# Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework

**Yana Safitri, Imam Riadi, Sunardi**
Universitas Ahmad Dahlan, Yogyakarta, Indonesia

**Article Info**

***Article history:***

Received May 21, 2023
Revised Juny 26, 2023
Accepted July 15, 2023

***Keywords:***

*Body Shaming*
*Digital Forensic*
*Mobile Forensic*
*IMO Messenger*

***ABSTRACT***

Body shaming is the act of making fun of or embarrassing someone because of their appearance, including the shape or form of their body. Body shaming can occur directly or indirectly. MOBILEdit Forensic Express and Forensic ToolKit (FTK) Imager are used to perform testing of evidence gathered through Chat, User ID, Data Deletion, and Groups based on digital data obtained on IMO Messenger tokens on Android smartphones. This study aimed to collect evidence of conversations in body shaming cases using the Association of Chiefs of Police (ACPO) framework with MOBILedit Forensic Express and FTK Imager as a tool for testing. Based on the research findings, MOBILedit Forensic Express got an extraction yield of 0.75%. In contrast, using the FTK Imager got an extraction yield of 0.25%. The ACPO framework can be used to investigate cases of body shaming using mobile forensics tools so that the extraction results can be found. The results of this study contributed to forensic mobile knowledge in cases of body shaming or cyberbullying ACPO framework as well as for the investigators.

***Corresponding Author:***

Yana Safitri, +6287762222550,
Faculty Technology Industry, Master Program of Informatics,
Universitas Ahmad Dahlan, Yogyakarta, Indonesia,
Email: yana2107048011@webmail.uad.ac.id

How to Cite:
Y. Safitri, I. Riadi, and S. Sunardi, ”Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework”, MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 22, no. 3, pp. 651-664, Jul. 2023. This is an open access article under the CC BY-SA license (https://creativecommons.org/licenses/by-sa/4.0/)

## 1. INTRODUCTION

The advancement of Internet technology is rapid. The total number of internet users in cyberspace has surpassed 3.8 billion [1]. People may access the internet from anywhere, including on smartphones. Smartphones have now become a daily must for everyone [2]. Smartphone use has become a lifestyle need in Indonesia, which has a total population of 274.9 million in 2021 [3, 4]. Mobile phones now include an operating system that allows them to perform various duties similar to a personal computer, including internet connectivity. An Android smartphone is a hybrid device that functions as both a telephone and a computer but in a more portable form [5]. Smartphones, which have a variety of functionalities, can be exploited as cybercrime instruments [6]. The advancement of information and communication technology affects every aspect of life. Currently, mobile phones have numerous advantages and intriguing characteristics, the most prominent of which is the use of communication and life in cyberspace or online, namely social media [7]. There are numerous consequences to using social media, including cyberbullying [8]. In terms of cyberbullying cases, Indonesia ranks third in the globe. Children account for up to 91% of all cyberbullying reports [9]. Every year, the number of criminal cases on the internet grows. The internet has altered people's social lives, schooling, and even community activities [10]. Human activities today are mostly concerned with data, information, and communication, which are directly or indirectly tied to computer technology equipment. People benefit greatly from social media, but it also has significant drawbacks, such as disseminating inaccurate information, fake news, and addiction [11]. The effect of technology makes communication easier for people. In addition to having a good influence, information technology and telecommunications improvements have a negative consequence, specifically the increase in crimes involving online applications. The crime will undoubtedly leave evidence, such as a crime report, in court [12].

Digital forensics is a branch of science that applies investigative and analytical techniques to computer media or digital storage media in order to find, acquire, examine, and save evidence of criminal cases in order for them to be legally justifiedforensic analysis of worldwide Internet connections from several networks [13, 14]. Digital forensics refers to efforts to gather digital evidence relating to past crime cases [15], like in the case of IMO Messenger. IMO Messenger is an instant messaging application for iOS and Android devices. This application has almost the same capabilities as what WhatsApp offers. Instant messaging is a real-time communication channel that uses text, graphics, voice, or video [16]. Social media content can be of tremendous use to detectives during a criminal investigation [17]. To investigate short message-based cybercrimes like body shaming cases, detectives must analyze victims' and suspects' devices to locate digital evidence. Instant messengers have implemented end-to-end encryption technology to prevent privacy violations such as widespread spying by intelligence agencies [18]. Smartphones and social media are currently being widely abused to perpetrate crimes (cybercrime) such as human trafficking, cyberbullying, fraud, spreading hoaxes, and other crimes. Body shaming is a form of cyberbullying. The belief that your own body is the most ideal among your pals is one of the traits of body shaming. Unconsciously, you compare yourself to others who are slimmer or heavier than you. The Association of Chief Police Officers (ACPO) framework is used in this study to adapt the digital forensic investigation framework [19]. According to the guidance, it aids in dealing with high-tech crime claims and ensuring that all evidence is collected in a timely and acceptable manner. According to a senior police official. The results of the two forensic apps were compared using the MOBILEdit Forensic Express application and the FTK imager. It is intended that by using these techniques, a forensic investigator will be able to locate necessary artifacts [20]. The purpose of research, the method or framework, and the tools utilized separate this research from earlier research. It is envisaged that the research would yield digital evidence that will strengthen the proof of criminal cases in court in the form of digital evidence analysis results.

