

# Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method

Afif Nur Ichsan  
Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta Indonesia

Imam Riadi  
Departement of Information System  
Universitas Ahmad Dahlan  
Yogyakarta Indonesia

## ABSTRACT

The development of mobile device technology is very rapid in this global era. This has an impact on the increase in cybercrime such as narcotics transactions using the Instant Messenger application. IMO Messenger is an Instant Messenger application that can be used as a medium for crime because it has increased the number of users every year. This study used three stages of the Digital Forensics Research Workshop (DFRWS) method, namely identification, preservation, collection. This study uses two smartphones with root and non-root conditions that have the IMO application installed. The case used in this research is narcotics transactions based on previous case scenarios. Evidence from the criminal case will be acquired using four forensic tools, namely, MOBILedit forensic express, DB Browser for SQLite, AccessData FTK Imager, and Belkasoft evidence center. This research produces digital evidence in the form of chat files, images, audio, video, perpetrator's accounts, and chat times that have been deleted from a smartphone device in root condition. Calculation of the percentage index number from the evidence obtained on a smartphone with root conditions using MOBILedit forensic express tools at 100%, DB Browser for SQLite at 33.33%, AccessData FTK Imager at 33.33% and Belkasoft evidence center at 83.33%, smartphones with non-root conditions, no digital evidence was found.

## Keywords

Forensics, Mobile, IMO Messenger, Cybercrime, DFRWS

## 1. INTRODUCTION

The development of information technology from time to time has increased very rapidly, one of which is the development of social media. The results of a survey conducted by Wearesocial HootSuite stated that the number of active users of social media via mobile devices in Indonesia reached 130 million users as of January 2019 [1]. The growth of social media and Instant Messenger messaging applications have facilitated the development of many serious cybercrimes and malicious activities [2]. IMO Messenger is an Instant Messenger application that offers real-time data transmission over the internet which allows users to send group chat text messages, share photos, videos, videos, and audio calls. IMO Messenger has the potential to be used as a means of criminal acts such as cyberstalking (the use of the internet or electronic devices to harass a person, group of people, or certain organizations), sextortion (sexual extortion in cyberspace), drug trafficking (drug trafficking crimes) [3]. Forensic methods are an important factor that supports a more effective and efficient crime investigation in handling a criminal case

[4]. Mobile forensics or mobile phone forensics is the application of science to recover digital evidence from mobile devices by methods that are generally accepted and pay attention to illegal aspects [5]. Digital Forensics Research Workshop (DFRWS) is one of the methods used to carry out the stages of digital forensic analysis. This method helps obtain evidence and a centralized mechanism for recording the information gathered.

## 1.1 Study Literature

### 1.1.1 Previous Researcher Study Previous

The researcher's study referred to research by Asyaky, Widiyasono, and Gunawan (2018) conducted a study entitled "Analysis and Comparison of Digital Evidence on Instant Messenger Applications on Android". This research was conducted to obtain a comparison of the results of digital evidence using scenarios through the Whatsapp, Telegram, Line, and IMO applications. [5].

Mukti, Masruroh, and Khairani (2017) conducted a study entitled "Analysis and Comparison of Forensic Evidence on Facebook and Twitter Social Media Applications on Android Smartphones". This study was conducted to find and compare forensic evidence on social media applications Facebook and Twitter accessed on an Android smartphone using simulation methods and several scenarios were carried out to get the results [6].

Suryana, Akbar, and Widiyasono (2016) conducted a study entitled "Email Spoofing Investigation with the Digital Forensics Research Workshop (DFRWS) Method". This study examines digital forensic investigations on e-mail spoofing and the results of e-mail spoofing can be sent using web hosting services that provide e-mail sending facilities using the programming language PHP [8].

Larasati and Hidayanto (2017) conducted a study entitled "Analysis of Live Forensics for Comparison of Instant Messenger Applications on the Windows 10 Operating System". This study examines the comparison of the Instant Messenger application on the Windows 10 operating system by involving 3 social media applications, namely Facebook, Instagram, and Twitter. The results obtained are data comparison and system design [9].

Akbar, Nugraha, and Alaydrus (2016) conducted research selling "WhatsApp Forensics on Android Smartphones: A Survey". This study examines a survey of various methods from WhatsApp forensics researchers using internet protocol and live memory methods to obtain the required information data. The results of this study are from several surveys that have been conducted, obtained various kinds of results [10].

### 1.1.2 Digital Forensics

Forensics is a science and technology in the field of computers that aims to obtain, collect, and analyze digital evidence that can be used in an information technology crime [11]. Digital forensics is simply the whole process of retrieving, recovering, storing, checking information or electronic documents contained in electronic systems or storage media, based on methods and tools that can be scientifically justified for evidentiary purposes [12].

