Digital Forensic Mobile Telegram Services in Online Gambling Case using National Institute of Standards and Technology Method

Eko Purwanto
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The study explores the impact of the use of the Telegram Mobile application in the context of online gambling, which contributes to addiction and financial problems. The main goal is to find digital evidence on the victim's smartphone using a method from the National Institute of Standards and Technology (NIST), which involves four stages: Collection, Examination, Analysis, and Report. The Tools used include MOBILedit Forensic Express, Magnet AXIOM, and Hash my Files. The process of collecting and analyzing digital evidence is carried out systematically and thoroughly to ensure data integrity. The results included 5 promotional images and gambling winnings posted on the Telegram group, as well as 4 solicitation messages deleted by the offender. Data Integrity analysis was performed by matching MD5Hash and SHA-256 codes using the My Files Hash. The findings provide strong evidence supporting the investigation and enforcement of illegal online gambling activities.

General Terms

Digital Forensic

Keywords

Digital Forensic, National Institute of Standards and Technology, Online Gambling, Magnet AXIOM, Hash My Files.

1. INTRODUCTION

The development of information and communication technology that is increasingly modern and sophisticated has a significant impact on human life. This technology has become an important part of everyday life, affecting the way humans communicate, work, learn, and socialize, as seen in the Telegram Mobile service application [1]. Telegram Mobile application is a cloud-based instant messaging application that emphasizes security and speed in sending messages. Its main purpose is to facilitate user communication easily and securely through text, audio, video, images and stickers [2]. However, the Telegram Mobile application is also used in some cases of criminal acts, such as fraud, hate speech, gambling and terrorism [3]. The method that will be used in this study is the National Institute of Standards and Technology (NIST) which is a standard in digital forensics that aims to develop guidelines or security standards for the authorities [4]. Digital forensics is a branch of Forensic Science that involves the recovery and investigation of digital devices related to computer crime. Originally synonymous with computer forensics, it now includes all digital data storage devices. Digital forensic investigation supports or rejects hypotheses in electronic discovery for criminal or civil cases in court [5].

2. RELATED WORKS

2.1.1 Previous Study

Salma Azizah, Sri Ayu Ramadhona, dan Kenny Willy Gustitio (2020) in “analysis of Digital evidence on Telegram Messenger using NIST Framework " discusses cases of online shop fraud. The study used NIST (National Institute of Standards and Technology) methods to obtain information from digital evidence through the stages of Collection, Examination, Analysis, and Reporting [3].

Delia Paramita Harahap (2022) in "Digital Forensic implementation of digital wallet and instant messaging applications on Android using NIST methods” examines the search for digital evidence in digital wallet and instant messaging applications using NIST methods as well as oxygen Forensic Detective and MOBILedit Forensic forensic tools for fraud cases [5].

Desti Mualfah dan Rizdqi Akbar Ramadhan (2021) in “digital forensic analysis of CCTV camera footage using NIST methods" discusses the investigation of CCTV footage cases using NIST methods. The process includes case simulation, data collection, data extraction from CCTV media into a format that can be processed by forensic tools, through the stages of Collection, Examination, Analysis, and Reporting [6].

Khairunnisak Nur Isnaini, Hamid Ashari, Adam Prayogo Kuncoro (2020) about "forensic analysis to detect the authenticity of Digital images using NIST methods” this study has a specific purpose to prove the sharpness of forensic tools in revealing the authenticity of a digital evidence to be analyzed by providing a detailed illustration of the role of digital Forensics in revealing the results in accordance with applicable law in Indonesia [7].

Riya Majalista, Tata Sutabri (2023) about "smartphone data retrieval analysis using NIST for Digital Forensic Investigation” this study helps digital forensic investigation by analyzing lost data from smartphones. The smartphone data sought is expected to be evidence of a crime that occurred in cyberspace. The dominant Data used is data stored in the WhatsApp application whether contacts, conversations, images or photos and others. Analysis of the search data in this study using the method of the National Institute of Standards and Technology (NIST) [8].

2.1.2 Digital Forensic

Digital forensics includes the collection, analysis, and presentation of digital evidence from electronic devices such as computers and smartphones for Investigative and judicial purposes [9]. This field aims to prove crimes related to high technology or computers, as well as collect digital evidence to enforce the law against perpetrators of crimes [10].

2.1.3 Mobile Forensic

Mobile forensics is a branch of digital forensics that focuses on the investigation and forensic analysis of mobile devices, such as smartphones, tablets, and other mobile devices. Its purpose is to obtain and analyze digital evidence related to criminal or unlawful activities taking place on such mobile devices. As mentioned earlier, digital forensics itself is a scientific method that studies the maintenance, collection, validation, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources. The focus is on the recovery, analysis and interpretation of digital data for legal purposes [11].

2.1.4 National Institute of Standards and Technology

The NIST method in digital forensics consists of four stages, namely collection, examination, analysis, and reporting [12].

2.1.5 Telegram Mobile

Telegram Mobile is a free and cloud-based multiplatform instant messaging application [13]. The innovative features and ease of use of this application are an attractive factor for many people to join and use Telegram Mobile as a communication platform [14].

2.1.6 Online Gambling

Online gambling is gambling that uses the internet media to make bets, where gamblers must agree to the terms of the game and what is at stake [15]. Gambling activities are considered a crime because they are contrary to social and religious norms in society, gambling through internet media is also included in crimes committed on the internet (Cybercrime) [16].

2.1.7 Digital Evidence

Digital or electronic evidence is evidence information that is stored or transmitted in digital format. This includes data such as text, images, audio, video, and other electronic files [5].

2.1.8 Recovery Data

Data recovery is the process of recovering lost, damaged, or deleted data from storage devices such as hard drives, USB drives, memory cards, and other digital media [8].

2.1.9 Pre-Acquisition

Pre-acquisition is the preparation for finding, identifying, and retrieving evidence in the handling of cases, including planning the equipment, hardware, and computer software used [17].

2.1.10 Core Acquisition

Core acquisition is at the heart of the digital forensics process. After thorough preparation, forensic experts carry out the stages of Collection, Examination, Analysis, and Report [17].

2.1.11 Acquisition

Acquisition is a process related to the management of digital evidence involving storage media such as hard disks, flash disks, CDs, and so forth. The purpose of the acquisition process is to extract and duplicate the evidence found, so that it can be used as an object of analysis [18].

2.1.12 MOBILedit Forensic Express

MOBILedit Forensic Express is a digital forensic software solution specifically designed to retrieve, analyze, and visualize data from various types of mobile devices, including smartphones,tablets, and Global Positioning System (GPS) devices [19].

2.1.13 Magnet AXIOM

Magnet AXIOMis a tool that can display files that have been deleted and formatted. One of the advantages of using magnet Axiom in the forensic process of storage media is its ability to provide audit reports that describe all stages and analysis processes in obtaining and restoring deleted, hidden, and formatted files. With this report, forensic investigators can easily track and reconstruct the activities carried out on the storage media under investigation, ensuring that the evidence found is obtained accurately and legally, by performing recovery on the Magnet Axiom software. [20].

2.1.14 Hash My Files

Hash My Files is a tool to compare the results of file extraction with the original file. The similarity of the hash value indicates the authenticity of the evidence without modification [21].

3. METHODOLOGY

This methodology serves as a guide for researchers in studying and understanding in depth every stage necessary to research goals, as well as responding to emerging challenges in an effective and efficient way. Structured methodology ensures the accuracy and reliability of digital forensic research results, thereby making significant contributions in the field of cyber security and law enforcement.

3.1 Object of Research

The object of the study is a digital forensic analysis of online gambling cases that occur in the Telegram mobile application. The study is carried out because of the increasing number of online gaming cases on social media platforms, including the Telegram app. The aim of the research is to analyze the evidence of online Gambling cases in Telegram. In the forensic process, the National Institute of Standards and Technology uses the software MOBILedit Forensic Express, Magnet AXIOM, and Hash My Files.

