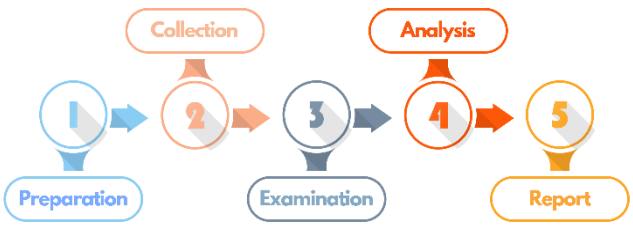


Figure 1: National Institute of Justice Method Workflow

Figure 1 is a workflow of the National Institute of Justice Method which consists of the stages of preparation, collection, examination, analysis, and reporting. Further explanation is as follows:

3.2.1 Preparation

The first stage of the research involved preparing the equipment needed to carry out the investigation process. At this stage, the process involved preparing all the tools that would be used during the investigation [33].

3.2.2 Collection

Collection is the stage where researchers search for documents, collect, or make copies of physical smartphone objects that contain digital evidence.

3.2.3 Examination

At this stage, an examination of the digital evidence that has been obtained in the previous stage is carried out. The goal is to ensure the authenticity of the digital evidence obtained from the collection that has been collected [33].

3.2.4 Analysis

The analysis stage is the stage where researchers will continue to evaluate or analyze the evidence that has been obtained from the results of trials conducted at the examination stage.

3.2.5 Reporting

At the reporting stage, the researcher attaches a report of the investigation that covers the entire process from start to finish, including the evidence found, the methodology used, and the conclusion of the case being solved [34].

3.3 Case Scenario

This research simulates a cyberbullying case through the Discord platform with the aim of obtaining relevant digital evidence. An in-depth discussion was conducted to describe the stages of the simulation, including Pre-Incident, Incident, and Post-Incident. It aims to uncover the cyberbullying activities carried out by a teenager against his friend.

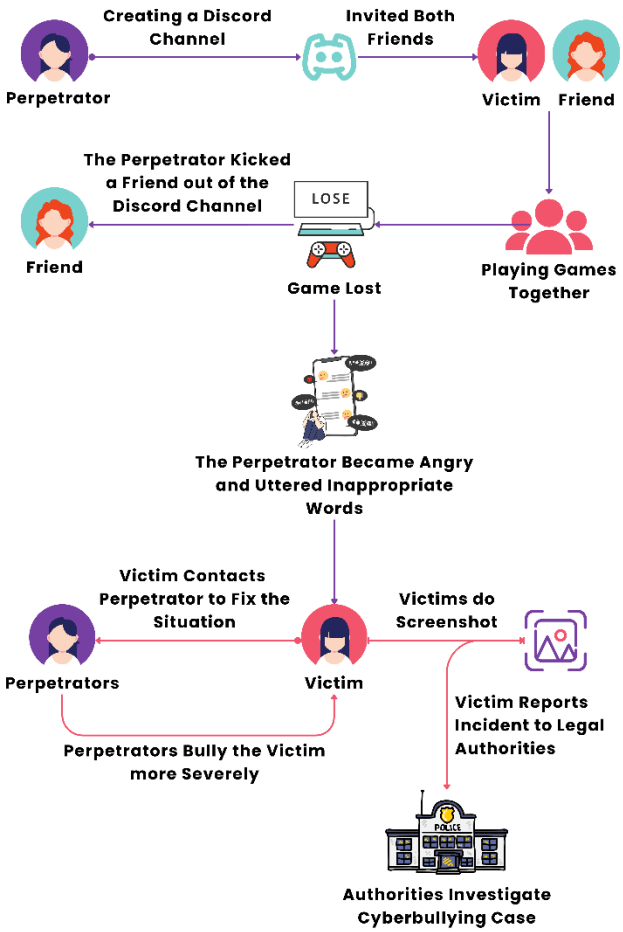


Figure 2: Cyberbullying Case Scenario on Discord

Figure 2 show the overall picture of the cyberbullying case scenario that occurred between two teenagers. The scenario will be further explained in 3 stages, namely Pre-Incident, Incident, and Post-Incident as follows:

3.3.1 Pra-Incident

The case scenario started with a teenager (the perpetrator) creating a discord server to communicate and play games, and inviting two friends, the victim and one other friend. They were close friends who were friends like any other teenagers. One day, they made an appointment to play an online game together, and then during the game, there was an incident that was accidentally committed by the victim and caused them to lose the game. After the losing incident, the victim suddenly returned to the discord application and took out one of his friends and started an argument by scolding the victim and saying harsh and inappropriate words.

3.3.2 Incident

During the argument, the victim was shocked and did not expect the attitude shown by the perpetrator. The victim knew the perpetrator as a good and reliable friend. But behind the shock, the victim felt more guilty because he thought his friend was angry because of his actions, so he continued to apologize, but the perpetrator still did not melt and finally they chose to go off discord.

The next day, the victim tried to contact the perpetrator again with the intention of mending their relationship. However, the situation did not go as the victim had hoped. The perpetrator instead used more severe bullying words and hurt the victim's heart. Feeling very hurt, anxious, and depressed by the words uttered by the perpetrator, the victim took a screenshot of their chat page. The screenshots showed messages containing insults, diatribes, curses, and bullying by the perpetrator.

3.3.3 Post-Incident

Because she could not stand the behavior of the perpetrator, the victim reported and explained the whole sequence of events to the authorities. After listening and recording all the necessary information from the victim, the authorities immediately processed the case. The process began with the authorities obtaining physical evidence in the form of a smartphone and information data in the form of the victim's discord account id and password, then continuing the investigation by following the National Institute of Justice's digital forensics procedure through the evidence that had been found.

4. RESULTS AND DISCUSSION

This section will present the results and discussion of the research using the National Institute of Justice's method for digital forensic analysis of the Discord application. Findings include the misuse of Discord as a medium for cyberbullying, emphasizing the urgency of this research in revealing the misuse of digital platforms for crime.

4.1 Implementation

This research uses the National Institute of Justice (NIJ) method to obtain digital evidence from the Discord Mobile application which contains chats between victims and perpetrators. The NIJ method was chosen because of its efficiency in systematically explaining the research steps: preparation, data collection, examination, analysis, and reporting.

4.2.1 Preparation

Preparation is the initial stage in finding digital evidence. At this stage, the researcher identifies and collects information, and then prepares the tools that will be used to support the investigation. These tools are chosen for their functions relevant to the research and their ability to find digital evidence. The tools consist of two types, namely hardware and software. The tools to be used are described in Table 3.