### 1.1.3 Mobile Forensics

Forensics or mobile phone forensics is the application of science to recover digital evidence from mobile devices with a method that is generally accepted and takes into account the illegal aspects [13]. Mobile phone forensics itself not only aims to fulfill the need for digital evidence in court (litigation process) but can also be used for non-litigation processes. Regardless of the ultimate goal, all procedures and implementation of mobile phone forensics must be based on methods commonly accepted by digital forensics.

### 1.1.4 Digital Evidence

Evidence is Electronic Information and/or Electronic Documents that meet the formal and material requirements stipulated in Law No. 11 of 2008 concerning Electronic Information and Transactions [14]. Digital evidence adheres to three main principles in the collection process, these principles refer to the Indonesian National Standard (SNI), namely ISO / IEC / 27037: 2014. The main principles of digital evidence include the relevance of the evidence to cases, the process that can be audited and repeated means that there is no damage to the evidence, and the evidence was taken is sufficiently large and precise in material [15].

### 1.1.5 Android

Android is a Linux-based operating system for mobile phones such as smart cell phones and tablet computers [16]. As an open application, Android is an open platform for developers to create applications that can be used by a variety of mobile devices.

### 1.1.6 IMO Messenger

IMO Messenger is an Instant Messenger application that offers real-time data transmission over the internet that allows users to send group chat text messages, share photos, videos, and audio calls. IMO messenger also allows users to talk to all contacts in the user's instant messaging account, including Facebook, Google Talk, Skype, MSN, ICQ, AIM, Yahoo! Messenger, Jabber, Hyves, V Kontakte, and even Steam.

### 1.1.7 Cybercrime

Cybercrime can be defined as a criminal act that violates the law by using computer technology as a criminal tool. Cybercrime occurs because there are advances in computer technology or the world of IT, especially internet media [17].

### 1.1.8 Digital Forensics Research Workshop

The Digital Forensics Research Workshop (DFRWS) method is one of the methods used to carry out the stages of digital forensic analysis. The DFRWS investigative model includes six stages that can help obtain evidence as well as a centralized mechanism for recording the information collected [18].

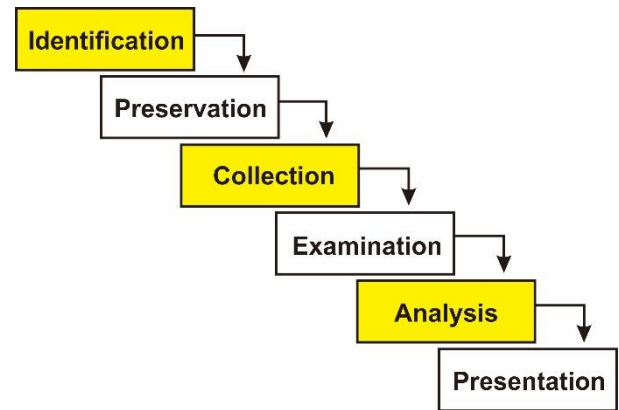


Figure 1. DFRWS Method

1. Identification  
The identification stage is the stage for determining needs including the research tools and materials needed for the investigation.
2. Preservation  
The maintenance stage is carried out to maintain the authenticity and validity of the digital evidence that has been obtained and to refute claims that the evidence has been sabotaged by irresponsible parties.
3. Collection  
The collection stage is the stage for identifying certain parts of digital evidence and identifying data sources in the smartphone database.
4. Examination  
The inspection stage is carried out to determine the filtering of data in certain parts of the data source from smartphone devices.
5. Analysis  
The analysis stage is the stage for determining where, by whom, how, and why the data was generated and obtained.
6. Presentation  
The presentation stage is the final stage carried out to present the information generated from the analysis stage.

### 1.1.9 Hashing

Hashing is a data identification method aimed at maintaining the integrity of data [19]. Hashing is not decodable so the user has to hash to see if the initial data is different from the current data. The way hashing works is more about matching the initial hashing result with the final hashing result. Examples of hashing are SHA-256 (Secure Hash Algorithm), MD5 (Message Digest), and Whirlpool. The SHA-256 algorithm can be used to check data integrity, create digital signatures, and others [20].

### 1.1.10 Rooting

The root is a system account that has the power to access and execute all files, commands, systems, in a Linux-based operating system [21]. Root has unlimited access which can give users the right to change, delete, add, or modify files or data located on the Android system. If analogous to the Windows computer operating system, the root function of Android is to grant administrator rights to the user.

## 2. METHODOLOGY

### 2.1 Research Scenario

The case scenario in this study uses two connected smartphones on the IMO Messenger application to make conversation interactions between two actors. Figure 2 illustrates the research scenario that occurs, where two perpetrators are suspected of committing crimes in the form of narcotics transactions using the IMO Messenger application.