Riski Yudhi Prasongko et al. [21] researched the Use of the ACPO (Association of Chief Police Officers) Method on Forensic WhatsApp. The study employs 13 factors, and the results demonstrate that Belkasoft Evidence Center detects digital authenticity 81.92% of the time, while HashMyFiles detects it 79.95% of the time. Ilham Algi Plianda et al. [22] researched Analysis and Performance Comparison of Digital Forensic Tools on Android Smartphones using Whatsapp Instant Messaging, notably the MOBILEdit and Oxygen Forensic tools. In order to identify the best recommendations, the two tools are compared in terms of performance. This study demonstrates the advantages of the MOBILEdit tool over Oxygen Forensic in the context of the specific case. Many factors can affect the performance of each tool, including the type of device, the specifications of the device utilized, the version of the tools, and the research topic. As a result, the MOBILEdit Forensic tool is recommended in this study for digital schemes involving WhatsApp IM items and Android-based smartphone devices. Research conducted by Imam Riadi et al. [23] in the title Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework, MOBILedit Forensic Evidence, and Magnet AXIOM passed the repeatability and reproducibility validation tests in the following research. The AXIOM magnet did not obtain the digital signal messenger evidence from the offender's smartphone. The MOBILedit Forensic tool, on the other hand, was able to obtain Signal Messenger contact information and information with a performance value of 22.22%. MOBILedit Forensics and Magnet AXIOM do not receive digital evidence from Signal Messenger, such as chats, pictures, GIFs, pdf documents, videos, voice call history, and video call history. Research conducted by Galih Fanani et al. [24] in the title Michat Application Forensics Using the

Digital Forensics Research Workshop Method, Further investigation was conducted using Michat objects and the DFRWS approach with MOBILedit Forensic Express Pro tools, DB Browser For SQLite, and Oxygen Forensic Detective. A comparison was conducted to evaluate the capabilities of three forensic programs with varying processing levels in acquiring evidence: MOBILedit Forensic Express Pro (66.7%), DB Browser For SQLite (33.3%), and Oxygen Forensic Detective (83%). In litigation, digital evidence can be used as confirming evidence.

Unlike previous research, the forensic process was carried out using the DFRWS Framework [23, 24]. While the objects in previous research were WhatsApp [21, 22], Signal Messenger [23], and Michat [24]. This research is limited to text messaging (chats), user ID, erasing data, and groups and focuses on the IMO Messenger with the ACPO Framework. The primary goals of this study are to 1) perform digital forensic simulations using the ACPO framework and two tools, MOBILEdit Forensic Express and FTK Imager. 2) Search for digital evidence of body shaming incidents on the IMO Messenger app. This study focuses on digital evidence derived from instant messages.

This article is structured as follows: Part 1. Introduction, which includes a distinction from previous studies, section 2. Research Methods, which discusses the ACPO Framework for obtaining the expected research results, section 3. Results and analysis, which describes the research analysis results using the ACPO framework on IMO Messenger, use the MOBILEdit Forensic Express and FTK Imager tools, section 4. The conclusion summarizes the research findings and provides recommendations for further research.

## 2. RESEARCH METHOD

This study simulates digital forensic investigation. A simulation of digital forensic research focuses on investigating and finding the contents of digital devices and related computer crimes. Body shaming cases were the subject of case study-style digital forensic research simulations. Stages of forensic investigation utilize the ACPO framework in digital forensic simulation research. This study aims to forensic examine the Android smartphone software IMO Messenger. MOBILedit Forensic and FTK Imager are the forensic software programs used in this study. Figure 1 shows the steps of the research.

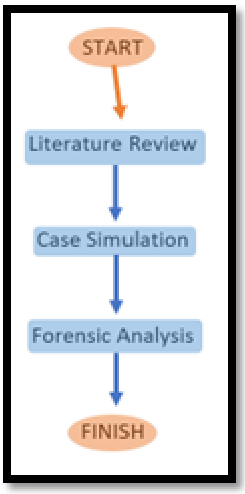


Figure 1. Research Flowchart

Following is a description of each stage of the research process. First is the literature review phase, which starts with gathering prior study data from different sources as a reference. Google Scholar, ResearchGate, and Science Direct were used to conduct literature searches on these websites. The terms Cybercrime, ACPO Framework, Mobile Forensics, Internet Messaging, Digital Forensics, and Body Shaming were used in the search process. Information for literature reviews is gathered from works published in reputable national and international publications. Articles from the past five years are those that are used. Investigations into Android-based devices can use earlier work in the fields of mobile forensics and the ACPO framework. The introduction and research methods section contains the literature review used as a study source.

The next case is a simulation step. Case simulation is developed at this stage. The study was started by carrying out a case simulation according to the previously designed case scenario shown in Figure 3. An Android device was used to carry out the case simulation, namely the victim's smartphone. Based on this research case study, the perpetrator was arrested with an Android smartphone which was used as evidence. Smartphones will be checked to see if there is any relevant digital evidence. A laptop with MOBILedit Forensic and FTK Imager tools was used for the investigation.

The third stage is forensic analysis. At this stage, the ACPO framework is used to assess the simulation data. Our research concentrates on text messages, user ids, deleted data, and groups to help with the search for digital evidence. The following are some of the variables sought in this study. The MOBILEdit Forensic and FTK Imager tools are used to identify research variables in the forensic analysis process. Analysis of forensic results is the last step, and the investigator examines the forensic findings.

### 2.1. Framework

The ACPO framework is used in this study to search for digital evidence in the form of text messages, user IDs, deleted data, and groups in four stages: Plan, Capture, Analyze, and Present. The ACPO framework was used to conduct this research. Figure 2 illustrates the four processes that must be completed to achieve good research results.