Table 3: Tools Preparation

Name	Type	Description
Mobile Phone	Hardware	Media to obtain physical evidence data
Micro-USB Cable	Hardware	Mobile phone to laptop connection device
Laptop	Hardware	Media for testing, identification, and analysis of evidence
Discord Mobile dan Web	Software	Objects or applications that will be tested in forensic activities
MOBILEdit Forensics Express	Software	Tools used to collect digital evidence data by means of acquisition and extraction of applications on smartphones

Systools SQLite Viewer	Software	Tools used to analyze files and databases from the extraction results performed on MOBILEdit Forensics Express
Discord Chat Exporter	Software	Tools used to retrieve chat history evidence data in the discord application using tokens taken from the Discord Developer Portal

4.2.2 Collection

The collection stage is a step to search for and collect digital evidence that supports the disclosure of cyberbullying crimes through the Discord application. The collection of digital evidence is done through the victim's Samsung Galaxy E7 smartphone, which is then rooted to give full access to the system and security of the device. This rooting process is important in order to access and extract data that is hidden or protected on the smartphone.

Figure 3: Physical Evidence of Samsung Galaxy E7 Smartphone

The victim's Samsung Galaxy E7 smartphone is important as evidence in the forensic process. Researchers need to understand the complete system and specifications of this device, including the brand, model serial number, IMEI, operating system, and other relevant data as listed in the table. Recording this information in a structured manner is critical to maintaining the integrity and authenticity of the digital evidence during the investigation.

Table 4: Smartphone Spesifications

No	Name	Description
1	Smartphone Brand	Samsung Galaxy E7
2	Model Number	SM-E700H
3	IMEI	358641061075361
4	Version	Android 5.1.1
5	Serial Number	LMY47X.E700HXXS1BQA1

The document search process is carried out on the victim's smartphone in a condition that the rooting process has been carried out, which functions to make it easier to access all security systems contained in the smartphone, smartphones that have been rooted can be checked in the Root Checker application, if the smartphone is not rooted there will be a notification in orange, then if the smartphone has been rooted there will be a green notification, as shown in Figure 4.

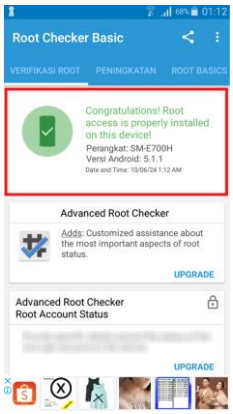


Figure 4: Checking Root Status

In addition to the Root Checker app as a tool to check the rooting status, there is also SuperSU as an app that supports users to manage root privileges on the device. SuperSU image display can be seen in Figure 5.

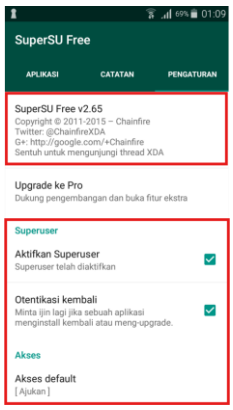


Figure 5: SuperSU as a Root Privilege Access Tool

4.2.2.1 Data Collection Using MOBILEdit Forensics Express

After collecting evidence and performing the previous steps, the next step is to use the MOBILEdit Forensics Express tool to capture digital evidence. This tool supports various image formats that are important for forensics. The evidence retrieval process is done by connecting the smartphone to a laptop that has MOBILEdit Forensics Express installed using a Micro-USB cable.

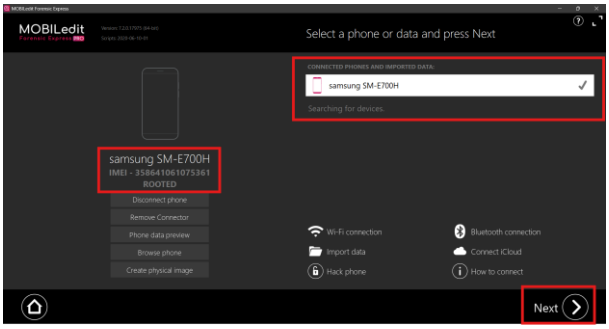


Figure 6: Smartphone Connected to MOBILEdit

Figure 6 show the MOBILEdit Forensics Express application page, after selecting the phone/data that you want to use, users

can continue to use this tool for various processes, such as selecting the extraction menu, selecting what applications you want to extract, and others.

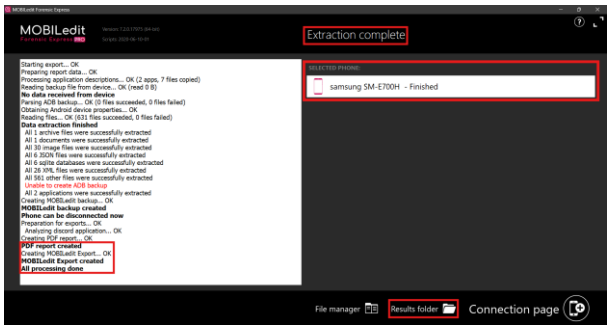


Figure 7: Smartphone Display and Application has been Extracted

Figure 7 show the display of the extraction process that has been completed, marked with the words "All processing done", then the words "Finished", and later the extraction results can be directly accessed by pressing the "Result folder" icon.

After all the data extraction processes are complete, the files and data from the extraction results will appear.

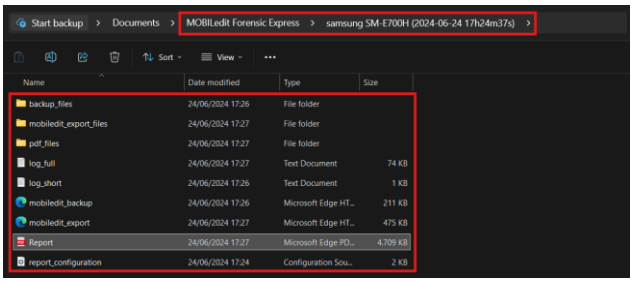


Figure 8: Extracted Folders and Files

The extraction results or folders found began to be opened, one of which was the Report.pdf file. This PDF file contains the extracted data and some details of the data that has been collected and processed from the Discord application and Gallery.

