Digital Forensic Analysis of Pornography Cases on Discord Platform using National Institute of Standards and Technology Method

Ivan Darmawan
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The dissemination and transaction of pornographic content through digital communication platforms such as Discord have become increasingly concerning due to their real-time and community-based features. This platform is frequently exploited as a medium for illegal activities involving the distribution of pornographic content through servers and direct messages. To address this issue, this study aims to conduct a digital forensic analysis of pornography-related cases on the Discord platform using the National Institute of Standards and Technology (NIST) framework, which consists of four main stages: collection, examination, analysis, and reporting. Primary data collection was also conducted through a simulated transaction scenario involving three user accounts: a link distributor, a buyer, and a server administrator. The investigation process focused on Android smartphones utilizing a combination of forensic tools, including MOBILedit Forensic, Magnet AXIOM, and Discord Chat Exporter. The results indicate that the investigation process successfully identified a total of 100 digital artifacts that served as evidence of the crime. These artifacts included chat histories, server links, media files, payment transaction records, profile pictures, and timestamps. The artifact distribution consisted of 58 artifacts recovered using Discord Chat Exporter, 22 artifacts obtained through Magnet AXIOM, and 20 artifacts extracted using MOBILedit Forensic Express. The combined use of these three tools proved to be complementary, enabling a highly comprehensive digital forensic investigation process.

Keywords
Discord, Pornography, Digital Forensics, NIST, Magnet AXIOM

1. INTRODUCTION
The development of information technology in Indonesia has shown a highly significant upward trend, particularly in internet usage and digital communication services. According to Badan Pusat Statistik, Indonesia's population in 2024 reached 281.6 million people, accompanied by positive growth in the adoption of digital communication technology across the country [1]. According to the Digital 2024 report published by Meltwater, the number of internet users in Indonesia exceeded 185.3 million people [2]. In contrast, the 2024 report from Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) estimated that internet users in Indonesia had surpassed 221,563,479 individuals [3]. This condition has driven the widespread use of online communication platforms, one of which is Discord. Discord is a free application that provides real-time communication services similar to Slack and Skype, enabling users to interact through text, voice, and video messages in a manner comparable to other voice chat platforms [4]. Discord offers high-quality chat room features for direct communication and also provides functionalities such as chat, video conferencing, and screen sharing, allowing users to communicate more flexibly and effectively [5]. Furthermore, Discord enables community management through structured and organized servers [6]. The platform functions as a hub for digital communities, making the communication patterns within it reflective of emerging future trends [7]. However, the anonymity features provided by Discord have also made the platform vulnerable to misuse. Previous studies have shown that Discord is frequently exploited for the distribution of illegal content such as child pornography, drug trafficking, and other cybercrimes, primarily due to its capability to conceal user identities, as well as its support for encryption and permanent message deletion [8]. The high potential for misuse has created new challenges in law enforcement processes. Therefore, an investigative method capable of uncovering concealed digital activities and recovering deleted evidence is urgently required. In this context, digital forensics plays a crucial role.

Digital forensics is a branch of computer science that supports data analysis and investigation processes, providing evidence of crimes involving digital devices and identifying cybercriminals [9]. Investigative procedures in digital forensics can be conducted using various methodologies, including the National Institute of Justice (NIJ), Integrated Digital Forensics Investigation Framework (IDFIF), Digital Forensics Research Workshop (DFRWS), and the National Institute of Standards and Technology (NIST) framework [10]. Among these, the NIST method is the most widely recommended and comprehensively adopted approach [11]. This framework provides a systematic yet comprehensive set of procedures consisting of four primary stages: Collection, Examination, Analysis, and Reporting [12]. Through this method, forensic investigation procedures can be conducted consistently, which is essential for maintaining the integrity of the investigative process [13].

The implementation of the NIST framework is often supported by various forensic tools. Previous studies have reported that Magnet AXIOM was capable of recovering up to 94.11% of digital artifacts from scenarios involving the distribution of sexual content through Discord. Meanwhile, forensic tools such as Autopsy have also been proven effective in restoring deleted files, including in data theft cases, with integrity validation performed using MD5 hash verification [14]. Other studies have further demonstrated the effectiveness of Magnet AXIOM in handling cases involving the distribution of pornographic content through cloud storage services such as Google Drive, successfully recovering deleted image and video files as legal digital evidence [15]. Although numerous studies have explored digital forensic investigations on instant messaging platforms, investigations specifically targeting the

dissemination and transaction of pornographic content on Discord using a combination of forensic tools simultaneously remain limited.

Based on this research gap, this study aims to conduct a digital forensic analysis of pornography-related cases on the Discord platform and to identify digital artifacts associated with such criminal activities. This research adopts a forensic approach based on the National Institute of Standards and Technology (NIST) framework by integrating MOBILedit Forensic, Magnet AXIOM, and Discord Chat Exporter to maximize the acquisition process and perform cross-validation of digital evidence. The findings of this study are expected to contribute academically and serve as a reference for law enforcement agencies in addressing cybercrime in Indonesia.

2. LITERATURE STUDY

2.1 Digital Forensics

Digital forensics is a scientific discipline focused on identifying, collecting, and evaluating digital data as evidence in information technology investigations [16]. Its primary objective is to obtain and preserve evidence that is legally admissible across various case resolution contexts [17]. This field serves as a comprehensive investigative approach for validating data in order to establish a strong evidentiary foundation in court proceedings [18]. Investigative practices within digital forensics must be conducted systematically through five main stages: identification, preservation, analysis, documentation, and presentation [19]. The main stages are illustrated in Figure 1.