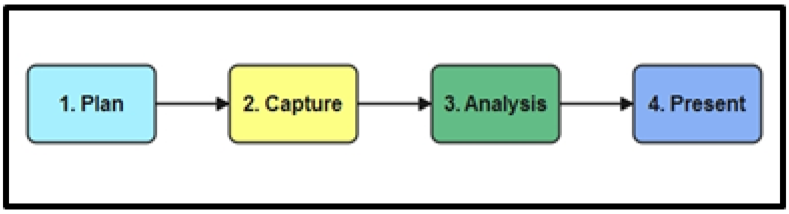


Figure 2. ACPO Flow

Figure 2 depicts the flow of the ACPO method, which consists of four stages:

#### 1. Plan

The planning phase starts with determining the hardware and software required for the research process in order to get research results. The planning process begins with determining the tools and research materials; research tools might be hardware or software, and their respective applications have been identified.

#### 2. Capture

This is the step in which all of the study results are recorded, stored, captured, and collected. Process capture on the results of the research process can make use of existing software as well as assistance hardware. The research will uncover data that can be used as evidence that there is no wrongdoing.

#### 3. Analysis

This is the step in which all of the study results are recorded, stored, captured, and collected. Process capture on the results of the research process can make use of existing software as well as assistance hardware. The research will uncover data that can be used as evidence that there is no wrongdoing.

### 2.2. Present

At this stage, an explanation of all actions carried out during the study is carried out and discussed in full the outcomes of the research and provides input or ideas linked to the study's conclusions.

### 2.3. Research Tools

Tools are now needed for this project in order to collect artifacts from the IMO Messenger program. There are two types of research tools: forensic software and hardware. The research materials utilized in this experiment are described in detail in Table 1.

Table 1. Research Tools

| Hardware and Software | Function |
|---|---|
| PC | A method used to transmit digital data from a smartphone to a storage device so that it can be analyzed |
| USB | Used to provide access from a smartphone and connect it to a computer |
| Smartphone | Used to store digital evidence data |
| KingRoot | Used to root the smartphone |
| MOBILedit Forensic Express | Used for the IMO Messenger application in the smartphone physical imaging process or data backup |
| FTK Imager | Used to carry out testing of digital evidence without changing the data or metadata of the original evidence |

### 2.4. Case Simulation

Simulation is utilized to collect the data required for the study's sample. Conversations in an instant messaging group are used to carry out the simulation. One of the group members became a victim of bullying. At this point, the researcher does mobile forensics, which uses ID numbers to look for criminals and serves as the foundation for retrieving an analysis report from a database. The method employed in this study involves retrieving conversational data from the victim's Imo database, which will then be further analyzed utilizing the MOBILEdit Forensic Express application as a tool to look for evidence in the form of chat and perpetrator id. a brief explanation of the mobile forensic workflow applied to the Figure 3; the scenario of a criminal investigation on the IMO instant messaging platform. The process of finding evidence will next be examined using the tools MOBILEdit Forensic Express and FTK Imager, which will offer data in the form of previously recorded conversations in the database.

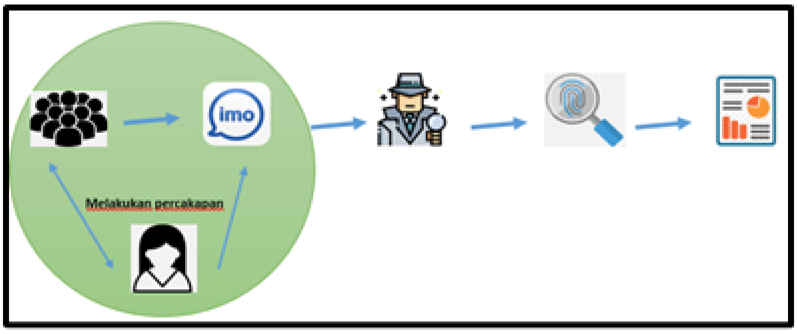


Figure 3. Case Simulation

In Figure 3, a case simulation was performed using a fictional group of teenage friends who regularly communicate on the IMO Messenger program in a group chat. However, one of them received a summons that referred to ”you are really fat right now” and other forms of body shaming, which caused the victim to complain and report it to the police. The investigator uses the victim's smartphone to perform an inquiry, and they receive the report's findings. The investigator constructed a scenario for this investigation. The scenario is a cyberbullying instance involving multiple attackers and one victim. In this case, the victim and the perpetrators had a chat that resulted in cyberbullying against the victim via the IMO Messenger application. As the victim's smartphone, a Samsung Galaxy Core 2 was used in this scenario.

## 3. RESULT AND ANALYSIS

This section will review how to use the Association of Chief Police Officers framework in IMO Messenger forensics.

### 3.1. Plan

This flow begins with preparing a plan outlining the stages to be taken in the research process, including creating scenarios and preparing research tools and materials. In this stage, a search, data collection, and documentation of evidence is carried out in the form of the victim's smartphone, according to the predetermined scenario. The evidence is alive, and the security feature is not active. At this stage, documentation related to the evidence is carried out. Documentation of evidence can be seen in Figure 4.

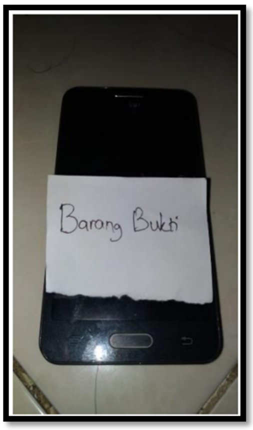
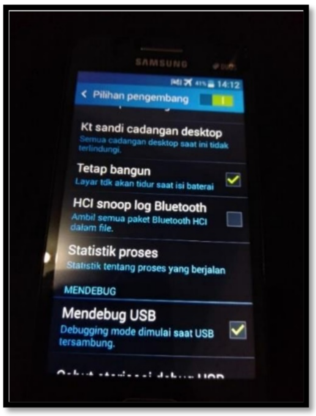


Figure 4. Protecting Evidence

The next step is to turn on Airplane mode to separate the evidence from the internet connection. Avoiding damaging evidence on the smartphone is the goal of Airplane Mode, then switch on the smartphone's Development Options feature. To prevent the smartphone from going into sleep mode if it is not used for a time, the Stay Awake and USB Debugging options must also be enabled. Sleep mode serves to stop smartphone devices from activating the security system during the forensic procedure. Figure 5 depicts the evidence isolation stage.