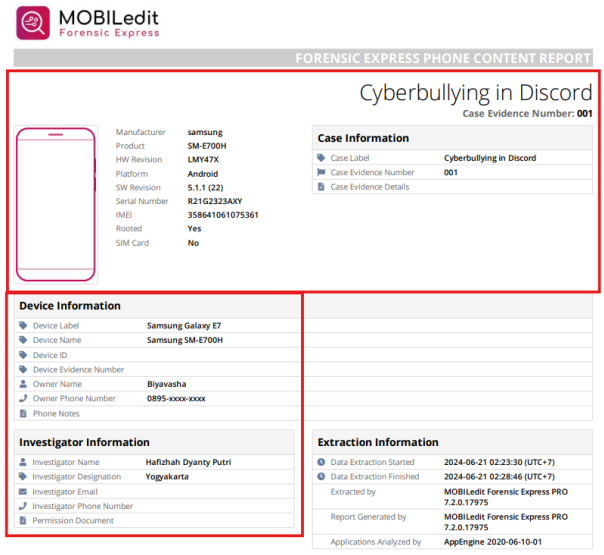


Figure 9: MOBILEdit Forensics Express Extraction Results Report

Figure 9 show the start page of the Report.pdf file, where there is general information about case information, device information, and investigator information.

4.2.2.2 Data Collection Using Discord Chat Exporter

After collecting digital evidence using MOBILEdit Digital Forensics, the next step was to use the Discord Chat Exporter to collect additional digital evidence. This tool is important because Discord does not store chat data locally on the device, but rather on their own servers. Discord Chat Exporter uses Discord's native token to verify and retrieve chat data directly from the server, ensuring the accuracy and authenticity of the evidence obtained.

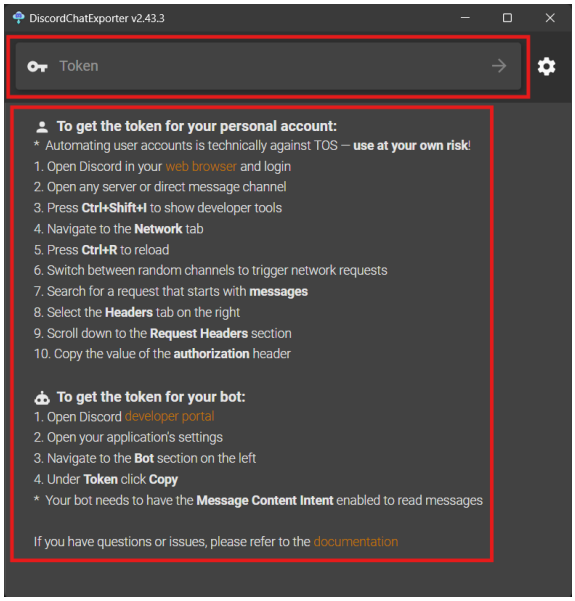


Figure 10: Discord Chat Exporter Home Page

Figure 10 show the Discord Chat Exporter home page, where there is a token column and information about how to get the discord token. The next process involves collecting Discord tokens by accessing the official Discord website.

The collection process begins with the authorities obtaining the victim's Discord account data for the data collection process. This data is used to login to the Discord website, which, if successful, will display the Discord home page.

After the login process is complete, then Ctrl+Shift+I will be performed to display the developer tools, after the developer tools are open, navigate to the Application tab and start typing "token".

If the Key tab does not display the Value containing the numeric number or token number, then Ctrl+R will be done to reload and the token will automatically appear.

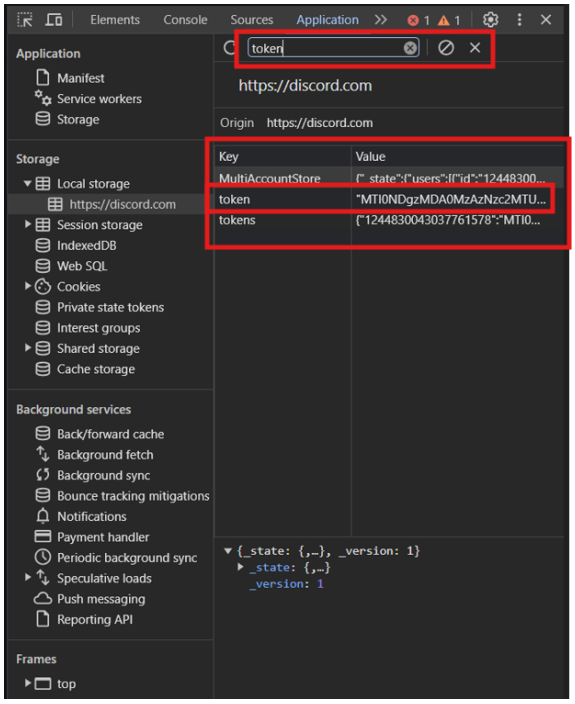


Figure 11: Take and Copy Token

Figure 11 show the Discord Website view after opening the developer tools page where the token is taken. The token that appears must be kept secret because if it is scattered it could be misused.

After the token appears as drawn, then copy the token and paste it into the column provided on the first page of the Discord Chat Exporter tool as previously displayed.

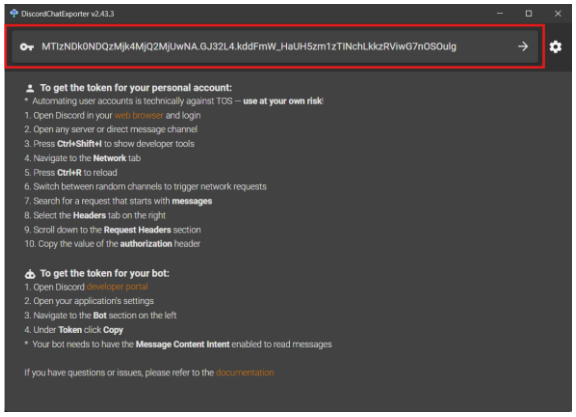


Figure 12: Paste Token ke Home Page Discord Chat Exporter

Figure 12 show the Discord Chat Exporter page after the token number that has been taken previously is pasted in the top column, next to the key logo.

After entering the token code and pressing Enter, the tool will display the Discord application page. Select the channel/server where the incident occurred, then select text channels and #general to download or export chat data by clicking the orange download logo in the lower right corner.

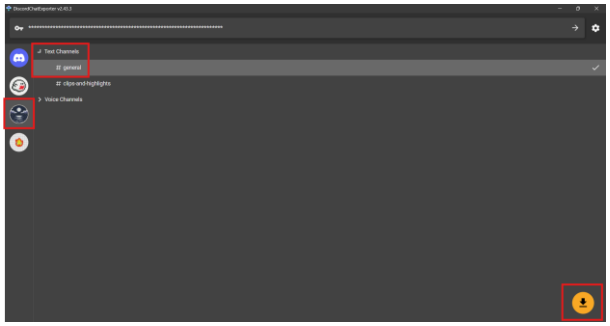


Figure 13: Pick Sever Page

Figure 13 show the page after selecting the server you want to download the chat history from.