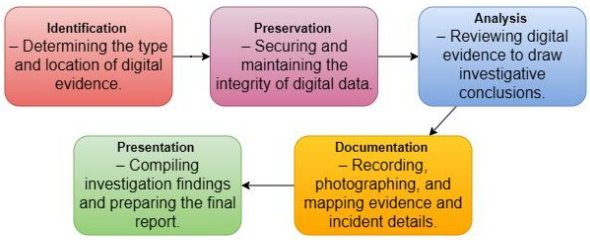


Figure 1: Main Stages of Digital Forensics

The existing branches of this discipline include computer forensics, which focuses on acquiring digital evidence from computer systems. In addition, mobile forensics is specifically concerned with the analysis of electronic evidence obtained from mobile devices [20].

2.2 Pornography

Pornography refers to the explicit representation of the human body or sexual activities, whether in the form of text or visual imagery, intended to stimulate the sexual desire of its audience [21]. In the digital era, the cycle of this criminal activity begins with the production of content, followed by its upload to online platforms such as Discord, and continues through both open and concealed distribution channels that ultimately lead to user consumption. Such content can be distributed extensively through various media formats, including audio, visual, and audiovisual content [22]. Excessive exposure to pornography may lead to highly destructive addictive behavior comparable to narcotics, often referred to as narkolema (visual narcotics), as it can flood the brain with dopamine and damage the structure of the prefrontal cortex (PFC) [23]. Therefore, preventive measures are essential through education, parental supervision of device usage, and cross-sector collaboration to protect users from the dangers of digital environments.

2.3 Discord

Discord is a free online communication application designed to facilitate real-time interaction through text, voice, and video messaging [24]. The platform enables users to manage communities in a structured manner through the creation of servers consisting of various specific channels [25]. In addition to its popularity as a community platform, Discord also demonstrates significant potential for utilization in various other fields, including education, as it supports more dynamic interactions between educators and students. The platform's functionality is further enhanced by its screen-sharing feature, which facilitates interactive and efficient remote collaboration [25]. Despite offering a wide range of advanced communication capabilities, the effectiveness of the platform remains highly dependent on external user-related factors, such as internet connection stability and device specifications [26].

2.4 National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is an institution responsible for developing standards and information security guidelines intended for digital forensic practitioners, including government agencies and law enforcement authorities. This framework serves as a guideline for resolving investigative issues more effectively through structured and detailed procedures [27]. To maintain the integrity of digital evidence so that it remains valid and admissible in court proceedings, the NIST framework establishes four primary stages: collection, examination, analysis, and reporting. The stages of the digital forensic investigation method based on the NIST framework are illustrated in Figure 2.

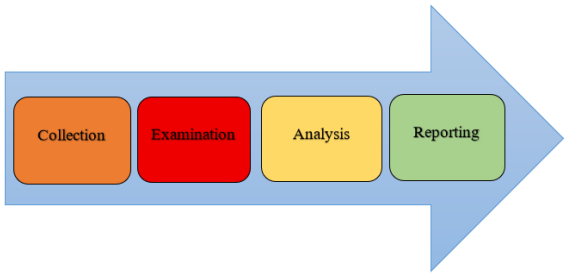


Figure 2: Stages of the NIST Methodology

2.5 Digital Evidence

Digital evidence encompasses all forms of electronic information obtained from physical devices and cloud services that are essential to investigative and law enforcement processes [28]. In practice, digital evidence is not limited to file contents or message data, but also includes metadata, system logs, and hidden artifacts that specifically record user interactions [29]. The examination of all such data elements must be conducted rigorously to ensure the validity, evidentiary strength, and integrity of the evidence so that it can be legally admissible in court proceedings [30].

2.6 Magnet AXIOM

Magnet AXIOM is an integrated digital investigation platform designed to recover, analyze, and generate evidence reports from various sources, including mobile devices, computers, and cloud services [31]. The software is equipped with Magnet AI technology, which is capable of detecting sexually explicit conversations or indications of grooming, as well as identifying illegal images related to child exploitation as part of digital investigative evidence [32].

2.7 MOBILedit Forensic Express

MOBILedit Forensic is a digital forensic software solution specifically designed for smartphone investigations to perform data extraction, artifact analysis, and forensic report generation [31]. This tool has proven effective in recovering deleted data and acquiring comprehensive information, including contacts, messages, multimedia files, passwords, and communication histories from various social media applications [32].

2.8 Discord Chat Exporter

Discord Chat Exporter is a software application designed to export Discord conversation histories from private messages, group chats, and server channels into various file formats, including TXT, HTML, JSON, and CSV. The application also supports markdown-format extraction as well as the retrieval of various media attachments contained within conversations [33].

3. RESEARCH METHOD

This study simulated the dissemination and transaction of pornographic content on Discord using three fictitious accounts within a controlled environment. The primary object of investigation was a rooted Android smartphone (Xiaomi Redmi 9A), enabling investigators to access system directories and internal application data. Digital evidence extraction and analysis were conducted using MOBILedit Forensic, Magnet AXIOM, and Discord Chat Exporter to maximize evidence acquisition and cross-validation. MOBILedit and Magnet AXIOM were utilized for logical acquisition and timeline reconstruction, while Discord Chat Exporter was specifically used to extract conversation histories through account tokens. All investigative procedures strictly adhered to the National Institute of Standards and Technology (NIST) framework, including Collection, Examination, Analysis, and Reporting, to ensure the integrity and admissibility of digital evidence.

3.1 Research Scenario

This scenario simulates the dissemination and transaction of pornographic content on Discord using three fictitious accounts: Agif (link distributor), Beh (buyer), and Ipan (server administrator and content seller). The simulation is divided into three main stages: pre-incident, incident, and post-incident.