3.2 Research Materials and Tools

In this study, used hardware and software to support the research process. For easy reference and guidance, a detailed and complete information table will be provided. Information on materials and tools used from hardware and software is shown in Table 1 and Table 2. Here are the materials and tools used in this study :

Table 1. Tools and Software materials used in this study

Software	Specifications
MOBILedit forensic express	MOBILedit forensic express Pro 7.4.1.21057
Magnet AXIOM	For Windows 64-bit version
Hash My Files	For Windows 64-bit version
Operation System	Windows 11
Telegram	Mobile Telegram version 8.6.1

Table 2. Hardware tools and materials used in this study

Hardware	Specifications
Laptop	Laptop ASUS ROG Strix G513IH AMD Ryzen™ 7 4800H CPU @ 8M Cache, up to 4.2 GHz, Memory 8GB
Mobile Phone	Samsung Galaxy J2 Internal 8GB, Ram 1GB

3.3 Research Phase

Each process in the NIST method is carefully integrated to support the primary goal of research, namely achieving accurate and reliable results. Implementation of this method also includes data validation as well as process verification, to ensure consistency and reliability of the results. In addition, continuous evaluation is carried out at every stage to detect and address potential errors from an early stage.

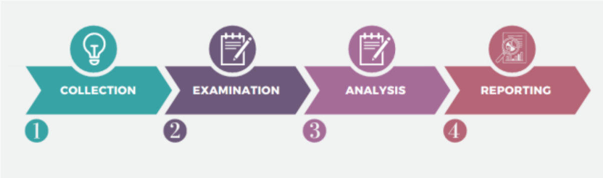


Figure 1: Schematic method of the National Institute of Standards and Technology

Figure 1 show a general scheme of the NIST method that includes several stages: Collection, Examination, Analysis, and Report as the final stage. Details of these stages are as follows:

3.3.1 Collection

Collection is the process of collecting data from various sources that are relevant to the purpose of research. At this stage, it is important to maintain the integrity of such data so that the data collected remains original and does not undergo unauthorized changes [22].

3.3.2 Examination

Examining is the stage where the files that have been collected from the previous stage will be tested to obtain the desired information from the data. The analysis process will be carried out using a variety of digital forensic techniques and tools aimed at revealing hidden digital traces, identifying potential evidence, and deciphering the contents of significant files [23].

3.3.3 Analysis

The analysis stage is the stage where the relevant evidence or data that has been collected and analyzed will be examined in detail to obtain evidence related to the case under investigation [24].

3.3.4 Reporting

Reporting is a stage where the preparation of an analysis report includes an explanation of the actions taken and the identification of data used as evidence related to the Telegram mobile online gambling case [25].

3.4 Research Simulation Scenario

This research diskenariokan a case of online gambling on the mobile application telegram, where gambling admins put the victims into the online gambling group in telegram, which is unnoticed by the user, then the admin invites to join the online gambling site and promises a big win to the victim.

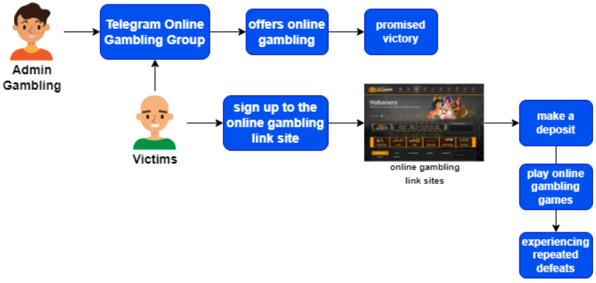

Admin Gambling
Telegram Online Gambling Group
offers online gambling
promised victory
Victims
sign up to the online gambling link site
online gambling link sites
make a deposit
play online gambling games
experiencing repeated defeats

Figure 2: Case Simulation Illustration

Figure 2 show illustrations of scenario or simulation that have been described in previous study. This illustration covers the stages and overall flow of the study, which consists of three main stages: pre-incident, incident, and post-incident. The details of the simulation illustration of the case are as follows:

3.4.1 Pre Incident

This case scenario begins when the admin begins to enter the victims into the online gambling group without the user realizing it, then the admin in the online gambling group offers an online gambling site that promises victory to every user. Then the victim feels curious and finally tries the online gambling. Then the victims began to enter the online gambling site link provided by the admin in the telegram group and the victim began depositing his money into the online gambling site. The victim began to play online gambling games provided by the website and unwittingly the victim felt defeated repeatedly and never won, while at first the admin had promised victory to the victim in the telegram group.

3.4.2 Incidents

In this case, telegram users who find a group containing online gambling in it and then persuade to do the gambling and promise victory can be reported to the relevant authorities evidence in this case. After that, the collection of digital physical evidence related to this case is carried out, as well as comparing it with the provisions contained in the law on information and Electronic Transactions of the ITE Law. The evidence collected will be used as evidence in this case. The evidence will be thoroughly analyzed, and then it will proceed to the next stage, where the entire evidence that has been obtained will be displayed.

3.4.3 Post-Incident

Post-incident is the stage where the digital evidence that has been obtained will be processed and processed using the MOBILedit Forensic Express and Magnet AXIOM applications. This application has the ability to collect important data directly related to the digital evidence being sought, including messages related to online gambling activities on the mobile-based telegram application. By using this application, it is expected to be able to identify and collect relevant information for this case related to the online gambling activities carried out. Then, after the data has been processed and collected, the next step is to enter the stage of evidence analysis findings. This analysis will be done using Hash My Files Software. Using this application, the evidence that has been found will be processed and analyzed further to identify relevant information and provide a deeper understanding of the case.

3.5 Research Process Flow

The research process flow includes stages in a digital forensic investigation known as forensic imaging. Based on the research process, at the data collection stage, an illustration of the core acquisition is made, where all files that have gone through the research process will be collected in full.

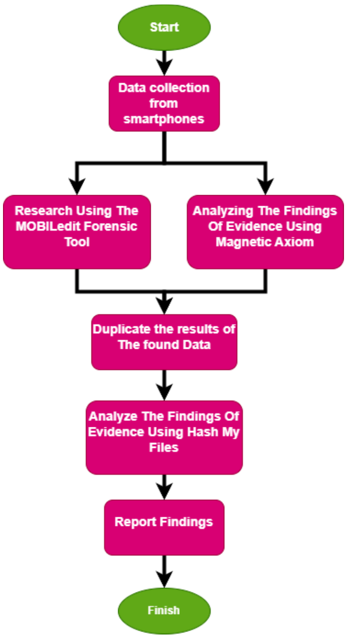

Start
Data collection from smartphones
Research Using The MOBILedit Forensic Tool
Analyzing The Findings Of Evidence Using Magnetic Axiom
Duplicate the results of The found Data
Analyze The Findings Of Evidence Using Hash My Files
Report Findings
Finish

Figure 3: Core Acquisition Step Scheme

Figure 3 show the phase of the research process starting with collecting all the data from a smartphone, then conducting an examination using MOBILedit Forensic Express and Magnet AXIOM, after the data is found, the analyst will dialakukan using Hash my Files and then reporting.

4. RESULTS AND DISCUSSION

This study discusses the research process to obtain results from digital forensics using the National Institute of Standards and Technology (NIST) method, which describes four stages in the research: Collection, Examination, Analysis, and Report. The object of this study is the mobile application Telegram.

4.1 Data Collection

The study used questionnaires to collect data from Telegram users who without their knowledge were put into Online gambling groups. Data from about 14 respondents showed that they were once included in a group that invites to gamble with the lure of a big win. In addition to questionnaires, researchers also use structured surveys to facilitate data analysis and identify trends related to online gambling.

4.2 Implementation

The test results were carried out using the methods of the National Institute of Standards and Technology (NIST), which suggest several stages in the forensic process: Collection, Examination, Analysis, and Reporting. The Collection stage involves retrieving data from relevant sources and maintaining the integrity of the evidence. The Examination stage includes a forensic examination to verify the authenticity of the data collected. The Analysis phase (research) involves a detailed analysis to prove the validity of the data technically and legally. The last stage, Reporting, is carried out after the examination and analysis process is completed, where the results are used as digital evidence that can be scientifically and legally accountable.

4.2.1 Collection

This stage is carried out data collection is carried out through a rooted mobile phone, providing full access to the system and security of the device. This rooting process is important to access and extract hidden or protected data on the phone.

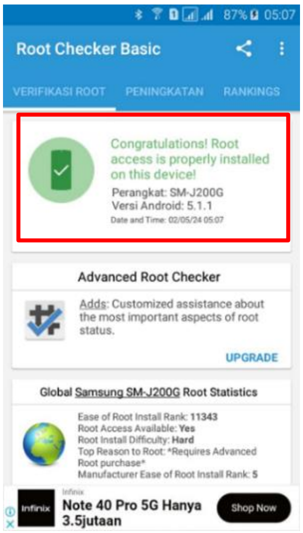
Figure 4: Mobile Phone Samsung Galaxy J2

Figure 4 show the detailed specifications of the Samsung Galaxy J2 smartphone used as evidence, it is important to ensure a smooth process. Table 3. displaying the detailed specifications of the Samsung Galaxy J2 smartphone used as evidence, it is important to ensure a smooth process.