After clicking download, the tool will redirect to the output path selection menu for the destination where the download results will be saved, and select the desired output format, such as TXT, HTML, CSV, or JSON. Then when finished, click export to start the exporting and download process.

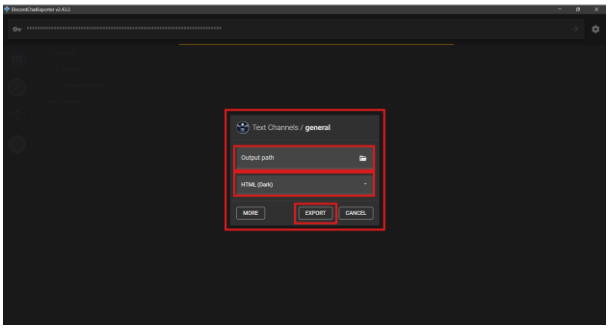


Figure 14: Selection of Storage Destination and Output Format, Export

Figure 14 show the menu for selecting the desired storage destination and output file format.

The results of the export or download of the discord server digital evidence data will appear in the previously selected file folder. The download file contains full digital evidence of the chat history of the perpetrator and victim, further examination of the exported file will be carried out at a later stage.

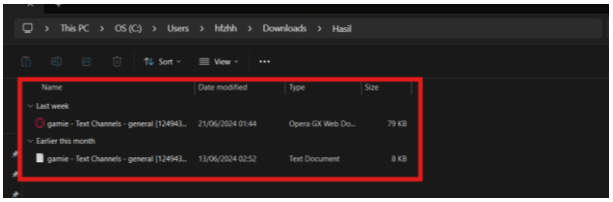


Figure 15: Export Download File

Figure 15 show two files from the export and download results of Discord Chat Exporter, the file is made into two formats, namely a TXT file which if opened will display evidence of chat in notepad, then the other file is a file with HTML format which if opened the user will be directed to google or other web browsers. used to get a comparison of the contents of the file which will be discussed in the examination sub-chapter.

4.2.3 Examination

At the examination stage, the data obtained was analyzed in detail. Report.pdf files from MOBILEdit Forensics Express, as well as TXT and HTML files from Discord Chat Exporter were

examined, along with databases from Systools SQLite Viewer. These tools were used to identify, understand and verify the data to ensure the accuracy and integrity of the digital evidence.

4.2.3.1 Examination of Report File from MOBILEdit Forensics Express

The PDF main page contains the victim's processed smartphone specifications and other information such as Case Information, Device Information, Investigator Information, Extraction Information, and Device Properties.

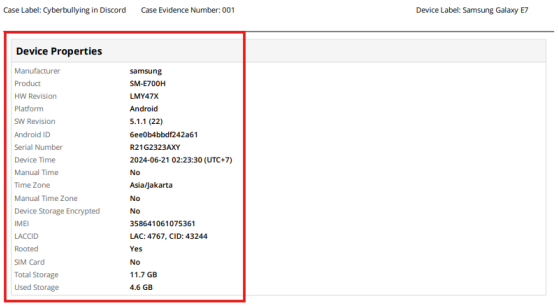


Figure 16: Smartphone Specification Information Page

Figure 16 show the page about the specification information of the victim's smartphone.

The report shows the complete structure of the rooted smartphone, including Case Information such as Case Label, Case Evidence, and Case Evidence Details. In addition, there are Device Properties such as Manufacturer, Product, Android ID, Serial Number, IMEI, Rooted, and SIM Card. If the PDF file is scrolled down, there is a Table of Contents that presents information about the data obtained from the Discord and Gallery extraction process. This Table of Contents lists content such as images and other media files, with the total amount of data from each of these apps.

Figure 17: Table of Contents Page

Then on the next pages, the results of the discord extraction are found, namely information data related to the discord application and image files such as profile photos of the victim, perpetrator, and their friends, and profile pictures of the server/channel where the victim and perpetrator occurred.

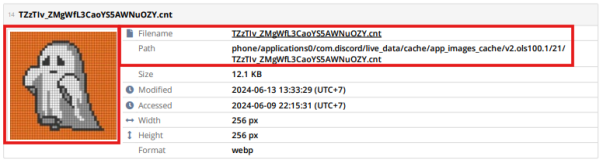


Figure 18: Digital Evidence in the Photo Profile used by the Perpetrator

Figure 18 show the photo profile used by the perpetrator during the incident.

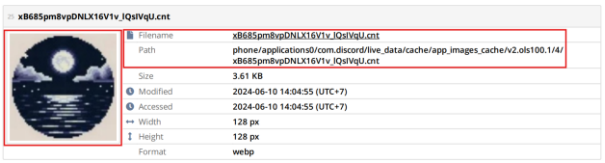


Figure 19: Digital Evidence in the Profile Picture of the Discord Server where the Incident Occurred

Figure 19 show the profile picture of the game server/channel where the cyberbullying incident was carried out by the perpetrator against the victim. In addition, there are screenshots sent by the victim on the game channel as a threat to the perpetrator, one of which can be seen in Figure 20.

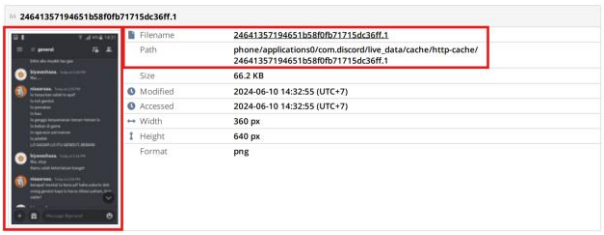


Figure 20: Screenshot Digital Evidence of Cyberbullying Actions Committed by the Perpetrator to the Victim

Figure 20 show one of the digital evidence in the form of screenshots of the victim containing cyberbullying acts committed by the perpetrator.

The results of the Gallery app extraction found only one image used as a smartphone wallpaper, as shown in the Figure 21. The other screenshots could not be read by MOBILEdit Forensics Express.