1. Pre-Incident

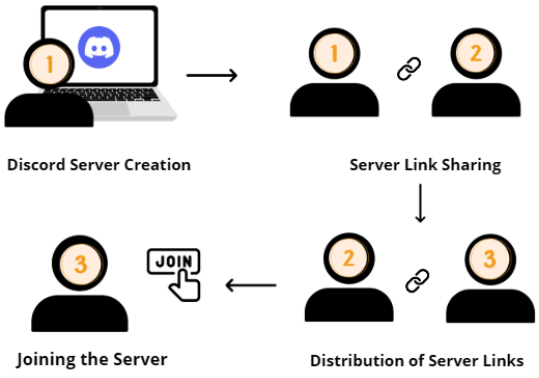


Figure 3: Pre-Incident Simulation

Figure 3 illustrates that the preparation stage began with the creation of a private Discord server by Ipan. Ipan then provided an invitation link to Agif, who distributed it to Beh through a direct message along with information regarding the availability of paid content. After Beh received the invitation and joined the server, all activities were monitored to record the initial conditions prior to the occurrence of the illegal transaction. This stage was designed to simulate the initial interaction process and establish the digital traces required for forensic investigation. Furthermore, the generated communication activities served as the primary source of digital evidence for the subsequent forensic analysis process.

2. Incident

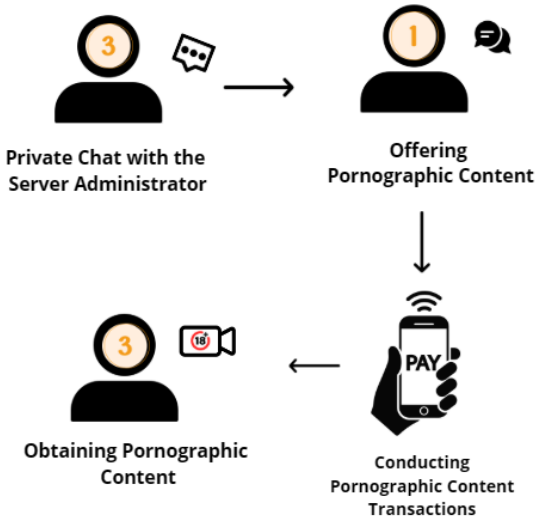


Figure 4: Incident Simulation

Figure 4 illustrates that this phase began when Beh contacted Ipan through a direct message on Discord to purchase pornographic content. After an agreement regarding the price and payment method was reached, Ipan delivered the illegal content files to Beh. All communication histories, transaction records, and media files in this scenario were intentionally preserved without deletion to ensure that digital traces, such as timestamps, account identities, and file exchange histories, were automatically recorded on the target Android device for forensic extraction purposes.

3. Post-Incident

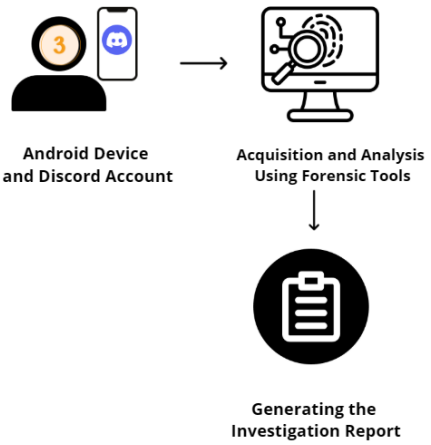


Figure 5: Post-Incident Simulation

Figure 5 illustrates that the final stage focused on handling digital evidence through the acquisition and analysis of data obtained from Beh's smartphone. Using a combination of MOBILedit Forensic, Magnet AXIOM, and Discord Chat Exporter, investigators extracted various digital artifacts, including conversation histories, media files, server links, and

activity timestamps. All findings were then thoroughly investigated based on the National Institute of Standards and Technology (NIST) framework, encompassing the stages of Collection, Examination, Analysis, and Reporting, before being compiled into a valid, comprehensive, and accountable forensic report.

3.2 National Institute of Standards and Technology Framework

The digital forensic investigation process in this study was specifically conducted based on the four stages of the National Institute of Standards and Technology (NIST) framework, namely :

1. Collection

The digital data collection stage was conducted on the target Android smartphone using MOBILedit Forensic, Magnet AXIOM, and Discord Chat Exporter to ensure that the authenticity of the data was preserved without modification. The data collected during this stage included conversation histories, media files, server links, and user activity timestamps. All acquired data were securely preserved to maintain the integrity and reliability of the digital evidence throughout the investigation process.

2. Examination

This stage focused on the examination and extraction of digital artifacts that had been successfully secured from the target device. The three forensic tools were utilized to filter and extract information specifically related to illegal activities conducted through the Discord application.

3. Analysis

All extracted digital artifacts were subsequently analyzed to identify and determine the relationships between user activities. The analysis focused on conversation histories, server link distribution, payment transactions, and media file transfers.

4. Reporting

This final stage involved compiling all examination and analysis results into a structured digital forensic report. The report documented all valid digital evidence related to the dissemination and transaction of pornographic content on the Discord application.

4. RESULTS AND DISCUSSION

This section presents the results of a digital forensic investigation on the dissemination and transaction of pornographic content through Discord using an Android smartphone. The investigation followed the National Institute of Standards and Technology (NIST) framework and utilized MOBILedit Forensic, Magnet AXIOM, and Discord Chat Exporter to obtain valid and comprehensive digital evidence.

4.1 Collection

The evidence collection stage began with securing the target Android smartphone (Xiaomi Redmi 9A) belonging to the investigation target (Beh account). The technical specifications of the device were thoroughly documented and verified to have root access using Root Checker Basic and Magisk, enabling investigators to obtain full access privileges to the device's protected system directories. Detailed specifications of the smartphone secured as the primary digital evidence are presented in Table 1. Verifying root access at this stage was crucial, as standard Android security sandboxing restricts access to private application folders (including Discord's databases). Confirming superuser privileges allowed the investigators to bypass these system-level restrictions, ensuring a complete and unrestricted data extraction in the subsequent steps.