Table 3. Specification of Smartphone Evidence

Specification Type	Proof Specifications
Brand	Samsung
Series	Galaxy J2
IMEI	354921074384396
Operating System	Android
Operating System Version	5.1.1

The data collection process begins by rooting the smartphone using the Root Checker application to facilitate access to data stored in Android devices. Once the rooting process is complete, the phone can download the TWRP and Magisk Manager apps via Google Chrome.



Congratulations! Root access is properly installed on this device!
Perangkat: SM-J200G
Versi Android: 5.1.1
Date and Time: 02/05/24 05:07

Advanced Root Checker

Adds: Customized assistance about the most important aspects of root status.

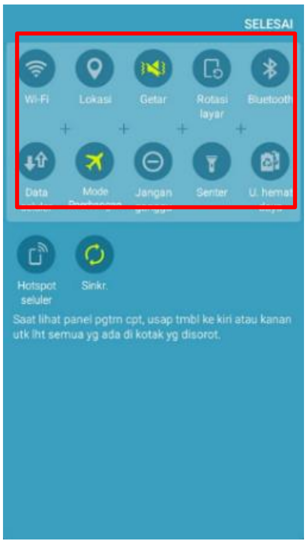
Global Samsung SM-J200G Root Statistics

Ease of Root Install Rank: **11343**
Root Access Available: **Yes**
Root Install Difficulty: **Hard**
Top Reason to Root: *Requires Advanced Root purchase*
Manufacturer Ease of Root Install Rank: **5**

Infinix
Note 40 Pro 5G Hanya 3.5jutaan

Figure 5: The Process of Rooting A Samsung Android Smartphone

Figure 5 show a rooted android phone allow the user to have greater access into the system. In general, on Non-Rooted Android phones, some features have been disabled to prevent users from damaging the operating system.



Saat lihat panel pgtm cpt, usap tmbl ke kiri atau kanan utk lht semua yg ada di kotak yg disorot.

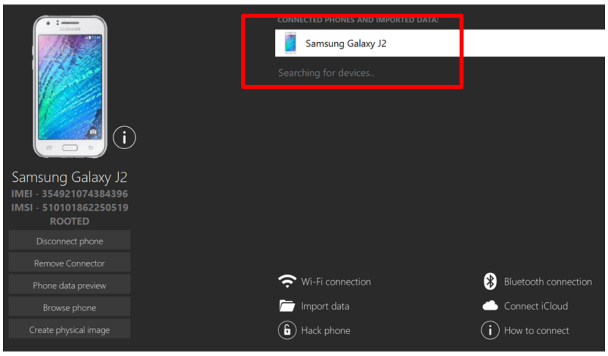
Figure 6 : Insulation Techniques on Smartphone

Figure 6 show the isolation techniques used on a smartphone includes an important step in switching the device to airplane mode. This step requires a series of coordinated steps in which the device disconnects all wireless connections, including Wi-Fi, mobile data, and Bluetooth, thus creating an isolated environment from external networks. When collecting evidence, it is likely that the data and evidence that has been deleted will be restored using forensic Tools that have been connected via a USB cable for debugging to a laptop and collecting evidence that has been deleted using MOBILedit Forensic Exoress software, Magnet AXIOM and then analyzed using Hash My Files.

A. MOBILedit Forensic Express

The first forensic tool used in this phase is MOBILedit Forensic

Express, which allows creating backups or system backups. MOBILedit Forensic Express supports a variety of image formats that can be used with a variety of forensic tools. The process of collecting data using MOBILedit Forensic Express is done by connecting evidence to a laptop that has been installed MOBILedit Forensic Express. After that, further forensic analysis can be carried out to obtain more detailed information of the investigated device.

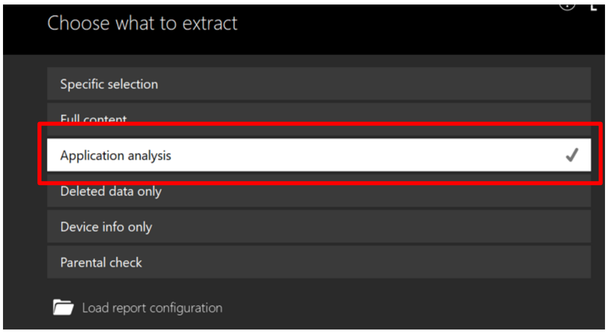


Samsung Galaxy J2
IMEI - 354921074384396
IMSI - 510101862250519
ROOTED

CONNECTED PHONES AND IMPORTED DATA:
Samsung Galaxy J2
Searching for devices..

Figure 7: Smartphone Connected to MOBILedit

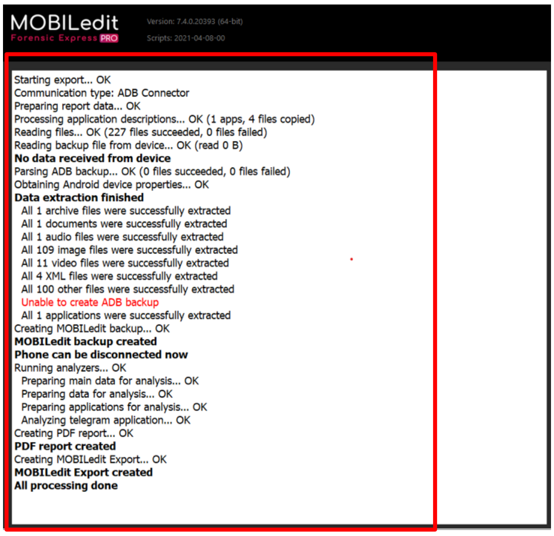
Figure 7 show the process of connecting a Samsung Galaxy J2 phone to the MOBILedit Forensic Express application. This connection enables direct access to the cell phone data, facilitating the collection of more detailed forensic evidence.



Choose what to extract

Figure 8: Select What to extract page

Figure 8 show the smartphone that has been connected to MOBILedit Forensic Express. After clicking Next, the user is redirected to the Choose Time to Extract page. In the following step, select “Application Analysis”.

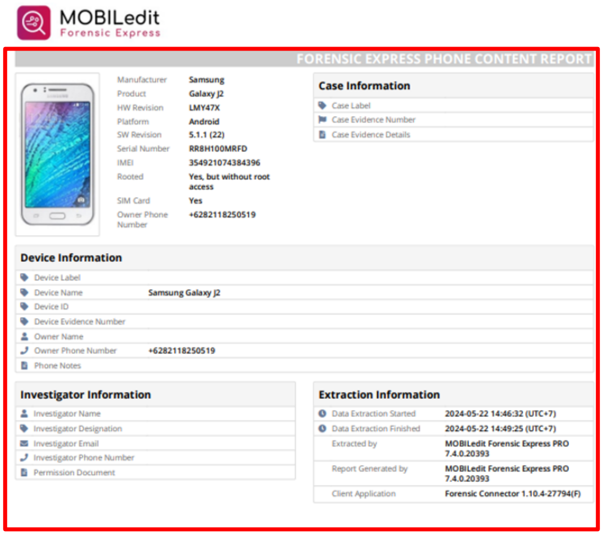


Version: 7.4.0.20393 (64-bit)
Scripts: 2021-04-08-00

```
Starting export... OK
Communication type: ADB Connector
Preparing report data... OK
Processing application descriptions... OK (1 apps, 4 files copied)
Reading files... OK (227 files succeeded, 0 files failed)
Reading backup file from device... OK (read 0 B)
No data received from device
Parsing ADB backup... OK (0 files succeeded, 0 files failed)
Obtaining Android device properties... OK
Data extraction finished
  All 1 archive files were successfully extracted
  All 1 documents were successfully extracted
  All 1 audio files were successfully extracted
  All 109 image files were successfully extracted
  All 11 video files were successfully extracted
  All 4 XML files were successfully extracted
  All 100 other files were successfully extracted
  Unable to create ADB backup
  All 1 applications were successfully extracted
Creating MOBILedit backup... OK
MOBILedit backup created
Phone can be disconnected now
Running analyzers... OK
  Preparing main data for analysis... OK
  Preparing data for analysis... OK
  Preparing applications for analysis... OK
  Analyzing telegram application... OK
Creating PDF report... OK
PDF report created
Creating MOBILedit Export... OK
MOBILedit Export created
All processing done
```

Figure 9: Complete Extraction View

Figure 9 show the procedure following the selection of the file storage location. To begin the data extraction, click on "Export." During this operation, the messages "Please wait or press Connect more" and "Extraction complete" signify that the extraction is underway and has finished successfully, respectively.