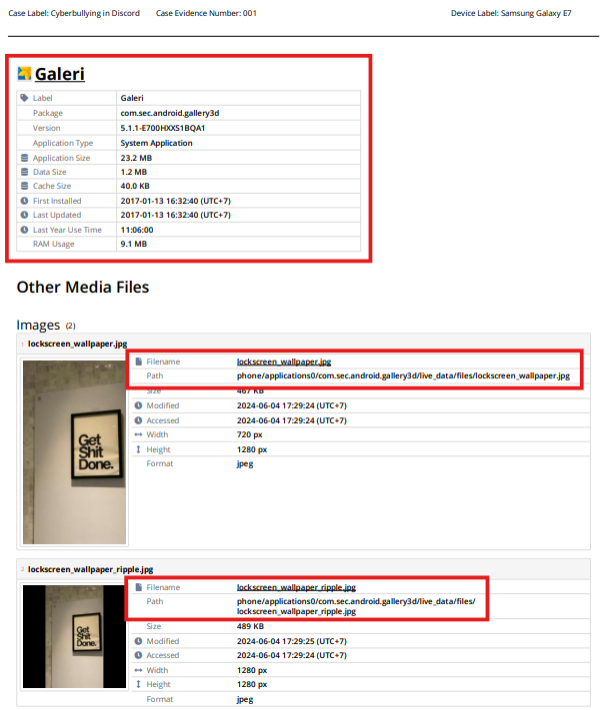


Figure 21: Gallery Extraction Result

Figure 21 show the results of the extraction report carried out in the gallery. It can be seen that the extraction process carried out in the gallery only produces 2 images in the form of cellphone wallpapers used by the victim.

Examination of the Report.pdf file from MOBILEdit Forensics Express succeeded in obtaining evidence in the form of server member profile photos, Discord server profiles, and screenshots of chat on the game server used by the perpetrator for cyberbullying. This investigation was then continued with the examination of digital evidence using Discord Chat Exporter.

4.2.3.2 Examination of TXT and HTML Files from Discord Chat Exporter

Digital evidence data capture using the Discord Chat Exporter produces files in TXT and HTML formats. The TXT file contains a history of chatting on the Discord server "gamie" on the "general" channel, covering the initial interaction to the confrontation that became cyberbullying. Two of the contents of the TXT file corresponds to the digital evidence found earlier as in Figure 22 and Figure 23.

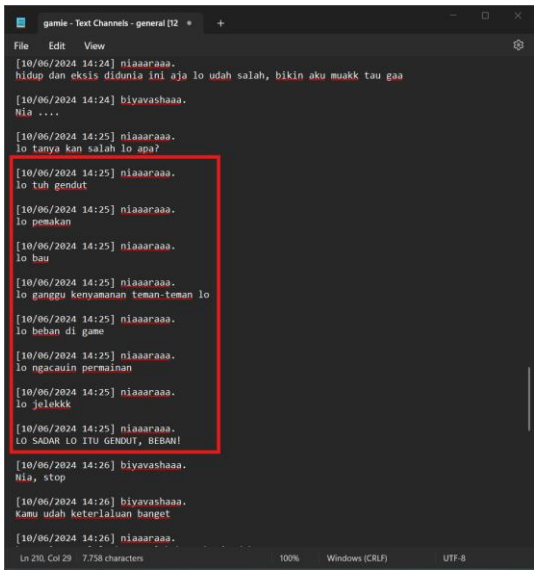


Figure 22: Digital Evidence of Cyberbullying Actions of the Perpetrator to the Victim obtained from TXT Files

Figure 22 show the action of cyberbullying committed by the perpetrator to the victim, the digital evidence is taken from the export of Discord Chat Exporter with TXT file format.

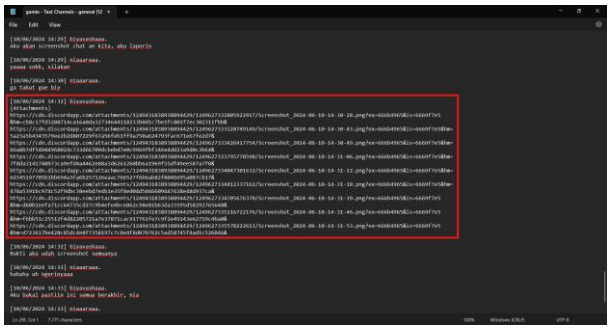


Figure 23: Digital Evidence of Chat Export results with TXT File Containing Screenshot Link

Figure 23 show digital evidence containing screenshots taken by Biya, the victim, who showed and sent them to a chat room with the perpetrator. The victim threatened the perpetrator, but was ignored by the perpetrator.

Examination of the TXT file showed that the screenshot image file sent by the victim could not be displayed directly. Instead, the image file is converted into a link. Users can copy and paste this link into a browser to view the screenshots.

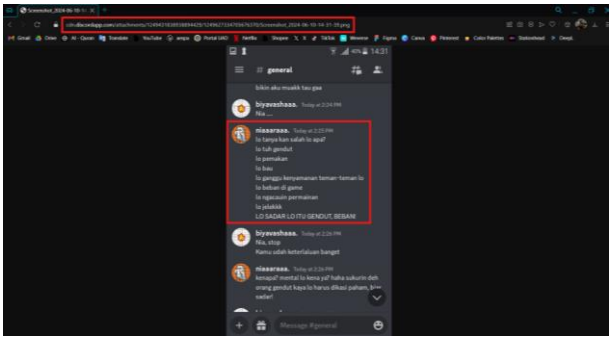


Figure 24: Link in TXT file Containing Screenshot Evidence

Figure 24 show one of the screenshot images taken from the link in the TXT file from the download export that was previously done. It can be seen that the screenshot results are exactly the same as those sent by the victim before, and can be called the same because the naming of the file in the link is the same as the original.

When the download file in HTML format is clicked, digital evidence will be displayed through the website with a Discord-like appearance of the website version. The HTML file can display images or screenshots directly in the chat room. The digital evidence of the HTML file will be presented in Table 5.