Table 1. Smartphone Specifications

Description	Detail
Smartphone Brand	Redmi 9A
Model Number	M2006C3LG
IMEI 1	861716052758504
IMEI 2	861716052758512
Android Version	10 QP1A.190711.020
Chipset	Octa-core Max 2.00GHz
Storage	32 GB
MIUI Version	MIUI Global 12.0.10 Stabil 12.0.10.0 (QCDIDXM)
RAM	3 GB

Following the device verification process, digital evidence acquisition was performed using three forensic tool approaches: These approaches were strategically combined to establish a multi-layered acquisition workflow, targeting both local physical storage and cloud-based server logs. This multi-faceted extraction ensures maximum artifact recovery while enabling cross-validation of the retrieved digital evidence.

A. MOBILedit Forensic Express

The The initial physical extraction process was performed through a Micro-USB cable connection using the Application Analysis method. This method specifically extracted local package data from the Discord application (com.discord) stored on the device and generated it into a final forensic report document. By targeting the local application directory directly, this method ensures that local cache files, database configurations, and temporary application assets are retrieved without tampering. This local acquisition serves as a critical baseline to verify and secure locally stored digital evidence before the examination phase begins. The acquisition results obtained from MOBILedit Forensic are presented in Figure 6.

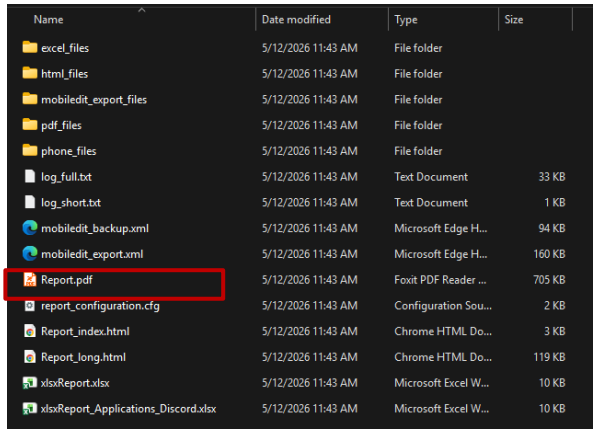
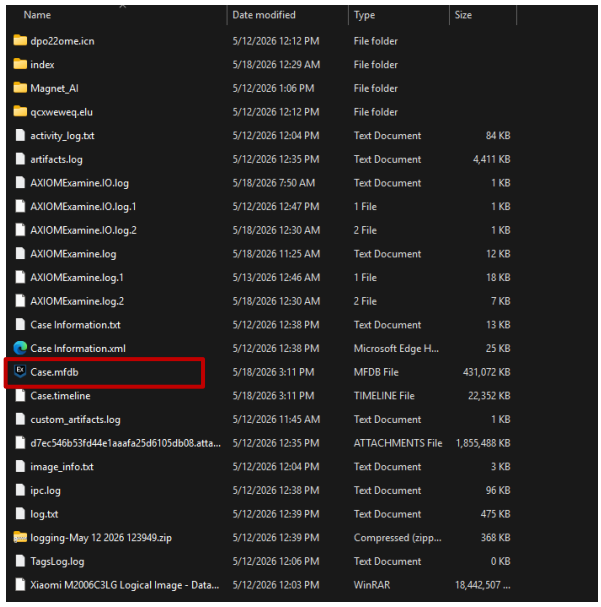


Figure 6: Extraction Folder Generated by MOBILedit Forensic Express

B. Magnet AXIOM

The data acquisition process was continued using Magnet AXIOM through the Logical Acquisition method based on an Android Debug Bridge (ADB) connection in Unlocked mode. Since the target smartphone had already been rooted, this method enabled the imaging process to securely copy user and application data to the forensic workstation without damaging or altering the authenticity of the data stored in the device's

physical memory. The acquisition results obtained from Magnet AXIOM are presented in Figure 7.

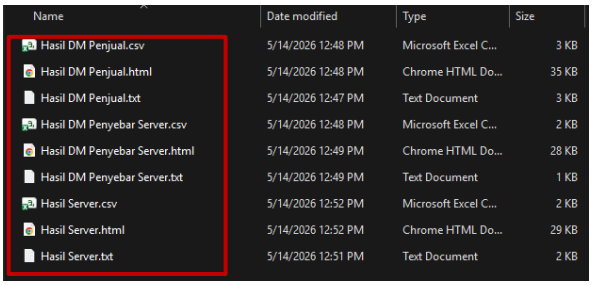


Name	Date modified	Type	Size
dpo22ome.icn	5/12/2026 12:12 PM	File folder	
index	5/18/2026 12:29 AM	File folder	
Magnet_AI	5/12/2026 1:06 PM	File folder	
qcxweweq.elu	5/12/2026 12:12 PM	File folder	
activity_log.txt	5/12/2026 12:04 PM	Text Document	84 KB
artifacts.log	5/12/2026 12:35 PM	Text Document	4,411 KB
AXIOMExamine.IO.log	5/18/2026 7:50 AM	Text Document	1 KB
AXIOMExamine.IO.log.1	5/12/2026 12:47 PM	1 File	1 KB
AXIOMExamine.IO.log.2	5/18/2026 12:30 AM	2 File	1 KB
AXIOMExamine.log	5/18/2026 11:25 AM	Text Document	12 KB
AXIOMExamine.log.1	5/13/2026 12:46 AM	1 File	18 KB
AXIOMExamine.log.2	5/18/2026 12:30 AM	2 File	7 KB
Case Information.txt	5/12/2026 12:38 PM	Text Document	13 KB
Case Information.xml	5/12/2026 12:38 PM	Microsoft Edge H...	25 KB
Case.mfdb	5/18/2026 3:11 PM	MFDB File	431,072 KB
Case.timeline	5/18/2026 3:11 PM	TIMELINE File	22,352 KB
custom_artifacts.log	5/12/2026 11:45 AM	Text Document	1 KB
d7ec546b53fd44e1aaafa25d6105db08.atta...	5/12/2026 12:35 PM	ATTACHMENTS File	1,855,488 KB
image_info.txt	5/12/2026 12:04 PM	Text Document	3 KB
ipc.log	5/12/2026 12:38 PM	Text Document	96 KB
log.txt	5/12/2026 12:39 PM	Text Document	475 KB
logging-May 12 2026 123949.zip	5/12/2026 12:39 PM	Compressed (zipp...	368 KB
TagsLog.log	5/12/2026 12:06 PM	Text Document	0 KB
Xiaomi M2006C3LG Logical Image - Data...	5/12/2026 12:03 PM	WinRAR	18,442,507 ...