FORENSIC EXPRESS PHONE CONTENT REPORT

Manufacturer	Samsung
Product	Galaxy J2
HW Revision	LMY47X
Platform	Android
SW Revision	5.1.1 (22)
Serial Number	RR8H100MRFD
IMEI	354921074384396
Rooted	Yes, but without root access
SIM Card	Yes
Owner Phone Number	+6282118250519

Case Information

Case Label	
Case Evidence Number	
Case Evidence Details	

Device Information

Device Label	
Device Name	Samsung Galaxy J2
Device ID	
Device Evidence Number	
Owner Name	
Owner Phone Number	+6282118250519
Phone Notes	

Investigator Information

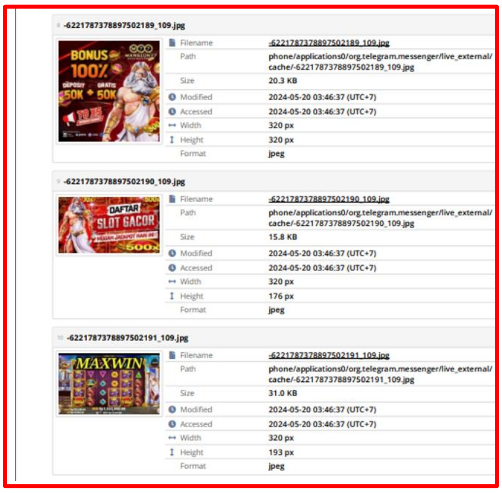
Investigator Name	
Investigator Designation	
Investigator Email	
Investigator Phone Number	
Permission Document	

Extraction Information

Data Extraction Started	2024-05-22 14:46:32 (UTC+7)
Data Extraction Finished	2024-05-22 14:49:25 (UTC+7)
Extracted by	MOBILedit Forensic Express PRO 7.4.0.20393
Report Generated by	MOBILedit Forensic Express PRO 7.4.0.20393
Client Application	Forensic Connector 1.10.4-27794(F)

Figure 10: Display of The Results Of The Main Report Images

Figure 10 show the report file on the main page, encompassing details like phone specifications, incident information, device data, investigator details, extraction data, and associated packages. Moreover, the report includes image data, providing information such as file name, location, size, modification date, access date, width, height, and format.



-6221787378897502189_109.jpg

Filename	-6221787378897502189_109.jpg
Path	phone/applications0/org.telegram.messenger/live_external/cache/-6221787378897502189_109.jpg
Size	20.3 KB
Modified	2024-05-20 03:46:37 (UTC+7)
Accessed	2024-05-20 03:46:37 (UTC+7)
Width	320 px
Height	320 px
Format	jpeg

-6221787378897502190_109.jpg

Filename	-6221787378897502190_109.jpg
Path	phone/applications0/org.telegram.messenger/live_external/cache/-6221787378897502190_109.jpg
Size	15.8 KB
Modified	2024-05-20 03:46:37 (UTC+7)
Accessed	2024-05-20 03:46:37 (UTC+7)
Width	320 px
Height	176 px
Format	jpeg

-6221787378897502191_109.jpg

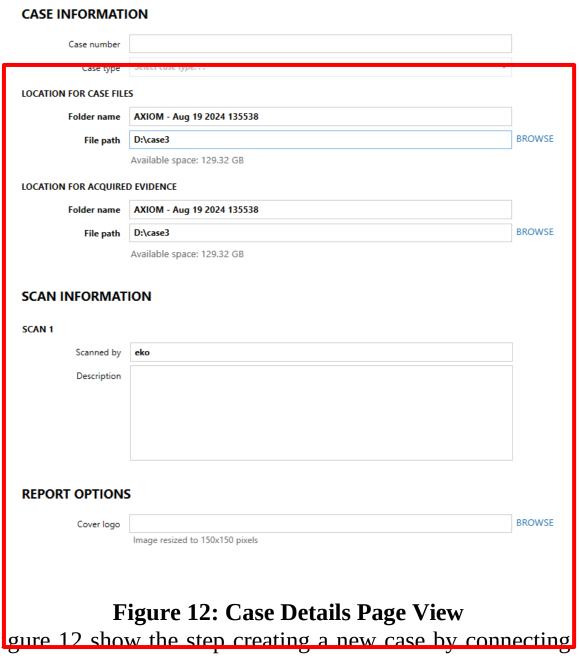
Filename	-6221787378897502191_109.jpg
Path	phone/applications0/org.telegram.messenger/live_external/cache/-6221787378897502191_109.jpg
Size	31.0 KB
Modified	2024-05-20 03:46:37 (UTC+7)
Accessed	2024-05-20 03:46:37 (UTC+7)
Width	320 px
Height	193 px
Format	jpeg

Figure 11: Display of Online Gambling Promotion Images Result

Figure 11 show the case of online gambling promotion of gambling link sites and winnings explained through a description of its structure and characteristics. The report includes important items such as File Names, which include paths and sizes. In addition, the report also records the modification date, access, width, and height of the image, with additional formatting support.

B. Magnet AXIOM

Magnet AXIOM because live extraction and extraction using physical images are possible, extraction is carried out in the direct extraction phase in this study. Magnet AXIOM is able to find evidence not found in other forensic applications, perform data validation, and integrate images captured by other tools into a single reporting document for the investigative process.



CASE INFORMATION

Case number

Case type Select case type...

LOCATION FOR CASE FILES

Folder name: AXIOM - Aug 19 2024 135538

File path: D:\case3 BROWSE

Available space: 129.32 GB

LOCATION FOR ACQUIRED EVIDENCE

Folder name: AXIOM - Aug 19 2024 135538

File path: D:\case3 BROWSE

Available space: 129.32 GB

SCAN INFORMATION

SCAN 1

Scanned by: eko

Description

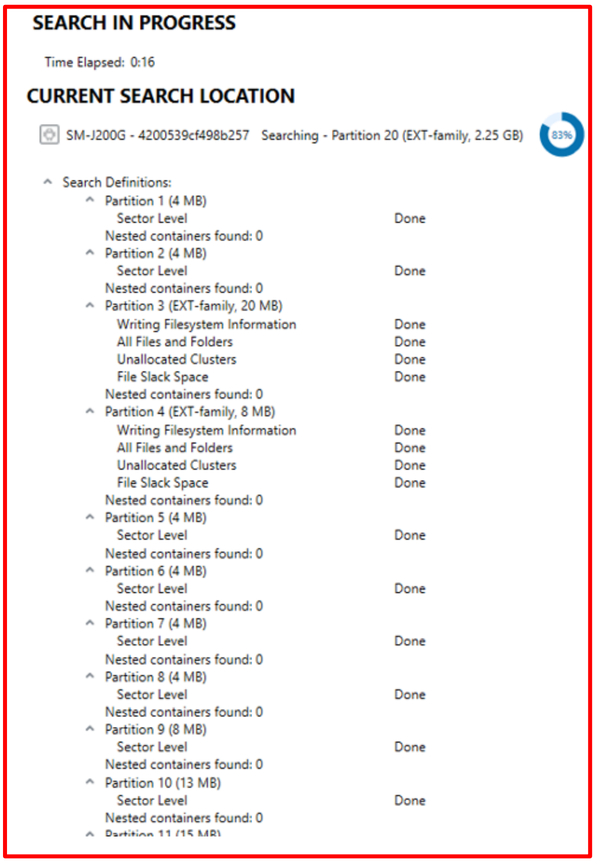
REPORT OPTIONS

Cover logo BROWSE

Image resized to 150x150 pixels

Figure 12: Case Details Page View

Figure 12 show the step creating a new case by connecting a smartphone to a laptop via a USB cable. This is the initial step for case creation on the case details page. In the case Information section, there is a case number that you want to create, and the type of case you want to investigate by entering the name of the folder for storing the case.