Table 5: Digital Proof of HTML Files

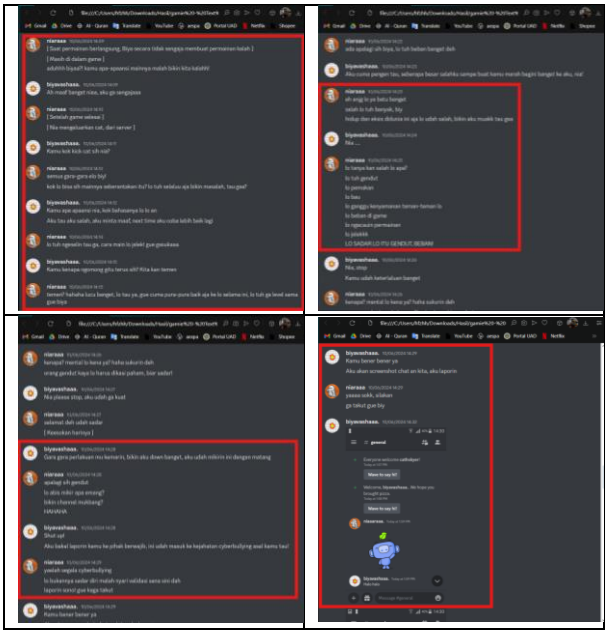


Table 5 show some snippets of the "gamie" server chat room page from the Discord Chat Exporter download in HTML file format. This chat room is used by the perpetrator, victim and their friend to play games, as seen, there are some bullying sentences, insults and curses. The chat room has become a place for cyberbullying.

4.2.3.3 Inspection with SysTools SQLite Viewer

Systools SQLite Viewer is used to inspect application databases that have been acquired during the previously conducted data collection process. The tool is designed to assist users in examining and analysing SQLite databases easily and efficiently, while ensuring data integrity is maintained. This

makes it very useful in digital forensics and data investigation activities.

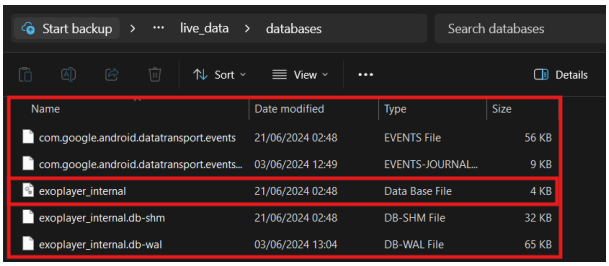


Figure 25: Database Folder from the Extraction Process of MOBILEdit Forensics Express

Figure 25 show the contents of the database folder obtained from the acquisition and extraction process during the data collection process. The database folder does not appear to have many files, this is because Discord stores all activities in discord on their own server. So the analysis process using this will be done with a makeshift database file.

The database files in the folder will then be examined with SysTools SQLite Viewer.

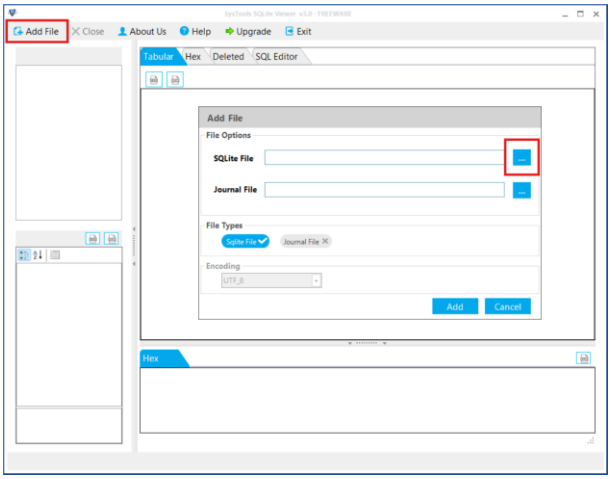


Figure 26: Database File Addition Process

Figure 26 show the process of adding a database file. Starting from clicking add-file in the upper left corner, then after the add-file menu appears, click the three dots next to the SQLite File column.

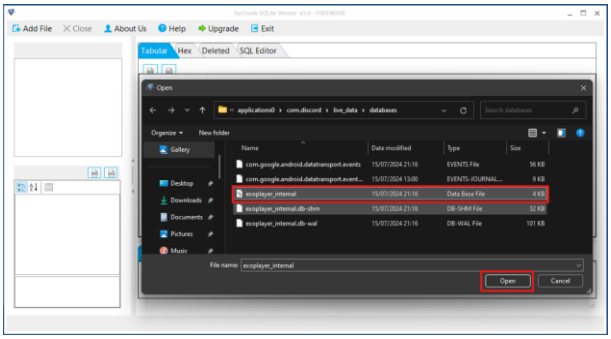


Figure 27: Open Database Process

Figure 27 show the database file obtained from the previous process. Select the file with the type "Data Base File" and click "Open" to continue the database inspection process.

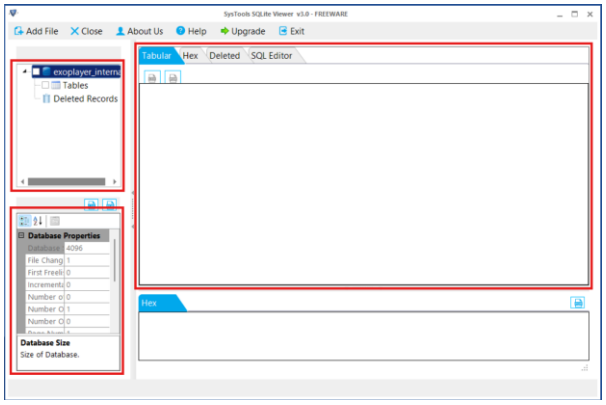


Figure 28: Contents of the Database File

Figure 28 show the Systools SQLite Viewer after inserting the database file. Since Discord does not store data locally, the database file was found to be empty and could not be examined further.

4.2.4 Analysis

The results of the digital evidence collection using MOBILEdit Forensics Express successfully acquired image evidence stored in the application cache files. Once identified, the evidence found pointed to cyberbullying activities in accordance with the reports received.

4.2.4.1 Analysis with MOBILEdit Forensics Express

The results of digital evidence collection using MOBILEdit Forensics Express successfully acquired image evidence stored in the application cache file. Once identified, the evidence found leads to cyberbullying activities according to the reports received.

4.2.4.2 Analysis with Discord Chat Exporter

From the results of examining the TXT and HTML files from the Discord chat export using tokens, the appearance of the chat room matches the original. This facilitates the identification of cyberbullying by user niaraaa against biyavashaaa, as evidenced by the similarity of the profile picture in the chat and during examination with MOBILEdit Forensics Express. A detailed comparison between the TXT, HTML, and original chat room files can be seen in Table 6.