< Pilihan pengembang

Kt sandi cadangan desktop
Semua cadangan desktop saat ini tidak terlindungi.

Tetap bangun ☑
Layar tdk akan tidur saat isi baterai

HCI snoop log Bluetooth □
Ambil semua paket Bluetooth HCI dalam file.

Statistik proses
Statistik tentang proses yang berjalan

MENDEBUG

Mendebug USB ☑
Debugging mode dimulai saat USB tersambung.

Figure 5. Development Option

Table 1 depicts the investigation of the instruments and materials utilized in forensic analysis.

Table 2. Tools and Material

| Tool Name | Description |
|---|---|
| USB Cable | Connector smartphone to Laptop |
| Smartphone | Evidence |
| FTK Imager | Software |
| MOBILedit Forensic Express | Software |
| Laptop | Acquisition Process |

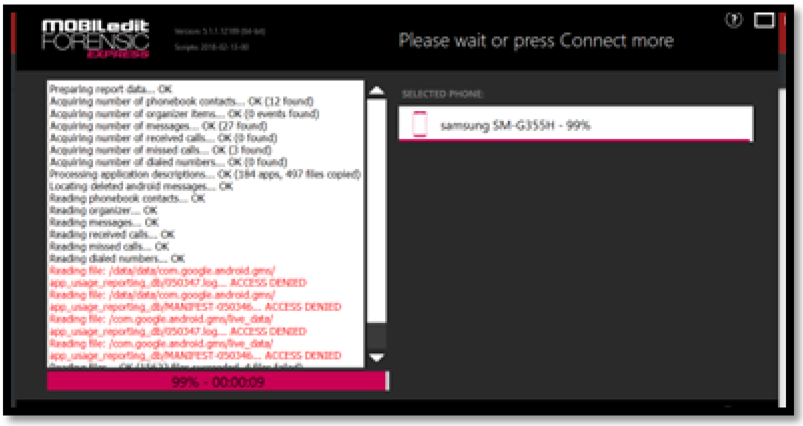
Table 2 shows the instruments utilized, which comprise an Acer Aspire E 14 core i3 laptop, a Samsung Galaxy Core 2 smartphone, and a USB connector. The IMO Messenger program, MOBILEdit Forensic Express, and FTK Imager tools are used to support this forensic research. The smartphone must first be rooted to extract data from an Android device.

The Imo application messenger, which is attached to the physical evidence, will evaluate the digital evidence utilizing the following investigation techniques on the evidence:

1. A smartphone running the Android operating system was purchased from the incident scene.
2. Isolation or signal coverage is turned off, and airplane mode is engaged.
3. By connecting to a laptop or PC with the ACER brand, MOBILEdit Forensic is used to back up smartphone evidence.
4. The MOBILEdit Forensic tool Express and FTK Imager are used for extraction and analysis.

### 3.2. Capture

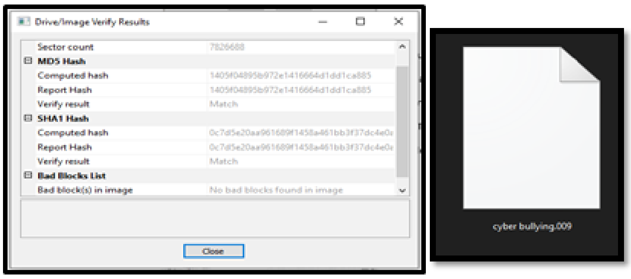
Capture is the process of storing or documenting all digital data obtained during the acquisition phase. The data is then classified according to its type. Because all forensics techniques utilized were able to gather, text chat and user Ids were the best results for confirming digital evidence data. Chat messages and user Ids are the most crucial and key data points for cyberbullying cases.



```
Preparing report data... OK
Acquiring number of phonebook contacts... OK (12 found)
Acquiring number of organizer items... OK (0 events found)
Acquiring number of messages... OK (27 found)
Acquiring number of received calls... OK (0 found)
Acquiring number of missed calls... OK (3 found)
Acquiring number of dialed numbers... OK (0 found)
Processing application descriptions... OK (184 apps, 497 files copied)
Locating deleted android messages... OK
Reading phonebook contacts... OK
Reading organizer... OK
Reading messages... OK
Reading received calls... OK
Reading missed calls... OK
Reading dialed numbers... OK
Reading file: /data/data/com.google.android.gms/
app_usage_reporting_db/050347.log... ACCESS DENIED
Reading file: /data/data/com.google.android.gms/
app_usage_reporting_db/MANIFEST-050346... ACCESS DENIED
Reading file: /com.google.android.gms/live_data/
app_usage_reporting_db/050347.log... ACCESS DENIED
Reading file: /com.google.android.gms/live_data/
app_usage_reporting_db/MANIFEST-050346... ACCESS DENIED
```