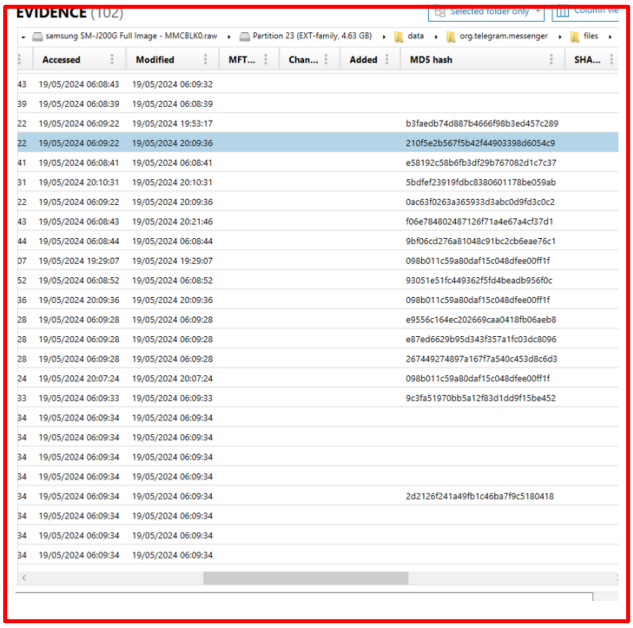


```
SEARCH IN PROGRESS
  Time Elapsed: 0:16
CURRENT SEARCH LOCATION
  SM-J200G - 4200539cf498b257   Searching - Partition 20 (EXT-family, 2.25 GB)   83%

  ^ Search Definitions:
      ^ Partition 1 (4 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 2 (4 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 3 (EXT-family, 20 MB)
          Writing Filesystem Information            Done
          All Files and Folders                     Done
          Unallocated Clusters                      Done
          File Slack Space                          Done
        Nested containers found: 0
      ^ Partition 4 (EXT-family, 8 MB)
          Writing Filesystem Information            Done
          All Files and Folders                     Done
          Unallocated Clusters                      Done
          File Slack Space                          Done
        Nested containers found: 0
      ^ Partition 5 (4 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 6 (4 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 7 (4 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 8 (4 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 9 (8 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 10 (13 MB)
          Sector Level                              Done
        Nested containers found: 0
      ^ Partition 11 (15 MB)
```

Figure 13: Extraction Process on a Smartphone

Figure 13 show the evidence extraction process that takes time varies depending on the type and amount of data on the cell phone being examined.



EVIDENCE (102)

samsung SM-J200G Full Image - MMCBLK0.raw ▸ Partition 23 (EXT-family, 4.63 GB) ▸ data ▸ org.telegram.messenger ▸ files ▸

	Accessed	Modified	MFT...	Chan...	Added	MD5 hash	SHA...
43	19/05/2024 06:08:43	19/05/2024 06:09:32					
39	19/05/2024 06:08:39	19/05/2024 06:08:39					
22	19/05/2024 06:09:22	19/05/2024 19:53:17				b3faedb74d887b4666f98b3ed457c289	
22	19/05/2024 06:09:22	19/05/2024 20:09:36				210f5e2b567f5b42f44903398d6054c9	
41	19/05/2024 06:08:41	19/05/2024 06:08:41				e58192c58b6fb3df29b767082d1c7c37	
31	19/05/2024 20:10:31	19/05/2024 20:10:31				5bdfef23919fdbc8380601178be059ab	
22	19/05/2024 06:09:22	19/05/2024 20:09:36				0ac63f0263a365933d3abc0d9fd3c0c2	
43	19/05/2024 06:08:43	19/05/2024 20:21:46				f06e784802487126f71a4e67a4cf37d1	
44	19/05/2024 06:08:44	19/05/2024 06:08:44				9bf06cd276a81048c91bc2cb6eae76c1	
07	19/05/2024 19:29:07	19/05/2024 19:29:07				098b011c59a80daf15c048dfee00ff1f	
52	19/05/2024 06:08:52	19/05/2024 06:08:52				93051e51fc449362f5fd4beadb956f0c	
36	19/05/2024 20:09:36	19/05/2024 20:09:36				098b011c59a80daf15c048dfee00ff1f	
28	19/05/2024 06:09:28	19/05/2024 06:09:28				e9556c164ec202669caa0418fb06aeb8	
28	19/05/2024 06:09:28	19/05/2024 06:09:28				e87ed6629b95d343f357a1fc03dc8096	
28	19/05/2024 06:09:28	19/05/2024 06:09:28				267449274897a167f7a540c453d8c6d3	
24	19/05/2024 20:07:24	19/05/2024 20:07:24				098b011c59a80daf15c048dfee00ff1f	
33	19/05/2024 06:09:33	19/05/2024 06:09:33				9c3fa51970bb5a12f83d1dd9f15be452	
34	19/05/2024 06:09:34	19/05/2024 06:09:34					
34	19/05/2024 06:09:34	19/05/2024 06:09:34					
34	19/05/2024 06:09:34	19/05/2024 06:09:34					
34	19/05/2024 06:09:34	19/05/2024 06:09:34					
34	19/05/2024 06:09:34	19/05/2024 06:09:34				2d2126f241a49fb1c46ba7f9c5180418	
34	19/05/2024 06:09:34	19/05/2024 06:09:34					
34	19/05/2024 06:09:34	19/05/2024 06:09:34					
34	19/05/2024 06:09:34	19/05/2024 06:09:34					

Figure 14: Display of Extraction Results on Magnet AXIOM

Figure 14 show the result of a call to action that has been deleted by the admin of the online gambling group in the form of an invitation to play on online gambling sites promoted by actors and also online gambling promotion images. In the case report above has items in the form of filename, Formatfile, Sizefile and MD5 Hash as supporting evidence which will then be analyzed to obtain relevant data in this research case.

C. Hash My Files

A third forensic tool, Hash My Files, is used for analysis and calculating MD5 as well as SHA-256 hashes on one or more files.

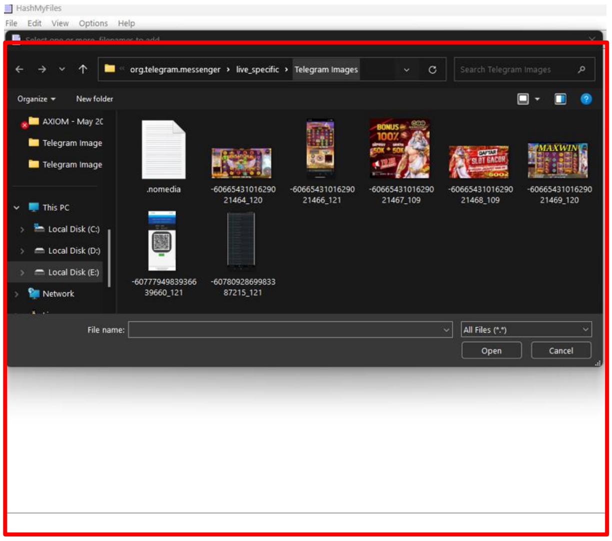
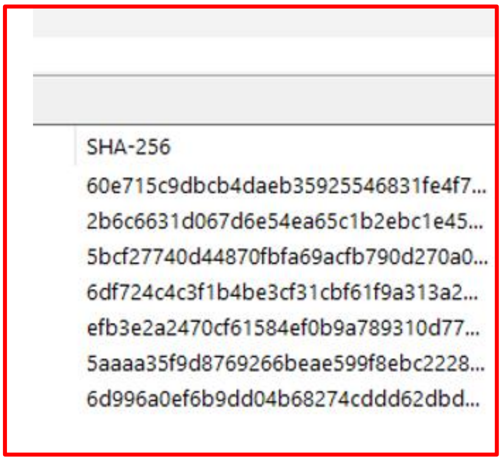


Figure 15 : Add Files Page View

Figure 15 show the stage of selecting location of the data storage folder that has previously been extracted using MOBILedit Forensic Express, the type of evidence type that will be analyzed, namely in the form of photos or images.



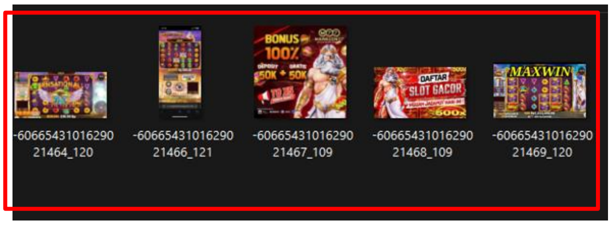
SHA-256
60e715c9dbcb4daeb35925546831fe4f7...
2b6c6631d067d6e54ea65c1b2ebc1e45...
5bcf27740d44870fbfa69acfb790d270a0...
6df724c4c3f1b4be3cf31cbf61f9a313a2...
efb3e2a2470cf61584ef0b9a789310d77...
5aaaa35f9d8769266beae599f8ebc2228...
6d996a0ef6b9dd04b68274cddd62dbd...