Table 6: Comparison of Digital Evidence of TXT, HTML, and Discord Chat Room Files

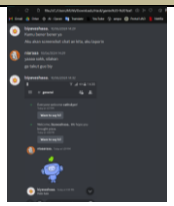
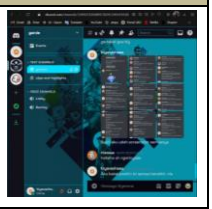
Evidence from TXT file	Evidence from HTML file	Chat Room from Discord
		

Table 6 show a comparison of the exported chat room evidence image with the original chat room. The screenshot image evidence that was sent by the victim to the chat room can also be evidence that the export results are valid. This is evidenced by the link obtained in the TXT file is the same as the screenshot link in the HTML file and the original chat room.

Comparison of links from TXT, HTML, and Discord Web files can be found in Table 7.

Table 7: Comparison of Links from TXT, HTML, and Original Discord Files

https://cdn.discordapp.com/attachments/**1249431838938894429/1249627332805922917/Screenshot_2024-06-10-14-30-28.png**?	TXT File
https://cdn.discordapp.com/attachments/**1249431838938894429/1249627332805922917/Screenshot_2024-06-10-14-30-28.png**?	HTML File
https://media.discordapp.net/attachments/**1249431838938894429/1249627332805922917/Screenshot_2024-06-10-14-30-28.png**?	Discord App

Table 7 show that the file naming of the results of the TXT and HTML file data export screenshots is exactly the same as that in the Discord Application, this corroborates the results of the checks that have been carried out.

4.2.4.3 Analysis with SysTools SQLite Viewer

Due to the absence of database files from the data retrieval process carried out previously, making database checks using Systools SQLite Viewer cannot be done, so analysis with Systools SQLite Viewer also cannot be done.

4.2.5 Reporting

This report presents the examination results and digital evidence related to cyberbullying cases on Discord Mobile. Evidence was collected using forensic tools such as MOBILEdit Forensics Express, Discord Chat Exporter, and Systools SQLite Viewer from the victim's smartphone and Discord account. The examination process involved in-depth analysis of the data, ensuring the integrity of the evidence as per the National Institute of Justice (NIJ) method. Details of the digital evidence are presented in Table 8.

Table 8: Digital Evidence Findings

Results of Findings	MOBIL Edit Forensic Express	Discord Chat Exporter	Systools SQLite Viewer	Total
Usernames of Server members	-	✓	-	3
Text of conversations between the victim and the perpetrator	-	✓	-	77
Profile picture of server members	✓	✓	-	6
Screenshot image sent by the victim	✓	✓	-	18
Total Application Findings	12	92	0	104

Table 8 show digital evidence from cyberbullying cases on the Discord Platform, investigated with three different forensic tools. MOBILEdit Forensics Express collected evidence from the Discord Mobile App, including acquisition and extraction reports in the form of PDF files. Discord Chat Exporter identified usernames, conversation texts, and screenshots from victims on Discord Mobile. The diagram in Figure 29 shows the percentage of evidence from each tool used.

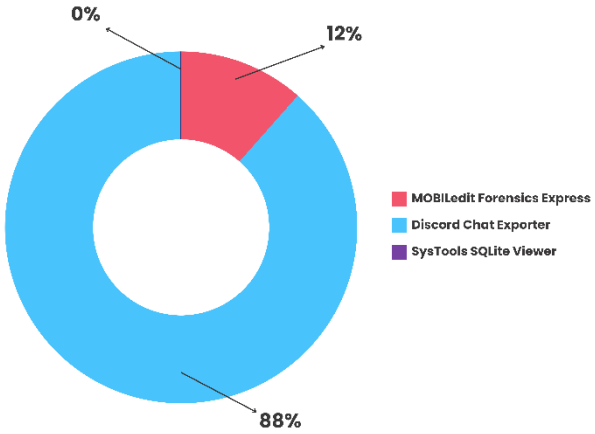


Figure 29: Percentage of Findings Diagram

Figure 29 show the percentage diagram of findings during the implementation process. Conversation texts from the Discord Chat Exporter were the most abundant, with 92 items (88%). Evidence included server member usernames, conversation text, profile pictures, and screenshots of the victim. MOBILEdit Forensics Express found 12 items (12%), which were profile pictures and screenshots. Systools SQLite Viewer found nothing, with 0%. This report was prepared according to the National Institute of Justice (NIJ) rules which include preparation, collection, examination, analysis, and reporting.

5. CONCLUSION

The results of research with the title 'Mobile Forensic Analysis of Discord Services Cyberbullying Case using National Institute of Justice Method' has been successfully carried out and several conclusions can be drawn as follows:

1. Research conducted using the National Institute of Justice (NIJ) method has proven to be successfully applied to cyberbullying digital forensics cases on Discord services. All processes of collecting and analysing digital evidence are carried out using the five stages in the NIJ method, namely preparation or identification, collection, examination, analysis, and reporting.
2. The collection and analysis process assisted by forensic tools such as MOBILEdit Forensics Express and Discord Chat Exporter produces digital evidence in the form of conversation text, screenshot images, usernames and profile pictures used by the perpetrator. And the use of Systools SQLite Viewer did not succeed in producing evidence because there were no files or databases that could be analysed. So that only MOBILEdit Forensics Express and Discord Chat Exporter can prove cyberbullying cases in accordance with the reports received.

6. REFERENCES

[1] 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.

[2] D. Yuliana, T. Yuniati, and B. P. Zen, "Analisis Forensik Terhadap Kasus CyberBullying pada Instagram dan

WhatsApp Menggunakan Metode National Institute of Justice (NIJ)," CyberSecurity dan Forensik Digital, vol. 5, no. 2, pp. 51–59, Nov. 2022.

[3] Werner Geyser, "The Latest Discord Statistics: Servers, Revenue, Data, and More," Influencer Marketing Hub. Accessed: Jun. 19, 2023. [Online]. Available: https://influencermarketinghub.com/discord-stats/

[4] 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, doi: 10.33096/busiti.v3i4.1425.

[5] F. R. D. Miarsa and A. H. Romadhon, "Pelanggaran Hukum dalam Tindakan Vandalisme di Ruang Cyberspace," Jurnal Ilmu Sosial dan Humaniora, vol. 1, no. 1, Oct. 2020.

[6] G. Pawitradi and I. K. G. Suhartana, "Acquisition of LINE Digital Social Media Evidence Using the National Institute of Justice (NIJ) Method," Jurnal Elektronik Ilmu Komputer Udayana, vol. 8, no. 2, Nov. 2019.

[7] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method," Int J Comput Appl, vol. 177, no. 27, pp. 35–42, Dec. 2019, doi: 10.5120/ijca2019919749.