Figure 7: Extraction Folder Generated by Magnet AXIOM

C. Discord Chat Exporter

Since the Discord application stores most conversation histories on its central servers, communication data could not be fully acquired solely through local device extraction. Therefore, additional data collection was conducted using Discord Chat Exporter by extracting the target account's authentication token through the Developer Tools feature in a web browser. Using this confidential token, complete conversation histories from server channels and private messages (direct messages) were retrieved and exported into TXT, HTML, JSON, and CSV formats to preserve the digital traces. The acquisition results obtained from Discord Chat Exporter are presented in Figure 8.

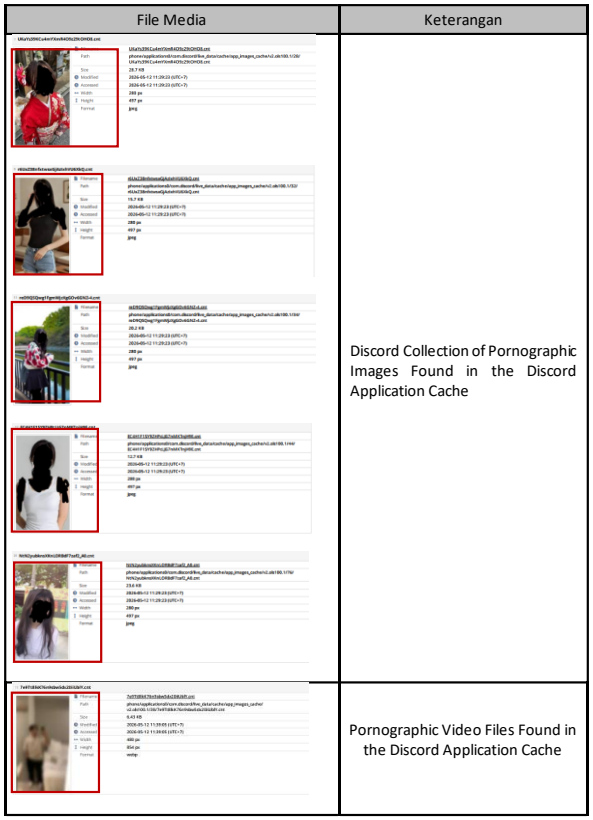


Name	Date modified	Type	Size
Hasil DM Penjual.csv	5/14/2026 12:48 PM	Microsoft Excel C...	3 KB
Hasil DM Penjual.html	5/14/2026 12:48 PM	Chrome HTML Do...	35 KB
Hasil DM Penjual.txt	5/14/2026 12:47 PM	Text Document	3 KB
Hasil DM Penyebar Server.csv	5/14/2026 12:48 PM	Microsoft Excel C...	2 KB
Hasil DM Penyebar Server.html	5/14/2026 12:49 PM	Chrome HTML Do...	28 KB
Hasil DM Penyebar Server.txt	5/14/2026 12:49 PM	Text Document	1 KB
Hasil Server.csv	5/14/2026 12:52 PM	Microsoft Excel C...	2 KB
Hasil Server.html	5/14/2026 12:52 PM	Chrome HTML Do...	29 KB
Hasil Server.txt	5/14/2026 12:51 PM	Text Document	2 KB

Figure 8: Extraction Folder Generated by Discord Chat Exporter

4.2 Examination

The examination stage aimed to extract raw data comprehensively using a combination of MOBILedit Forensic, Magnet AXIOM, and Discord Chat Exporter, which complemented one another throughout the investigation process. The initial examination of the extracted Report.pdf document generated by MOBILedit successfully validated the device specifications and revealed crucial artifacts within the cache directory, including the suspect's profile pictures, pornographic media files, and payment transaction evidence, as illustrated in Figure 9.



File Media	Keterangan
	Discord Collection of Pornographic Images Found in the Discord Application Cache
	Pornographic Video Files Found in the Discord Application Cache

Figure 9: Pornographic Media Files Identified in MOBILedit Forensic Express

The examination process continued using Magnet AXIOM to analyze the logical image file extracted from the target device. This software effectively reconstructed the user activity timeline, including search histories, download activities, and the execution timestamps of the Discord application on the smartphone, as illustrated in Figure 10.

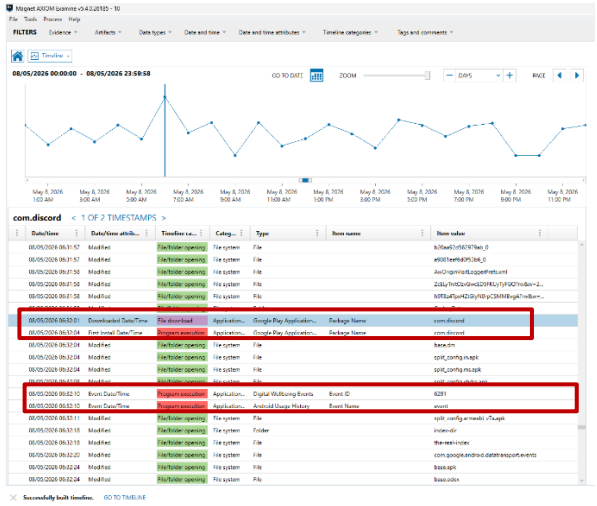


Figure 10: Download and Discord Execution Timeline in Magnet AXIOM

In-depth extraction of the cache directory also successfully identified hidden files with the .cnt extension, which, after validation, were found to contain pornographic content and records of bank transfer transactions.