Figure 16: Data Result View in Hash My Files

Figure 16 show the result above action is the process of analyzing using the Hash My Files application by exporting image data then getting results form hash and SHA-256 values.

4.2.2 *Examination*

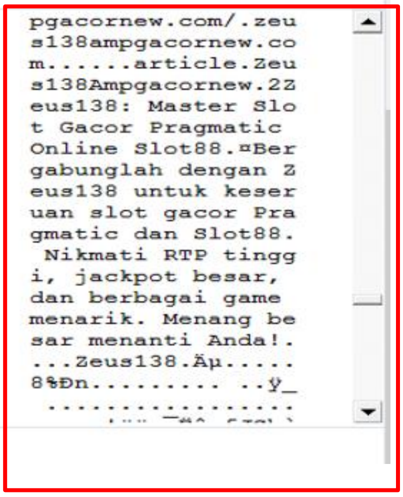
At this stage, the data obtained from the previous step is examined using three forensic tools: MOBILedit Forensic Express, Magnet AXIOM, and Hash My Files.



-6066543101629021464_120 -6066543101629021466_121 -6066543101629021467_109 -6066543101629021468_109 -6066543101629021469_120

Figure 17: Display of Figure Data Storage Location

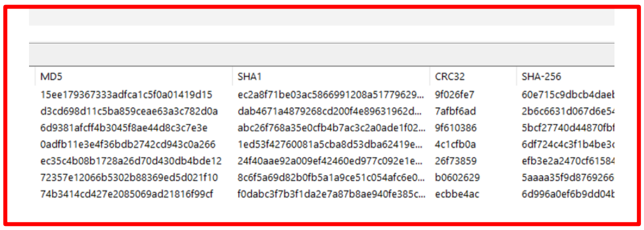
Figure 17 show the result of the first data check using MOBILedit Forensic Express, where the data was found on Local Disk E in the Samsung Galaxy J2 folder. This Folder contains various files, including promotional images of online gambling sites and online gambling winnings. These data have been verified and match the information submitted by the perpetrator. This examination confirmed that the files are relevant digital evidence in the investigation of online gambling cases.



```
pgacornew.com/.zeu
s138ampgacornew.co
m......article.Zeu
s138Ampgacornew.2Z
eus138: Master Slo
t Gacor Pragmatic
Online Slot88.¤Ber
gabunglah dengan Z
eus138 untuk keser
uan slot gacor Pra
gmatic dan Slot88.
 Nikmati RTP tingg
i, jackpot besar,
dan berbagai game
menarik. Menang be
sar menanti Anda!.
...Zeus138.Äµ.....
8%Đn......... ..ÿ_
 ..................
```

Figure 18: Display of Message Results in the Magnet AXIOM Application

Figure 18 show the result of the second check using the Axiom Magnet tools the data that has been checked and found on the Local Disk location D with the name fold case3\AXIOM-May 23 2024 025030 then select case and will enter Axiom Examine.



MD5	SHA1	CRC32	SHA-256
15ee179367333adfca1c5f0a01419d15	ec2a8f71be03ac5866991208a51779629...	9f026fe7	60e715c9dbcb4daet
d3cd698d11c5ba859ceae63a3c782d0a	dab4671a4879268cd200f4e89631962d...	7afbf6ad	2b6c6631d067d6e5
6d9381afcff4b3045f8ae44d8c3c7e3e	abc26f768a35e0cfb4b7ac3c2a0ade1f02...	9f610386	5bcf27740d44870fbf
0adfb11e3e4f36bdb2742cd943c0a266	1ed53f42760081a5cba8d53dba62419e...	4c1cfb0a	6df724c4c3f1b4be3
ec35c4b08b1728a26d70d430db4bde12	24f40aae92a009ef42460ed977c092e1e...	26f73859	efb3e2a2470cf6158
72357e12066b5302b88369ed5d021f10	8c6f5a69d82b0fb5a1a9ce51c054afc6e0...	b0602629	5aaaa35f9d8769266
74b3414cd427e2085069ad21816f99cf	f0dabc3f7b3f1da2e7a87b8ae940fe385c...	ecbbe4ac	6d996a0ef6b9dd04

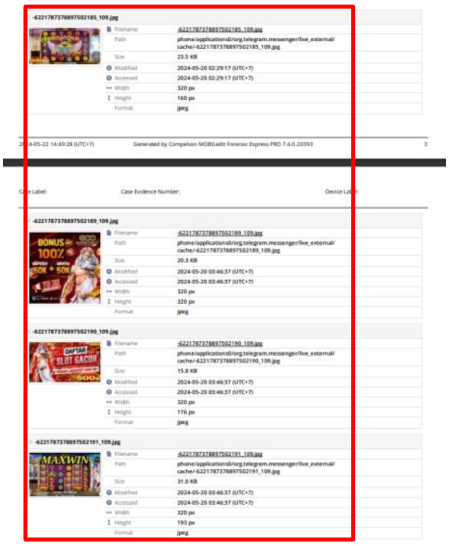
Figure 19: Import Result on My File Hash

Figure 19 show the result of checking the data using the My Files Hash tool using the image file obtained using the MOBILedit Forensic Express application to obtain MD5 hash, SHA1, CRC32, SHA-512 and SHA-384, file name, file size of the image in the form of promotions and online gambling winnings by the online gambling admin group, the MD5 Hash code and SHA-256.

4.2.3 *Analysis (Analisis)*

A. Analysis Using MOBILedit Forensic Express

Analysis using MOBILedit Forensic Express involves identifying data that has been deleted in the PDF report.



-6221787378897502185_109.jpg

Filename	-6221787378897502185_109.jpg
Path	phone/applications0/org.telegram.messenger/live_external/cache/-6221787378897502185_109.jpg
Size	23.5 KB
Modified	2024-05-20 02:29:17 (UTC+7)
Accessed	2024-05-20 02:29:17 (UTC+7)
Width	320 px
Height	160 px
Format	jpeg

2 4-05-22 14:49:28 (UTC+7) Generated by Compelson MOBILedit Forensic Express PRO 7.4.0.20393 3

C e Label: Case Evidence Number: Device La l:

-6221787378897502189_109.jpg

Filename	-6221787378897502189_109.jpg
Path	phone/applications0/org.telegram.messenger/live_external/cache/-6221787378897502189_109.jpg
Size	20.3 KB
Modified	2024-05-20 03:46:37 (UTC+7)
Accessed	2024-05-20 03:46:37 (UTC+7)
Width	320 px
Height	320 px
Format	jpeg

-6221787378897502190_109.jpg

Filename	-6221787378897502190_109.jpg
Path	phone/applications0/org.telegram.messenger/live_external/cache/-6221787378897502190_109.jpg
Size	15.8 KB
Modified	2024-05-20 03:46:37 (UTC+7)
Accessed	2024-05-20 03:46:37 (UTC+7)
Width	320 px
Height	176 px
Format	jpeg

-6221787378897502191_109.jpg

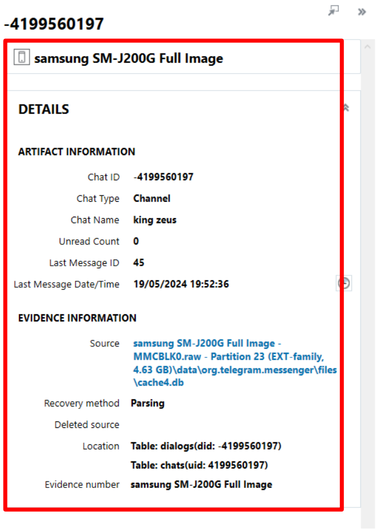
Filename	-6221787378897502191_109.jpg
Path	phone/applications0/org.telegram.messenger/live_external/cache/-6221787378897502191_109.jpg
Size	31.0 KB
Modified	2024-05-20 03:46:37 (UTC+7)
Accessed	2024-05-20 03:46:37 (UTC+7)
Width	320 px
Height	193 px
Format	jpeg

Figure 20: Digital Evidence Images MOBILedit Forensic Express

Figure 20 show the results of analyzing images containing online gambling content, including site promotions and screenshots of winnings that have been deleted by the perpetrators.