Figure 6. MOBILedit Forensic Express Capture Result

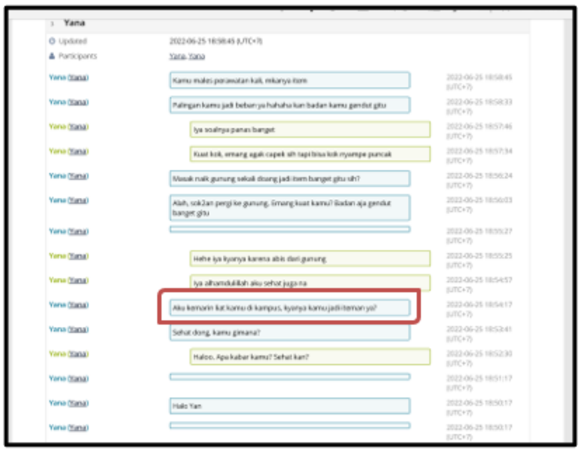
Figure 6 shows the output of a comprehensive report generated by the MOBILEdit Forensics Express tool. Then various reporting files in these outcomes will be employed as digital data. MOBILEdit Forensics Express is capable of logical as well as physical acquisition. MOBILEdit Forensics Express is capable of extracting data from smartphone devices. MOBILEdit Forensic Express can recognize a cell phone's International Mobile Equipment Identity (IMEI) and a registered SIM card's IMSI and Integrated Circuit Card Identifier (ICCID). MOBILEdit successfully obtained contact information, text messages, and group data.



| | |
|---|---|
| Sector count | 7826688 |
| ⊟ MD5 Hash | |
| Computed hash | 1405f04895b972e1416664d1dd1ca885 |
| Report Hash | 1405f04895b972e1416664d1dd1ca885 |
| Verify result | Match |
| ⊟ SHA1 Hash | |
| Computed hash | 0c7d5e20aa961689f1458a461bb3f37dc4e0 |
| Report Hash | 0c7d5e20aa961689f1458a461bb3f37dc4e0 |
| Verify result | Match |
| ⊟ Bad Blocks List | |
| Bad block(s) in image | No bad blocks found in image |

Figure 7. Capture Results and Imaging Results Using FTK Imager

Figure 7 depicts the SHA1 Hash value findings, where this value is utilized as a reference to match the hash value in the original file when imaging is performed. FTK Imager produced an imaging result file. FTK Imager is a tool for previewing and producing photographs for use in digital evidence testing. FTK Imagers may also create flawless duplicates (forensic images) of original evidence without altering the data or metadata.



Yana

Updated 2022-06-25 18:58:45 (UTC+7)

Participants Yana, Yana

Yana (Yana) Kamu males perawatan kali, mkanya item 2022-06-25 18:58:45 (UTC+7)

Yana (Yana) Palingan kamu jadi beban ya hahaha kan badan kamu gendut gitu 2022-06-25 18:58:33 (UTC+7)

Yana (Yana) Iya soalnya panas banget 2022-06-25 18:57:46 (UTC+7)

Yana (Yana) Kuat kok, emang agak capek sih tapi bisa kok nyampe puncak 2022-06-25 18:57:34 (UTC+7)

Yana (Yana) Masak naik gunung sekali doang jadi item banget gitu sih? 2022-06-25 18:56:24 (UTC+7)

Yana (Yana) Alah, sok2an pergi ke gunung. Emang kuat kamu? Badan aja gendut banget gitu 2022-06-25 18:56:03 (UTC+7)

Yana (Yana) 2022-06-25 18:55:27 (UTC+7)

Yana (Yana) Hehe iya kyanya karena abis dari gunung 2022-06-25 18:55:25 (UTC+7)

Yana (Yana) Iya alhamdulillah aku sehat juga na 2022-06-25 18:54:57 (UTC+7)

Yana (Yana) Aku kemarin liat kamu di kampus, kyanya kamu jadi iteman ya? 2022-06-25 18:54:17 (UTC+7)

Yana (Yana) Sehat dong, kamu gimana? 2022-06-25 18:53:41 (UTC+7)

Yana (Yana) Haloo. Apa kabar kamu? Sehat kan? 2022-06-25 18:52:30 (UTC+7)

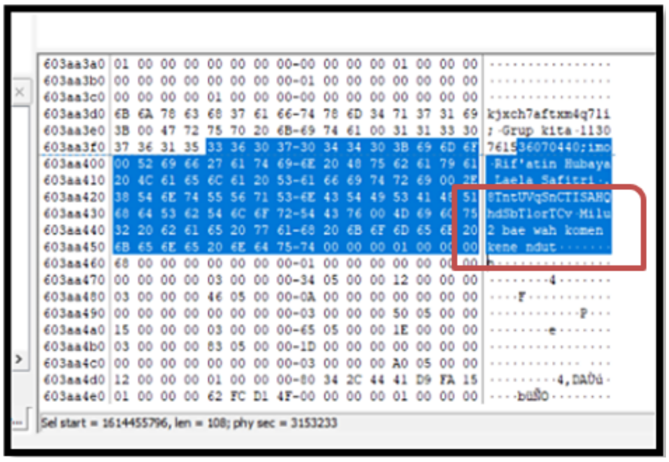
Yana (Yana) 2022-06-25 18:51:17 (UTC+7)

Yana (Yana) Halo Yan 2022-06-25 18:50:17 (UTC+7)

Yana (Yana) 2022-06-25 18:50:17 (UTC+7)