To strengthen the investigative findings, the final examination stage was conducted on the TXT and HTML output files generated by Discord Chat Exporter. These extraction results successfully displayed complete and transparent communication records resembling the original application interface. The extracted data revealed the chronology of direct message conversations involving the distribution of server invitation links, communication activities among members within server channels, and detailed negotiations regarding pricing and the delivery of pornographic content between the buyer and seller. A sample of the chat log evidence is shown in Figure 11.

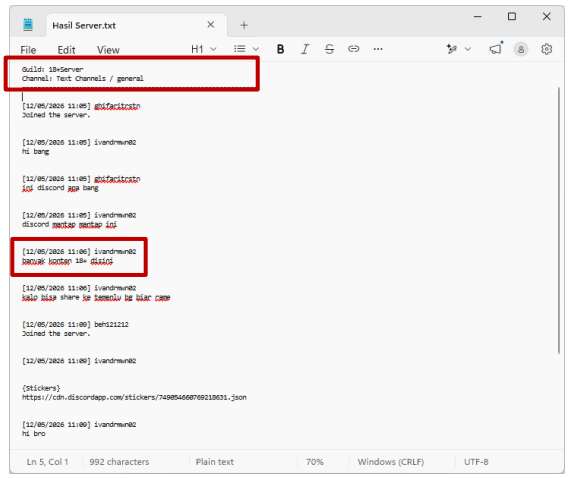


Figure 11: Chat Log Evidence Exported via Discord Chat Exporter

All artifact findings obtained from the three forensic tools were subsequently consolidated for further evaluation during the analysis stage.

4.3 Analysis

The analysis phase aims to correlate all digital artifacts identified during the examination stage to comprehensively reconstruct the sequence of the crime. A consolidated analysis utilizing three forensic software tools revealed a structured scheme involving the distribution and transaction of pornographic content within the Discord platform.

An in-depth analysis of the communication logs using Discord Chat Exporter explicitly demonstrated the interaction flow between users. The extraction of TXT and HTML files, which accurately replicated the original Discord interface, revealed that the account Agif actively distributed an invite link to the target account (Beh) via direct message. Once the target joined the private server designated as "18+Server," the account Ipan, acting as the administrator, instructed the user to proceed with the transaction privately. Further investigation of the direct messages between the Beh and Ipan accounts detailed the price negotiation process, payment confirmation, and the subsequent transmission of pornographic media files.

The findings derived from the cloud-based communication logs were subsequently corroborated by an analysis of local memory artifacts utilizing Magnet AXIOM and MOBILedit Forensic Express. Magnet AXIOM successfully reconstructed the user activity timeline, providing evidence that the Discord application was intentionally searched for, downloaded, installed, and actively executed on the target's smartphone. Furthermore, an examination of the application's cache directory using both tools revealed the presence of hidden files, including those with a .cnt extension. Subsequent analysis demonstrated that this cache directory retained the perpetrators' profile pictures (Agif and Ipan), screenshots of payment receipts, and a collection of pornographic images and videos identical to the files transmitted within the chat logs.

Overall, this analysis demonstrates that the utilization of these three forensic software tools is optimally complementary in an investigative context. Discord Chat Exporter proved highly effective in extracting comprehensive chat logs directly from Discord's cloud servers, whereas MOBILedit Forensic Express and Magnet AXIOM exhibited significant proficiency in reconstructing system timelines and recovering hidden local artifacts from the physical memory of the target device.

4.4 Reporting

The reporting phase constitutes the final stage in systematically documenting all findings of the digital forensic investigation. According to the reconstructed timeline, the incident commenced on May 12, 2026, at 11:08, when the account Agif transmitted an invite link for a Discord server hosting pornographic content to the target account (Beh) via direct message. Upon joining at 11:09, Beh communicated with the server administrator (Ipan) in the general channel at 11:10, who subsequently redirected the interaction to a private conversation. The negotiation process via direct message commenced at 11:13, followed by the execution of a payment transaction by Beh at 11:27. After verifying the payment, Ipan delivered multiple pornographic images at 11:29, accompanied by an additional video as a bonus. All digital traces of this incident remained entirely intact, with no evidence of any attempts to erase data on the target device.

Based on the investigation findings, the roles of the three fictitious actors were clearly identified: Agif acted as the link distributor, Ipan served as the server administrator and seller, and Beh functioned as the buyer. The recovered evidence included conversation histories, server invitation links, media files, payment transaction records, profile pictures, and activity timestamps, all of which demonstrated the dissemination and transaction of pornographic content on the Discord platform. Overall, the investigation successfully recovered a total of 100 validated digital artifacts, with the detailed percentage distribution of artifacts obtained from each forensic tool presented in Figure 12.

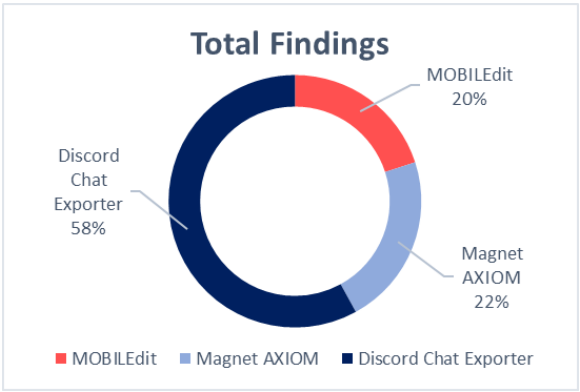


Figure 12: Percentage Distribution of Findings

As illustrated in Figure 12, Discord Chat Exporter yielded the highest percentage of findings, accounting for 58% (58 artifacts), which primarily consisted of chat logs and server links. This was followed by Magnet AXIOM at 22% (22 artifacts), encompassing timeline reconstructions and hidden media files. Meanwhile, MOBILedit Forensic accounted for the remaining 20% (20 artifacts). These findings demonstrate

that each forensic tool possesses distinct capabilities in recovering digital evidence from the target device. The combination of the three tools also improved the comprehensiveness and reliability of the forensic investigation results, while the detailed categories of digital artifacts identified by each tool are presented in Table 2.