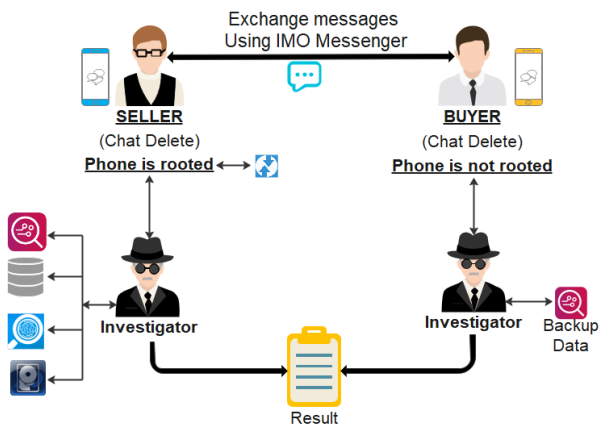


Figure 2. Research Scenario

Flow The scenario flow begins with the seller user communicating with the buyer user using a smartphone to exchange messages via Direct Message. Both users use the IMO Messenger application as a medium for communication and the results of their conversations will be stored in their respective device databases. The communication made by the two users is then deleted to leave a trace. The investigator will take over the second user's cellphone to examine the communication that has been deleted by the perpetrator user which contains cybercrime crimes.

The investigation process on the seller's user's smartphone is carried out a root process first using the TWRP tool to get data access rights on the device and on the buyer's user's smartphone, the root process is not carried out. The data backup process on both smartphones is carried out using the MOBILedit Forensic Express tools simultaneously when the data extract process. The data extraction process used four forensic tools, namely MOBILedit Forensic, DB Browser for SQLite, AccessData FTK Imager, and Belkasoft Evidence Center.

### 2.2 Research Stages

The research stage is a process where investigators carry out a forensic process through a predetermined procedure. The search for digital evidence is carried out by referring to the DFRWS steps. DFRWS steps can be seen in Figure 3.

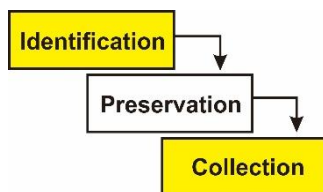


Figure 3. The stages of the research method

#### 2.2.1 Identification

The identification stage begins with preparing the tools that will be used by investigators or investigators in the process of




searching for digital evidence. The evidence used by investigators is secured to maintain the integrity and authenticity of the evidence found. Software and hardware is a tool that needs to be prepared for the process of finding digital evidence that can be seen in Table 1.

Table 1. Tools and Materials

| Tools and Materials            | Information  |
|--------------------------------|--|
| Laptop                         | Acer Swift 3 SF315-41 series OS Windows 10, 64 bit, AMD RYZEN™ 5 2500U Quad-core Processor |
| Kabel USB                      | Connect a smartphone with a laptop   |
| Smartphone 1                   | Lenovo A2020a40, root condition, Android OS, v5.1.1 (Lolipop)                              |
| Smartphone 2                   | Meizu U20, no root condition, Android OS, v6.0.1 (Marshmallow)                             |
| MOBILedit Forensic Express Pro | Forensic Tools   |
| DB Browser SQLite Manager      | Forensic Tools   |
| AccessData FTK Imager          | Forensic Tools   |
| Belkasoft Evidence Center      | Forensic Tools   |
| IMO Messenger                  | Messaging App  |
| Hash Tool                      | Hashing Tools  |

Evidence used in research as a medium for drug transaction crime in the form of two smartphones and one micro USB cable can be seen in Table 2.

Table 2. Evidence

| No | Evidence     | Picture   | Information   |
|----|--------------|---|---|
| 1  | Smartphone 1 |  | Smartphone 1<br>Lenovo A2020a40, root condition         |
| 2  | Smartphone 2 |  | Smartphone 2<br>Meizu U20, no root condition            |
| 3  | Data Cable   |  | Micro USB is used to connect a smartphone with a laptop |

### 2.2.2 Preservation

The maintenance phase begins by rooting the smartphone 1 to give full access rights to investigators. The root process is carried out using TWRP tools and a smartphone that has been rooted can be seen in Figure 4.