Figure 8. MOBILedit Forensic Express and Extracts Result

Figure 8 displays evidence gathered through chat. There are signs of cyberbullying in the chat since it comprises nasty sentences in the form of blasphemy toward the victim.



```
603aa3a0  01 00 00 00 00 00 00 00-00 00 00 00 01 00 00 00  ················
603aa3b0  00 00 00 00 00 00 00 00-01 00 00 00 00 00 00 00  ················
603aa3c0  00 00 00 00 01 00 00 00-00 00 00 00 00 00 00 00  ················
603aa3d0  6B 6A 78 63 68 37 61 66-74 78 6D 34 71 37 31 69  kjxch7aftxm4q71i
603aa3e0  3B 00 47 72 75 70 20 6B-69 74 61 00 31 31 33 30  ;·Grup kita·1130
603aa3f0  37 36 31 35 33 36 30 37-30 34 34 30 3B 69 6D 6F  761536070440;imo
603aa400  00 52 69 66 27 61 74 69-6E 20 48 75 62 61 79 61  ·Rif'atin Hubaya
603aa410  20 4C 61 65 6C 61 20 53-61 66 69 74 72 69 00 2E   Laela Safitri·.
603aa420  38 54 6E 74 55 56 71 53-6E 43 54 49 53 41 48 51  8TntUVqSnCTISAHQ
603aa430  68 64 53 62 54 6C 6F 72-54 43 76 00 4D 69 6C 75  hdSbTlorTCv·Milu
603aa440  32 20 62 61 65 20 77 61-68 20 6B 6F 6D 65 6E 20  2 bae wah komen 
603aa450  6B 65 6E 65 20 6E 64 75-74 00 00 00 01 00 00 00  kene ndut·······
603aa460  68 00 00 00 00 00 00 00-01 00 00 00 00 00 00 00  h···············
603aa470  00 00 00 00 03 00 00 00-34 05 00 00 12 00 00 00  ········4·······
603aa480  03 00 00 00 46 05 00 00-0A 00 00 00 00 00 00 00  ····F···········
603aa490  00 00 00 00 00 00 00 00-03 00 00 00 50 05 00 00  ············P···
603aa4a0  15 00 00 00 03 00 00 00-65 05 00 00 1E 00 00 00  ········e·······
603aa4b0  03 00 00 00 83 05 00 00-1D 00 00 00 00 00 00 00  ················
603aa4c0  00 00 00 00 00 00 00 00-03 00 00 00 A0 05 00 00  ················
603aa4d0  12 00 00 00 01 00 00 00-80 34 2C 44 41 D9 FA 15  ········4,DAÙú·
603aa4e0  01 00 00 00 62 FC D1 4F-00 00 00 00 01 00 00 00  ····büÑO········
Sel start = 1614455796, len = 108; phy sec = 3153233
```

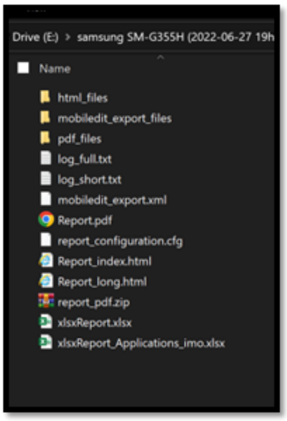
Figure 9. FTK Imager Data Extract Results

Figure 9 shows the outcome of the imaging results file recovered with the FTK Imager, which is the discussion between the criminal and the victim. However, because the conversations generated by data extraction are still scrambled, they must be found manually.

The extraction of text message data from the IMO Messenger application utilizing MOBILEdit Forensic Express and FTK Imager was successful. The outcomes of the extraction process were then evaluated. The digital data discovered in the analysis procedure in the form of text messages demonstrates that MOBILEdit Forensics Express and FTK Imager can gather digital data from the IMO Messenger program.

### 3.3. Analysis

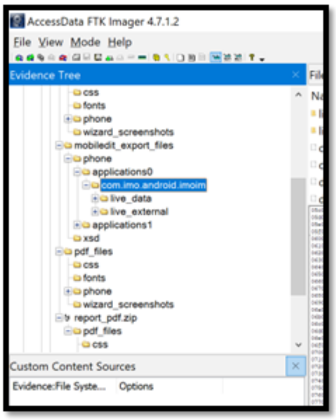
The following Table 2 contains IMO Messenger data that was used in the study. This stage involves the examination and processing of the data obtained through the examination process, followed by an investigation to obtain or discover proof of the required items, namely the Imo database kept on the smartphone device storage without affecting the integrity of the data.



```
Drive (E:) > samsung SM-G355H (2022-06-27 19h
Name
html_files
mobiledit_export_files
pdf_files
log_full.txt
log_short.txt
mobiledit_export.xml
Report.pdf
report_configuration.cfg
Report_index.html
Report_long.html
report_pdf.zip
xlsxReport.xlsx
xlsxReport_Applications_imo.xlsx
```

Figure 10. Full Report of MOBILedit Forensic Express

Figure 10 is the result of an extraction performed using the MOBILEdit Forensic Express tool found the report results which is a report on the results of digital evidence found in physical evidence.



```
      css
      fonts
    + phone
      wizard_screenshots
  - mobiledit_export_files
    - phone
      - applications0
        - com.imo.android.imoim
          + live_data
          + live_external
      + applications1
      xsd
  - pdf_files
      css
      fonts
    + phone
      wizard_screenshots
  - report_pdf.zip
    - pdf_files
        css
```

Figure 11. File Structure Tool of FTK Imager

The file structure that was extracted using the FTK Imager program is shown in Figure 11. The com.imo file found in the evidence is displayed by the FTK Imager program as the necessary database.

### 3.4. Present

This flow shows the evidence that was successfully acquired after the previous stages. The mobile forensic process and the ACPO flow on the Android platform were discovered to be capable of obtaining digital artifacts linked to the required evidence. These artifacts include conversations, User IDs, Data Delete, and Groups. In this study, the researchers focus exclusively on studying recorded and stored conversations in the database. Based on the testing findings, the index number formula determines each forensic tool's performance. The equation shows how the index number was calculated using an unweighted index.

$$P_{ar} = \frac{\sum ar0}{\sum arT} \times 100 \qquad (1)$$

Explanation:
$P_{ar}$ = Forensic tool accuracy index number.
$ar0$ = number of detected variables.
$arT$ = Total number of variables used [23].

Table 3 shows the analysis results based on the conclusions collected through digital evidence.