Table 2. Findings by Tool

Findings	MOBILedit Forensic Express	Magnet Axiom	Discord Chat Exporter
Discord Account Profile Pictures	✓	✓	✓
Pornographic Images	✓	✓	✓
Pornographic Videos	✓	✓	✓
Proof of Payment Transactions	✓	✓	✓
Discord Chat Logs	-	-	✓
Discord Server Links	-	-	✓
Discord Activity Timestamps	✓	✓	✓

4.5 Evaluation and Comparative Discussion of Forensic Tools

To provide a comprehensive evaluation of the utilized tools, their operational performance was analyzed based on data acquisition layers. Discord Chat Exporter demonstrated high efficiency for cloud-level recovery, extracting 58% of the total artifacts (primarily 40 chat logs and server links) directly from Discord's API using token authentication. However, it remains entirely dependent on token validity and is incapable of recovering local device telemetry. Conversely, Magnet AXIOM (22%) and MOBILedit Forensic Express (20%) targeted the device's physical storage, proving highly superior in reconstructing installation and execution timelines (e.g., tracking the Google Play search and download timestamp on May 8, 2026). Furthermore, they successfully extracted hidden .cnt cached files containing the actual images and payment receipts stored locally. This evaluation confirms that cloud tools are efficient for communication retrieval, whereas physical tools are indispensable for proving physical possession, thereby establishing a robust cross-validation framework.

4.6 Evaluation of Alternative Scenarios

To further evaluate forensic adaptability across different operational scenarios, a simulated deleted-data scenario was analyzed. If a suspect actively deletes Discord chat histories and cached media before device acquisition, the recovery efficiency shifts dramatically. In this scenario, cloud-level extraction using Discord Chat Exporter is rendered completely ineffective because Discord's API immediately synchronizes and wipes deleted messages from active server logs. However, physical-level tools demonstrate high resilience. Magnet AXIOM and MOBILedit Forensic Express can bypass application-level deletions by scanning the smartphone's physical memory partitions (specifically within the com.discord directories). Both tools leverage file-carving techniques to recover deleted localized cache files (such as .cnt images) and reconstruct database remnants stored in the Android system's unallocated space. This scenario comparison demonstrates that while cloud tools are optimal for intact data, local physical tools are indispensable for counteracting active anti-forensic deletion attempts.

5. REFERENCES

[1] Badan Pusat Statistik, "Jumlah Penduduk Pertengahan Tahun (Ribu Jiwa), 2024," Badan Pusat Statistik.

[2] Sue Howe, "Social Media Statistics for Indonesia [Updated 2024]," Meltwater.

[3] APJII, "APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," APJII.

[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. Juliansyah and S. N. Febryanti, "Persepsi Gamer terhadap Penggunaan Aplikasi Discord Sebagai Media Komunikasi Alternatif," JIIP - Jurnal Ilmiah Ilmu Pendidikan, vol. 7, no. 2, pp. 1648–1658, Feb. 2024, doi: 10.54371/jiip.v7i2.3913.

[6] M. Wibowo, M. R. Firmansyah, and R. S. Efendi, "Analisis Bukti Digital Pada Aplikasi Discord Desktop Dengan Menggunakan Framework Dfrws," Jurnal Teknologi Informasi Dan Komunikasi, vol. 15, no. 1, pp. 98–111, Mar. 2024, doi: 10.51903 /jtikp.v15i1.826.

[7] Farullah Jamaly, H. Muadz Muhammad, I. Dwi Cahyani, B. Fatwa Anbiya, F. Ilmu Tarbiyah dan Keguruan, and U. Walisongo Semarang, "Potensi Discord Sebagai Media Pembelajaran Interaktif Dalam Pendidikan," Jurnal Teknologi Pendidikan JTekpend, vol. 5, no. 1, 2025.

[8] A. Khansa Nayla, E. Wahyu, B. Prasetyo, and B. H. Novaludin, "Pola Komunikasi Masyarakat dalam Sosial Media Discord," 2024.

[9] A. Q. I. Hidayat, E. I. Alwi, and A. W. M. Gaffar, "Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS," Jurnal Minfo Polgan, vol. 13, no. 1, pp. 1138–1146, Aug. 2024, doi: 10.33395 /jmp.v13i1.13966.

[10] T. Ruslan, I. Riadi, and S. Sunardi, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST," Jurnal Fasilkom, vol. 13, no. 02, pp. 286–292, Aug. 2023, doi: 10.37859/jf.v13i02.5540.

[11] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," Jurnal Informatika Universitas Pamulang, vol. 5, no. 1, p. 89, Mar. 2020, doi: 10.32493/informatika.v5i1.4578.

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

[13] R. 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, no. 2, pp. 332–338, Aug. 2024, doi: 10.37859/jf.v14i2.7100.

[14] D. Julian and T. Sutabri, "Jurnal Informatika Terpadu Analisa Kinerja Aplikasi Digital Forensik Autopsy Untuk Pengembalian Data Menggunakan Metode Nist Sp 800-86," Jurnal Informatika Terpadu, vol. 9, no. 2, pp. 136–142, 2023, [Online]. Available: https: //journal.nurulfikri.ac.id/index.php/JIT

[15] P. Aditya, P. Putra, N. K. Sukerti, I. Ketut, and P. Suniantara, "Akusisi Forensik Digital Pada Aplikasi Google Drive Sebagai Bukti Digital Dalam Penyelidikan Kasus Pornografi," Prosiding Spinter, Jun. 2024, Accessed: Jun. 30, 2025. [Online]. Available: https://spinter.stikombali.ac.id/index.php/spinter/article/view/163

[16] M. Pratama Sirait, M. Hatta, and Z. Akli, "Penggunaan Teknologi Forensik Digital Dalam Penegakan Hukum Terhadap Tindak Pidana Pembunuhan Berencana (Analisis Kasus Kopi Sianida Putusan Mahkamah Agung Nomor 498 K/PID/2017)," Jurnal Ilmiah Mahasiswa Fakultas Hukum Universitas Malikussaleh, vol. 8, no. 1, Jan. 2025, doi: 10.29103/jimfh.v8i1.19275.