A. Analysis Using Magnet AXIOM

The analysis using Magnet AXIOM started from the extraction results during the data collection process, where information such as account names, contacts, and messages were found.



-4199560197

samsung SM-J200G Full Image

DETAILS

ARTIFACT INFORMATION

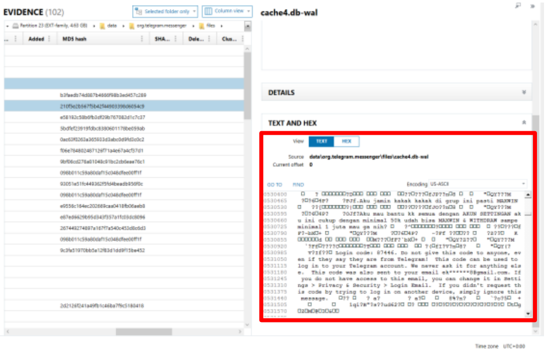
Chat ID	-4199560197
Chat Type	Channel
Chat Name	king zeus
Unread Count	0
Last Message ID	45
Last Message Date/Time	19/05/2024 19:52:36

EVIDENCE INFORMATION

Source	samsung SM-J200G Full Image - MMCBLK0.raw - Partition 23 (EXT-family, 4.63 GB)\data\org.telegram.messenger\files \cache4.db
Recovery method	Parsing
Deleted source	
Location	Table: dialogs(did: -4199560197) Table: chats(uid: 4199560197)
Evidence number	samsung SM-J200G Full Image

Figure 21: Digital Evidence of Online Gambling Group Name

Figure 21 show important findings related to this case, including the identification of a Telegram group called "King Zeus" and ID unique -4199560197.



Source data\org.telegram.messenger\files\cache4.db-wal
Current offset 0

```
?PJf.Aku jamin kakak kakak di grup ini pasti MAXWIN
?OJf?Aku mau bantu kk semua dengan AKUN SETTINGAN ak
u ini cukup dengan minimal 50k udah bisa MAXWIN & WITHDRAW sampe
minimal 1 juta mau ga nih?
Login code: 87446. Do not give this code to anyone, ev
en if they say they are from Telegram! This code can be used to
log in to your Telegram account. We never ask it for anything els
e. This code was also sent to your email ek******8@gmail.com. If
you do not have access to this email, you can change it in Setti
ngs > Privacy & Security > Login Email. If you didn't request th
is code by trying to log in on another device, simply ignore this
message.
```

Figure 22: Chat Results Deleted by the Perpetrator

Figure 22 show an important aspect of the investigation, where a series of messages deleted by the perpetrator were revealed.

B. Analysis Using Hash My Files

From the results of the examination data carried out on the MOBILedit Forensic Express application in the form of images.

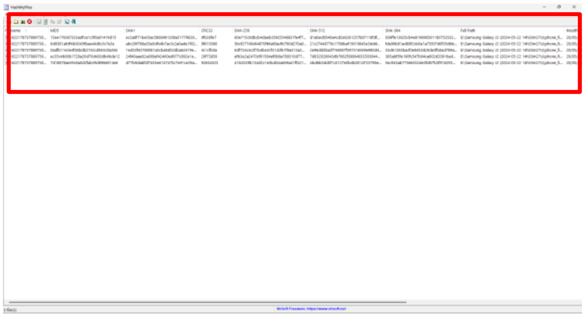


Figure 23: Hash My Files with MD5 and SHA-256 codes

Figure 23 show the result has been obtained from the MOBILedit Forensic Express application which is then processed in the Hash My Files application.

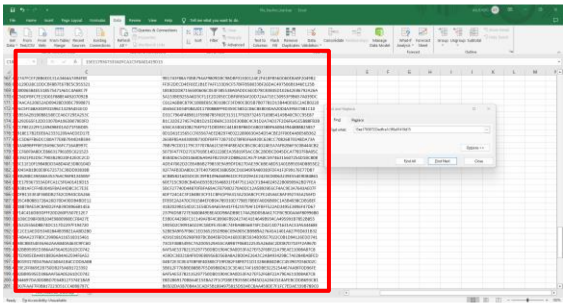


Figure 24: Display of MD5 and SHA-256 code matching results in file_hashes_backup

Figure 24 show the data presentation matches the MD5 and SHA-256 Hash codes obtained from the Hash My Files application with the extracted Excel folder using MOBILedit Forensic Express, called file_hashes_backup. This process involves copying the MD5 and SHA-256 codes from Hash My Files, and then inserting them into file_hashes_backup which includes the file path, file path, MD5, and SHA-256.

C. Online Gambling Case Analysis

The method of analyzing online gambling in Telegram applications involves selecting the fields necessary to identify online gambling activities, allowing for preprocessing to recognize gambling activities in the group. The identification process is based on simulated data from admins and victims communicating in Telegram groups, with examples documented in Table 4.

Tabel 4. Example of Conversation in an Online Gambling Group

Victim	Perpetrator
Wow how do you do it?	I want to help all of you with my SETTING ACCOUNT, just with a minimum of 50k you can MAXWIN & WITHDRAW up to 1 million, don't you want it?
May I join you?	You can do this by entering our link, we guarantee that you will MAXWIN
alright	Okay, I'll help you right away, before you have to register first, how to fill in: Username: Phone Number: Account Number: Bank/E-Wallet Name:
Okay, I'll help you right away, before you have to register first, how to fill in: Username: japirkur18 Phone Number: 087729527322 Account Number: 6558923445 Bank/E-Wallet Name: Japir Kurniawan	Okay, I'll list it right away.
How come instead of winning I lost a lot	-
What a cheater	-

4.2.4 Report

The results of the evidence obtained in the Telegram online gambling group are in the form of promotional images and online gambling winnings, then a message in the form of an invitation to join to play on the online gambling site promoted by the admin. This evidence is used by the perpetrator to attract victims to play online gambling. Promotional images often display large prizes and lucrative winnings, while invitation messages contain direct links to the advertised gambling sites.

Table 5. Results of Evidence Collection

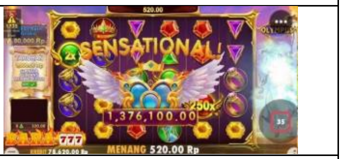
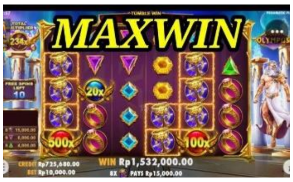
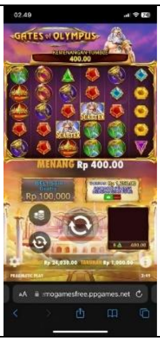
Message Result	Image Result
I want to help all of you with my SETTING ACCOUNT, just with a minimum of 50k you can MAXWIN & WITHDRAW up to 1 million, don't you want it?	BONUS 100% MANSION77 DEPOSIT 50K + GRATIS 50K TO X5
You can do this by entering our link, we guarantee that you will MAXWIN	DAFTAR SLOT GACOR MUDAH JACKPOT HARI INI! 500x
Okay, I'll help you right away.	
You have to register first, how to fill in: Username: Phone Number: Account Number: Bank/E-Wallet Name:	
Okay, I'll list it right away	

Table 5 contains evidence collected in the research of online gambling cases in the Telegram application. This evidence includes invitation messages such as "I want to help all of you with my SETTING ACCOUNT, just with a minimum of 50k you can MAXWIN & WITHDRAW up to 1 million, don't you want it?", followed by offering a link to an online gambling site "The trick is if you enter our link, we guarantee you will MAXWIN", as well as assistance to victims with the message "Okay, let me help you" for the registration process which requests information such as Username, Phone Number, Account Number, and Bank/E-Wallet Name. The admin also pretends to register victims with the message "Okay, I'll register you right away", and the perpetrator sends promotional images of the site and the results of online gambling winnings to attract victims.

The final step displays the results of the information collection of the examination results and evaluates the digital evidence in the Telegram application. The results obtained using forensic tools such as MOBILedit Forensic Express, Magnet AXIOM and Hash My Files are shown in Table 6.