Table 3. Digital Evidence

| Data Type | MOBILedit Forensic Express | FTK Imager |
|---|---|---|
| Text Messaging | ✓ | ✓ |
| User ID | ✓ | - |
| Deleting Data | - | - |
| Group | ✓ | - |
| Percentage % | 0.75 | 0.25 |

Since it can only locate three of the four digital evidence parameters sought by the MOBIL edit Forensic Express tool's equation, its performance value is only 0.75%. The FTK Imager, nevertheless, has a performance value of 0.25% since it can only locate one of the four characteristics of digital evidence. The following formula can be used to obtain the performance value needed to gauge each forensic tool's potential.

$$\text{MOBILedit Forensic Express: } P_{ar} = \frac{3}{4} \times 100\% = 0.75\% \tag{2}$$

$$\text{FTK Imager: } P_{ar} = \frac{1}{4} \times 100\% = 0.25\% \tag{3}$$

The evidence extraction is in Table 3 illustrates that the MOBILEdit Forensic and FTK Imager tools can discover the digital chat evidence you are looking forthe total findings of the evidence forensic process for the Samsung Galaxy Core 2 android smartphone. The evidence discovered at the scene of the occurrence includes both digital and physical evidence. The victim's smartphone was discovered as physical evidence. Furthermore, an investigative process is carried out on the victim's smartphone to acquire digital evidence. Table 3 is the outcome of obtaining digital evidence using percentages. The overall findings of the forensic process for the evidence of the Samsung Galaxy Core 2 android smartphone after the stages were completed following the ACPO method step technique utilized for research. A comparison of research results obtained in other studies using the ACPO framework can be seen in Table 4.

Table 4. Comparison with previous research

| Title | Object | Artifact | Tools | Results |
|---|---|---|---|---|
| Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method with ACPO Standard. | Whatsapp | msgstore.db.crypt12 | Bluestack, FTK Imager, Whatsapp Viewer, and SQLite | The approach can be followed to perform WhatsApp analysis on the Android Bluestack simulator. Communication information about the Whatsapp application was collected from the Whatsapp database file msgstore.db.crypt12 as a result of the method. |
| Forensic Analysis of the TikTok Application on Android Smartphones Using the Association of Chief Police Officers Framework. | TikTok | Contact, Messages, Video, Hashtag | Magnet Axiom | The findings of the research process on the forensic analysis of the TikTok application, which runs on rooted Android smartphones, have several conclusions, including digital evidence obtained in the form of accounts, contacts, messages, videos, and hashtags related to defamation cases. A framework is used in the forensic procedure. ACPO's work and Magnet Axiom tools can be used to extract digital evidence from the TikTok app installed on the Samsung Galaxy Tab A SM-P355 smartphone. |
| Forensic Analysis of Dana Applications Using the ACPO Framework. | Dana | Profile Picture and Screenshot Transaction | Belkasoft Evidence Center & MOBILedit Forensic Express Pro | The results of the forensic analysis results obtained with two forensic tools, Belkasoft Evidence Center, failed to find artifacts that can be used as digital evidence. In contrast, the tool MobilEdit Express Pro forensics only managed to find artifacts in the form of photographs of users and screenshots of transactions made. |
| This study | IMO Messenger | Text Messaging, User ID, Deleting data, Group | MOBILedit Forensic Express and FTK Imager | The result found 0.75% data using MOBILEdit Forensic and 0.25% data using FTK Imager. |

In Table 4, research conducted by Kurniadin Abd. Latif et al. [25] titled Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method with ACPO Standard. Based on research, WhatsApp with the tools Bluestack, FTK Imager, Whatsapp Viewer, and SQLite. The findings of this investigation demonstrate that forensic analysis on Android devices using the Bluestacks simulator can be carried out following ACPO guidelines. Fitri Anggraini et al. [26] conducted research on the title Forensic Analysis of the TikTok Application on Android Smartphones Using the Association of Chief Police Officers Framework with the tool Magnet Axiom. The Magnet Axiom forensics software and the ACPO forensics framework are combined in this study. Together, they generated 77% of the proof through data messages, videos, and hashtags, in cases where these data were previously specified as initial data posted throughout the simulation procedure. Ermin et al. [27] researched Forensic Analysis of Dana Applications Using the ACPO Framework. Based on the research, the forensic analysis results were obtained using two forensic tools, Belkasoft Evidence Center and MobilEdit Express Pro Forensic Tools, and both failed to find artifacts that could be used as digital evidence. Compared with previous research, this research uses MOBILEdit Forensic and FTK Imager tools to search for digital evidence. Previous research did not use many tools to obtain information about the object to be tested.

## 4. CONCLUSION

According to the research findings of the Application of the Association of Chief Police Officers Framework for Body Shaming analysis Using the MOBILEdit Forensic Express tools, it has a 0.75% extraction percentage, and FTK Imager has a 0.25% extraction percentage. The findings of this study can be used as a resource for future studies; it is believed that the usage of forensic tools will become more diverse with the latest editions, allowing for the collection of additional digital artifacts from the IMO Messenger application. MOBILEdit Forensic gets more digital evidence, while FTK Imager only gets text messages and has to be searched manually. For future research, the researcher suggests studying mobile forensic techniques and frameworks and using other forensic instruments with recent updates to expect them to produce more precise results when collecting digital evidence.

## 5. ACKNOWLEDGEMENTS

Thank you to the Ahmad Dahlan University MTI Study Program for facilitating the Research Laboratory to complete the research.

## 6. DECLARATIONS

AUTHOR CONTIBUTION

This study was compiled by three authors divided into their respective tasks. Yana Safitri compiles and designs work, collects, analyzes, and interprets data. Imam Riadi and Sunardi as supervisors for articles to be published.