[8] K. D. O. Mahendra and I. K. A. Mogi, "Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases," Jurnal Elektronik Ilmu Komputer Udayana, vol. 9, no. 3, Feb. 2021.

[9] Herman, A. Yudhana, and F. Anggraini, "Akusisi Bukti Digital TikTok Berbasis Android Menggunakan Metode National Institute of Justice," Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), vol. 10, no. 1, pp. 89–96, Feb. 2023, doi: 10.25126/jtiik.2023106416.

[10] R. A. Ramadhan and D. Mualfah, "Implementasi Metode National Institute of Justice (NIJ) Pada Fitur TRIM SOLID STATE DRIVE (SSD) Dengan Objek Eksperimental Sistem Operasi Windows, Linux dan Macintosh," IT Journal Research and Development, vol. 5, no. 2, pp. 183–192, Nov. 2020, doi: 10.25299/itjrd.2021.vol5(2).5750.

[11] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," Jurnal Media Informatika Budidarma, vol. 6, no. 2, pp. 1263–1271, 2022.

[12] R. N. Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial," Techno. Com, vol. 20, no. 4, pp. 527–539, 2021.

[13] I. Riadi, A. Yudhana, and M. C. F. Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)," Jurnal Teknik Informatika dan Sistem Informasi, vol. 4, no. 2, pp. 219–227, 2018.

[14] R. Adijisman and I. Riadi, "Mobile Forensic on WhatsAppServices using National Institute of Standards and Technology Method," Int J Comput Appl, vol. 183, no. 29, pp. 41–48, Oct. 2021, doi: 10.5120/ijca2021921680.

[15] M. Marzuki and T. Sutabri, "Analisis Forensik Media Sosial MiChat Metode Digital Forensik Integrated Investigation Framework (IDFIF)," Blantika: Multidisciplinary Journal, vol. 2, no. 1, pp. 56–70, 2023.

[16] U.S. Departement of Justice, "About NIJ | About the National Institute of Justice." Accessed: Jun. 21, 2023. [Online]. Available: https://nij.ojp.gov/about-nij

[17] Y. Prayudi, "Problema dan Solusi Digital Chain of Custody Dalam Proses Investigasi Cybercrime," in Senasti-Seminar Nasional Sains dan Teknologi Informasi, 2014, p. 8.

[18] Moh. Ali, Y. Prayudi, and B. Sugiantoro, "Storage Area Network Architecture to support the Flexibility of Digital Evidence Storage," Int J Comput Appl, vol. 182, no. 41, pp. 30–35, Feb. 2019, doi: 10.5120/ijca2019918496.

[19] G. Mishardila, "Analisa Dan Pencarian Bukti Forensik Digital Pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik," Thesis, Universitas Islam Riau, Riau, 2020.

[20] A. S. Prashinta, "Pengembangan Aplikasi Akuisisi Forensik Digital Menggunakan Sistem Operasi Linux Debian," Universitas Islam Indonesia, Yogyakarta, 2020.

[21] A. Yudhana, R. Umar, and A. Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)," vol. X, no. X, pp. 8–13, 2018.

[22] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," J-SAKTI (Jurnal Sains Komputer dan Informatika), vol. 6, no. 2, pp. 1112–1120, 2022.

[23] N. M. Jalal, M. Idris, and M. Muliana, "Faktor-faktor cyberbullying pada remaja," IKRA-ITH HUMANIORA: Jurnal Sosial dan Humaniora, vol. 5, no. 2, pp. 1–9, 2021.

[24] P. Widiandana and I. Riadi, "Implementasi Metode Jaccard pada Analisis Investigasi Cyberbullying WhatsApp Messenger Menggunakan Kerangka Kerja National Institute of Standards and Technology," Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. 4, no. 6, pp. 1046–1051, 2020.

[25] D. Fitri, A. Anismar, M. Fazil, and C. W. Ula, "Smartphone Sebagai Gaya Hidup Mahasiswa (Studi pada Mahasiswa FISIP 2018)," Jurnal Jurnalisme, vol. 10, no. 1, p. 32, Aug. 2021, doi: 10.29103/jj.v10i1.4791.

[26] T. Adella and T. Widodo, "Utilization of Android Technology in an Integrated Information System for Car Booking Service," Int J Comput Appl, vol. 186, no. 4, pp. 12–17, Jan. 2024, doi: 10.5120/ijca2024923380.

[27] Bayu and Surti, "Discord: Pengertian, Kelebihan, dan Cara Menggunakannya | Gamer dapat saling komunikasi tanpa ganggu sistem bermain.," Fortune Indonesia. Accessed: Jun. 24, 2023. [Online]. Available: https://www.fortuneidn.com/tech/bayu/pengertian-discord-adalah

[28] Nur Maghfirah Aesthetika and M. S. Rizal, "Efektifitas Penggunaan Aplikasi Discord Dalam Meningkatkan Komunikasi Interpersonal Di Kalangan Pencinta Film," Medium, vol. 10, no. 1, pp. 19–27, Apr. 2022, doi: 10.25299/medium.2022.vol10(1).8882.

[29] Forensic Focus, "Mobiledit Forensic Express From Compelson," Forensic Focus For Digital Forensics & E-Discovery Professionals. Accessed: Jun. 24, 2023. [Online]. Available: https://www.forensicfocus.com/reviews/mobiledit-forensic-express-from-compelson/

[30] I. Anshori et al., "Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ," IT Journal Research and Development (ITJRD), vol. 5, no. 2, 2021, doi: 10.25299/itjrd.2021.vol5(2).4664.

[31] Oleksii Holub, "Discord Chat Exporter," GitHub. Accessed: Jun. 14, 2024. [Online]. Available: https://github.com/Tyrrrz/DiscordChatExporter

[32] SoftwareSuggest, "What is SysTools SQLite Viewer?," SoftwareSuggest. Accessed: Jun. 26, 2023. [Online]. Available: https://www.softwaresuggest.com/systools-sqlite-viewer

[33] Y. Arif, E. I. Alwi, and M. A. Asis, "Analisis Bukti Digital Direct Message Pada Twitter Menggunakan Metode National Institute Of Justice (NIJ)," INFORMAL: Informatics Journal, vol. 8, no. 2, p. 165, Aug. 2023, doi: 10.19184/isj.v8i2.34025.

[34] L. C. Pakaya and I. Riadi, "Forensic Analysis of Web-based Instant Messenger Applications using National Institute of Justice Method," Int J Comput Appl, vol. 185, no. 35, pp. 44–51, Sep. 2023, doi: 10.5120/ijca2023923145.