Table 6: results of Evidence Obtained from Each Tools

Tools	Order	Image	Code MD5Hash	Code SHA	Amount
MOBILedit Forensic Express	X	V	V	V	15
Magnet AXIOM	V	X	V	X	5
Hash My Files	X	X	V	V	10

Figure 25 show the results of the three main forensic tools. MOBILedit Forensic Express had the highest percentage of 80.50%, as it successfully collected evidence in the form of images, MD5Hash and SHA-256 codes. Meanwhile, Magnet AXIOM and Hash My Files had a percentage of 40.25% each. Magnet AXIOM is only able to find evidence in the form of messages with MD5Hash codes, while Hash My Files can only generate MD5Hash and SHA-256 codes. This discrepancy may be due to limitations in extracting data from Android smartphones with Intel Atom chipsets, due to differences in phone architecture and a lack of technical knowledge about such chipsets. As a result, the report has been completed by providing a structured explanation and discussion in accordance with the stages of the National Institute of Standards and Technology (NIST), which include Collection, Examination, Analysis, and Report.

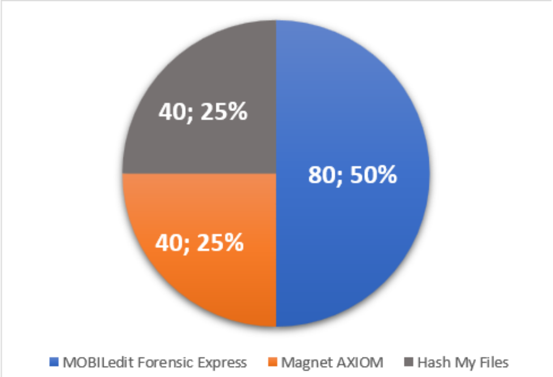


Figure 25: Percentage Number of Application Findings

5. CONCLUSION

The process of collecting digital evidence from smartphone devices in online gambling investigations through the Telegram Mobile app shows that the method of the National Institute of Standards and Technology (NIST) is very effective. The method involves four main steps: Collection, Examination, Analysis, and Reporting. By following this method, researchers can more easily find and identify evidence of digital crime relevant to the smartphone device involved in online Gambling cases. In digital evidence analysis, various forensic tools such as MOBILedit Forensic Express, AXIOM Magnet, and Hash My Files are used. MOBILedit Forensic Express managed to identify evidence in the form of pictures of the promotion and the winning results sent by the perpetrators. AXIOM magnet found a conversation message containing an invitation to join an online gambling site. Meanwhile, Hash My Files is used to compare the MD5 and SHA-256 code similarities of the image file found with the previously extracted file_hashes_backup. The results of the use of these tools suggest that the applied digital forensic techniques can effectively uncover evidence that is crucial to the investigation of online gambling cases.

6. REFERENCES

[1] M. H. Ahda, "Analisis Bukti Digital Cyberbullying Pada Media Sosial Menggunakan Metode National Institut of Standard and Technology (NIST)," *Publ. Ilmu Komun. Media dan Cine.*, vol. 4, no. 1, pp. 49–55, 2021.

[2] A. Fitriansyah, Fifit, "Penggunaan Telegram Sebagai Media Komunikasi Dalam Pembelajaran Online," *J. Hum. Bina Sarana Inform.*, vol. 20, no. Cakrawala-JurnalHumaniora,p.113,2020,Available:http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala

[3] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," *J. Repos.*, vol. 2, no.10,pp.14001405,2020,doi:10.22219/repositor.v2i10.1066.

[4] D. P. Harahap, "Implementasi Digital Forensik Aplikasi Dompet Digital Dan Pesan Instan Pada Android Dengan Menggunakan Metode NIST," vol. 6, no. November, pp. 533–541, 2022, doi: 10.30865/komik.v6i1.5715.

[5] R. Rahmansyah, "Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook Dan Instagram Dengan Metode NIST," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 49–57, 2021, doi: 10.14421/csecurity.2021.4.1.2421.

[6] D. Mualfah and R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.

[7] K. N. Isnaini, H. Ashari, A. P. Kuncoro, "Analisis Forensik Untuk Mendeteksi Keaslian Citra Digital Menggunakan Metode NIST" *Key Concepts Mod. Indian Stud.*, vol. 3, no. 2, pp. 111–112, 2015, doi: 10.1007/978-3-322-91586-3_37.

[8] R. Majalista, T. Sutabri, "Analisis Pencarian Data Smartphone Menggunakan NIST Untuk Penyelidikan Digital Forensik," vol. 5, no. 1, pp. 81–85, 2023.

[9] 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, 2021, doi: 10.5120/ijca2021921680.

[10] R. B. Kusumadewa, Z. Sari, and E. A. Hakim, "Analisis Perbandingan Bukti Digital Forensik pada Instant Messaging Berbasis Smartphone Android Menggunakan Framework NIST," pp. 1–11, 2022.

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

[12] A. C. N. Hidayah and I. Riadi, "Digital Forensic Analysis on Mobile-based MiChat Services using National Institute of Standard Technology Method," *Int. J. Comput. Appl.*, vol. 184, no. 31, pp. 49–55, 2022, doi: 10.5120/ijca2022922387.

[13] S. M. Dusu and I. Riadi, "Mobile Forensic of Facebook Services using National Institute of Standard Technology (NIST) Method," *Int. J. Comput. Appl.*, vol. 183, no. 33, pp. 9–15, 2021, doi: 10.5120/ijca2021921716.

[14] Rudi Dian Arifin, "Transformasi Interaksi Sosial Sebagai Dapak Media Sosial Pada Siswa SMA Negeri 1PetasiaMorowali,"*dianisa.com*,2023.https://dianisa.com/pengertian-telegram/ (accessed Jun. 16, 2023).

[15] Asriadi, "Analisis Kecanduan Judi Online (Studi Kasus Pada Siswa SMK An Nas Mandai Maros Kabupaten maros)," *Pap. Knowl. Towar. a Media Hist. Doc.*, vol. 5, no. 2, pp. 40–51, 2020.

[16] F. H. Lubis, M. Pane, and Irwansyah, "Fenomena Judi Online di Kalangan Remaja dan Faktor penyebab Maraknya Serta Pandangan Hukum Positif dan Hukum Islam (Maqashid Syariah)," *J. Pendidik. dan Konseling*, vol. 5, no. 2, pp. 2655–2663, 2023,. Available:https://journal.universitaspahlawan.ac.id/index.php/jpdk/article/view/13284/10396

[17] G. Mishardila, "Analisa Dan Pencarian Bukti Forensik Digital Pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik," *Skripsi,Univ.IslamRiau*,2020.Available:https://repository.uir.ac.id/11694/%0Ahttps://repository.uir.ac.id/11694/1/153510355.pdf

[18] Mkfaridi, "Melakukan Akuisisi dengan Menggunakan Metode Physical dan Logical Aquisition pada Aplikasi FTK Imager Terhadap Bukti Elektronik," *DigitalForensiku*,2018.https://digitalforensiku.wordpress.com/2018/01/10/melakukan-akuisisi-dengan-metode-physical-dan-logical-aquisition-terhadap-bukti-elektronik-menggunakan-aplikasi-ftk-imager/ (accessed Jun. 16, 2023).

[19] D. Yuliana, T. Yuniati, and B. P. Zen, "Analisis Bukti Digital Cyberbullying Pada Media Sosial Menggunakan Metode National Institut of Standard and Technology (Nist) 800-101," *LEDGER J. Inform. Inf. Technol.*, vol. 1, no. 3, pp. 113–123, 2022, doi: 10.20895/ledger.v1i3.812.

[20] N. Saputri and R. Indrayani, "Analisis Data Forensik Investigasi Kasus Peredaran Narkoba Pada Smartphone Berbasis Android," *Djtechno J. Teknol. Inf.*, vol. 3, no. 2, pp. 156–166, 2022, doi: 10.46576/djtechno.v3i2.2597.

[21] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," *J. Sains Komput. Inform.*, vol. 6, no. 2, pp. 1112–1120, 2022.

[22] T. Irawan and I. Riadi, "Mobile Forensic Signal Instant Messenger Services in Case of Web Phishing using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 184, no. 32, pp. 30–40, 2022, doi: 10.5120/ijca2022922394.

[23] A. ahmadi, T. Akbar, and H. Mandala Putra, "Perbandingan Hasil Tool Forensik Pada File Image Smartphone Android Menggunakan Metode Nist," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.

[24] I. Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, “Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST),” *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.

[25] A. P. Utami and I. Riadi, “Mobile Forensics Analysis of Line Messenger on Illegal Drug Transaction Case using National Institute of Standard Technology (NIST) Method,” *Int. J. Comput. Appl.*, vol. 183, no. 32, pp. 23–33, 2021, doi: 10.5120/ijca2021921712.