FUNDING STATEMENT

This study received no specific financing from any funding agency in the public, commercial, or non-profit sectors.

COMPETING INTEREST

I am unrepresented by conflicting financial, public, or institutional interests.

## REFERENCES

[1] I. Riadi, A. Yudhana, and M. A. Barra, “Forensik Mobile pada Layanan Media Sosial LinkedIn,” *JISKA: Jurnal Informatika Sunak Kalijaga*, vol. 6, no. 1, pp. 9–20, 2021.

[2] B. Fakiha, “Effectiveness of Forensic Firewall in Protection of Devices from Cyberattacks,” *International Journal of Safety and Security Engineering*, vol. 12, no. 1, pp. 77–82, 2022.

[3] A. Alanda, D. Satria, H. A. Mooduto, and B. Kurniawan, “Mobile Application Security Penetration Testing Based on OWASP,” *IOP Conference Series: Materials Science and Engineering*, vol. 846, no. 1, pp. 1–13, 2020.

[4] N. Setyaningsih, “Metode NIJ Untuk Analisis Forensik Layanan Dropbox Pada Smartphone Android,” *JURNAL CYBERAEREA*, vol. 2, no. 6, pp. 1–10, 2022.

[5] I. Riadi, “Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express,” *Jurnal Informatika Universitas Pamulang*, vol. 5, no. 1, pp. 89–94, 2020.

[6] R. Y. Patil and S. R. Devane, “Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 2031–2044, 2022.

[7] K. Gibson, “Bridging the digital divide: Reflections on using WhatsApp instant messenger interviews in youth research,” *Qualitative Research in Psychology*, vol. 19, no. 3, pp. 611–631, 2022.

[8] I. Riadi and S. Sunardi, “Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics,” *Jurnal Resti (Rekayasa Sistem dan Teknologi Informasi)*, vol. 1, no. 10, pp. 730–735, 2021.

[9] G. M. Abaido, “Cyberbullying on social media platforms among university students in the United Arab Emirates,” *International Journal of Adolescence and Youth*, vol. 25, no. 1, pp. 407–420, 2020.

[10] S. R. Ardiningtias, “Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice,” *JEPIN: Jurnal Edukasi & Penelitian Informatika*, vol. 7, no. 3, pp. 322–328, 2021.

[11] O. C. Hang and A. S. Media, “Cyberbullying Lexicon for Social Media,” *ICRIIS: International Conference on Research and Innovation in Information System*, 2019.

[12] I. Anshori, K. Eka, S. Putri, and U. Ghoni, “Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ,” *ITJRD: IT Journal Research & Development*, vol. 5, no. 2, pp. 118–134, 2021.

[13] S. Sotnik, T. Shakurova, and V. Lyashenko, “Development Features Web-Applications,” vol. 7, no. 1, pp. 79–85, 2023. [Online]. Available: https://openarchive.nure.ua/handle/document/21600

[14] S. Sunardi and I. Riadi, “Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi,” *RESTI: Rekayasa Sistem dan Teknologi Informasi*, no. June, 2020.

[15] A. K. Priyanka and S. S. Smruthi, “WebApplication Vulnerabilities:Exploitation and Prevention,” *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020*, pp. 729–734, 2020.

[16] R. N. Dasmen, F. Kurniawan, T. Komputer, U. B. Darma, S. Inggris, U. B. Darma, and D. Forensik, “Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial,” *Jurnal Teknologi Infomasi*, vol. 20, no. 4, pp. 527–539, 2021.

[17] M. El-tayeb, A. Taha, and Z. Taha, “Video Reconstruction for Firefox Browser Forensics,” *Ingénierie des Systèmes d ’ Information*, vol. 26, no. 4, pp. 337–344, 2021.

[18] J. Son, Y. Woong, D. Bin, and K. Kim, “Forensic Science International : Digital Investigation Forensic analysis of instant messengers : Decrypt Signal , Wickr , and Threema,” *Forensic Science International: Digital Investigation*, vol. 40, p. 301347, 2022.

[19] I. Riadi, R. Umar, and M. A. Aziz, “Forensik Web Layanan Instant Messaging Menggunakan Metode Association Of Chief,” *Mobile and Forensics (MF)*, vol. 1, no. 1, pp. 29–38, 2019.

[20] T. Hermawan and L. Roselina, “Android Forensic Tools Analysis for Unsend Chat on Social Media,” *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, pp. 233–238, 2020.

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

[22] I. A. Plianda and R. Indrayani, “Analisa dan Perbandingan Performa Tools Forensik Digital pada Smartphone Android menggunakan Instant Messaging Whatsapp,” *Jurnal Media Informatika Budidarma*, vol. 6, no. 1, p. 500, 2022.

[23] I. Riadi, H. Herman, and N. H. Siregar, “Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework,” *MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer*, vol. 21, no. 3, pp. 489–502, 2022.

[24] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," *RESTI*, vol. 6, no. April, pp. 1263–1271, 2022.

[25] K. A. Latif, R. Hammad, T. T. Sujaka, K. Marzuki, and A. S. Anas, "Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method With ACPO Standard," *International Journal of Information System & Technology Akreditasi*, vol. 5, no. 3, pp. 331–338, 2021.

[26] F. Anggraini, H. Herman, and A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," *JURIKOM (Jurnal Riset Komputer)*, vol. 9, no. 4, p. 1117, 2022.

[27] M. R. Setyawan and F. Tella, "Forensic Analysis Of Dana Applications Using The ACPO Framework," *JURASIK: Jurnal Riset Sistem Informasi dan Teknik Informatika*, vol. 8, pp. 1–8, 2023.

**[This page intentionally left blank.]**