[17] L. Ode Muhram, "Fungsi Digital Forensik Dalam Pembuktian Tindak Pidana Siber (Studi Kasus di Polda Sultra)," Jurnal Unsultra, vol. 07, no. 1, pp. 3744–3756, Apr. 2025, [Online]. Available: https: //jurnal-unsultra.ac.id/index.php/sulrev

[18] D. Maesyaroh, "Peran Digital Forensik Terhadap Pencurian Data Pribadi Di Sektor Perbankan Digital," Datin Law Jurnal, vol. 5, no. 2, pp. 76–86, Dec. 2024, doi: 10.36355/dlj.v5i2.1698.

[19] Program Studi Informatika, "Tahapan Digital Forensik secara umum," TIF UAD.

[20] I. Riadi, A. Yudhana, and M. Al Barra, "Forensik Mobile pada Layanan Media Sosial LinkedIn," JISKA (Jurnal Informatika Sunan Kalijaga), vol. 6, no. 1, pp. 9–20, Jan. 2021, doi: 10.14421/jiska.2021.61-02.

[21] N. Nurhasanah, F. Z. Nurel Alam, and A. M. Prayoga, "Pencegahan Pornografi Dan Pornoaksi Dihubungkan Dengan Kasus 'Bugil' Di Bandara Yogyakarta Dalam Prespektif Hukum Islam," Jurnal Dialektika Hukum, vol. 5, no. 2, Dec. 2023, doi: 10.36859/jdh.v5i2.867.

[22] A. S. I. Melati, A. Y. Septiani, L. Fitrisusanti, N. Septia, and R. Anggraini, "Literature Review: Peran Orang Tua dalam Mencegah Bahaya Pornografi pada Remaja," Jurnal Ilmu Kesehatan Bhakti Husada: Health Sciences Journal, vol. 14, no. 02, pp. 183–192, Dec. 2023, doi: 10.34305/jikbh.v14i02.798.

[23] S. Lumban Gaol et al., "Studi Kasus Pada Peserta Didik Kecanduan Remaja Menonton Pornografi," Jurnal Pendidikan Sosial dan Humaniora, vol. 2, no. 1, 2023, [Online]. Available: https://publisherqu.com /index.php/pediaqu

[24] M. R. Ridho, M. Muhaimin, and H. S. Harjono, "Pengaruh Aplikasi Discord Dalam Pembelajaran Daring Terhadap Hasil Belajar Pada Matakuliah Komputer," Jurnal Ilmiah Bina Edukasi, vol. 14, no. 1, pp. 22–35, Jun. 2021, doi: 10.33557/jedukasi .v14i1.1367.

[25] M. B. Huda, "Pemanfaatan Discord Sebagai Alternatif Media Pembelajaran Secara Daring," Jurnal Ilmu-ilmu Sosial, vol. 19, no. 2, 2022, Accessed: Jul. 01, 2025.[Online].Available:https://jurnal.stkippgritulungagung.ac.id/index.php/inspirasi/article/view/2697

[26] T. Y. Ardiyansah, R. W. Batubara, and P. K. Auliya, "Using Discord to Facilitate Students in Teaching Learning Process during COVID-19 Outbreak," Journal of English Teaching, Literature, and Applied Linguistics, vol. 5, no. 1, p. 76, Feb. 2021, doi: 10.30587/jetlal.v5i1.2528.

[27] N. A. I. Maniar and T. Yuniati, "Implementasi Mobile Forensic Pada Aplikasi Michat Dan Telegram Dengan Framework Nist 800-101," Cyber Security dan Forensik Digital, vol. 5, no. 2, pp. 60–65, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3764.

[28] C. Mustafa, "Integritas Chain Of Custody Pada Pemeriksaan Bukti Digital," Judex Laguens, vol. 2, no. 1, pp. 75–96, Mar. 2024, doi: 10.25216/ ikahi.2.1.4.2024.75-96.

[29] Aidil Wijaya Kusuma, Erick Irawadi Alwi, and Ramdaniah Ramdaniah, "Analisis Bukti Digital Pada Media Penyimpanan Flash Disk Menggunakan Metode National Institute Of Standards And Technology (NIST)," Cyber Security dan Forensik Digital, vol. 7, no. 1, pp. 18–24, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4345.

[30] D. P. E. Andrian, D. H. Fudholi, and Y. Prayudi, "Karakteristik Metadata Pada Sharing File Di Media Sosial Untuk Mendukung Analisis Bukti Digital," Jurnal Ilmiah SINUS, vol. 19, no. 1, p. 13, Jan. 2021, doi: 10.30646/sinus.v19i1.494.

[31] Bhushan Ghode, Akhlesh Kumar, Khevna Maniar, and Dr. S. K. Jain, "A Forensic Approach on Data Retrieval from IC/eMMC of Damaged Windows Mobile Phone using Easy JTagPlus Box tool and Magnet Forensic Axiom," Int. J. Sci. Res. Sci. Technol., pp. 499–508, Oct. 2021, doi: 10.32628/ IJSRST218568.

[32] S. L. Sanna, L. Regano, D. Maiorca, and G. Giacinto, "Exploring the Robustness of AI-Driven Tools in Digital Forensics: A Preliminary Study," ArXiv, Dec. 2024,[Online].Available:http://arxiv.org/abs/2412.01363

[33] Tyrrz, "Discord Chat Exporter." Accessed: May 19, 2026. [Online]. Available: https://github.com/Tyrrrz/ Discord Chat Exporter