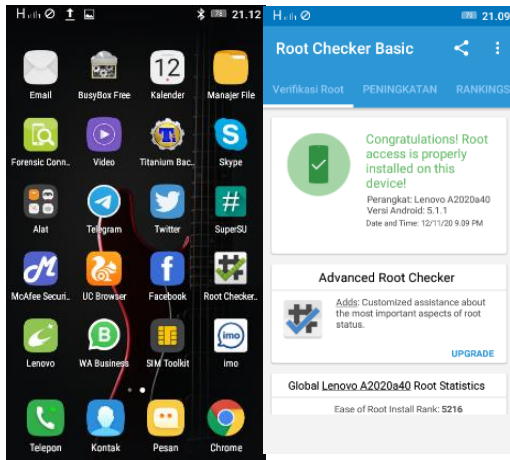


Figure 4. Smartphone root conditions

The next step is to create an imaging file or physical image on a smartphone 1 that is already rooted using the MOBILedit Forensic tools to maintain authenticity and integrity. data from the analyzed evidence. The imaging file process can be seen in Figure 5.

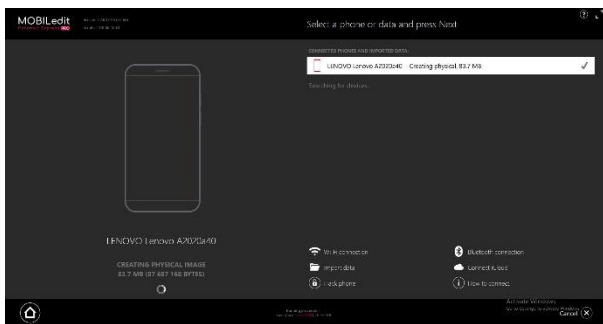


Figure 5. Display of the imaging file

The Imaging process on smartphone 2 using MOBILedit Forensic tools cannot be done because the create physical image menu does not appear as seen in Figure 6.

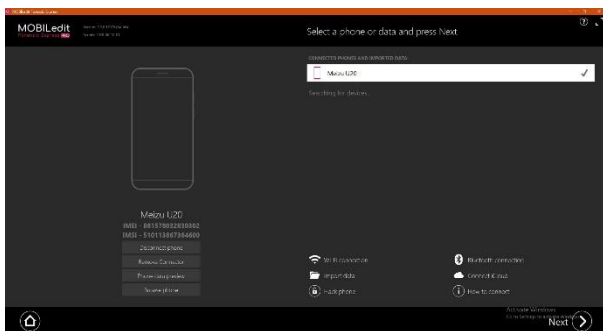


Figure 6. The initial appearance of MOBILedit

They create a physical image menu option that does not appear because the smartphone 2 status is not rooted.

### 2.2.3 Collection

The collection stage is the stage of the acquisition and data extraction process on the perpetrator's smartphone to seek and obtain digital evidence. The data acquisition process is carried out by extracting the physical image file that was previously created using the MOBILedit forensic tool. At this stage, investigators carry out the data acquisition process using four forensic tools, namely MOBILedit forensic, DB Browser for SQLite, AccessData FTK Imager, and Belkasoft Evidence Center.

#### 2.2.3.1 MOBILedit Forensic

The data acquisition process begins by analyzing the physical image that has been previously created. After the physical image is opened, a selection of applications (IMO) will appear that will be extracted. Application options can be seen in Figure 7.

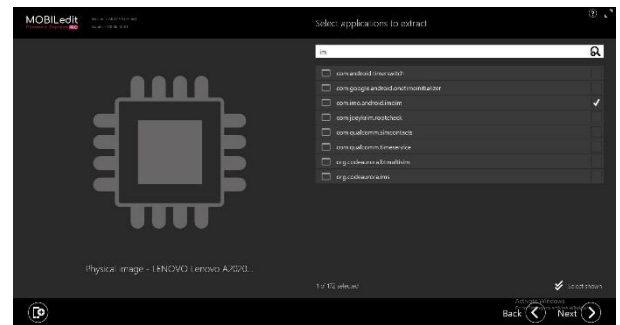


Figure 7. Display application options

The next process is data extraction in the selected application which can be seen in Figure 8.

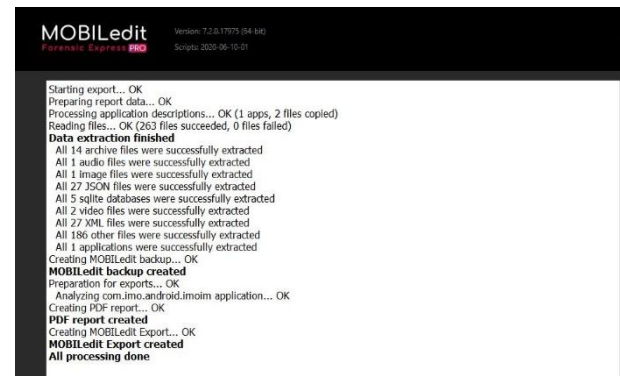


Figure 8. Data extraction process

The report file will be formed after the data extraction process is complete. The contents of the report file in PDF form show the results of a chat that was deleted by the perpetrator which was successfully restored by the MOBILedit tools. The contents of the chat that the perpetrator deleted can be seen in Figure 9.

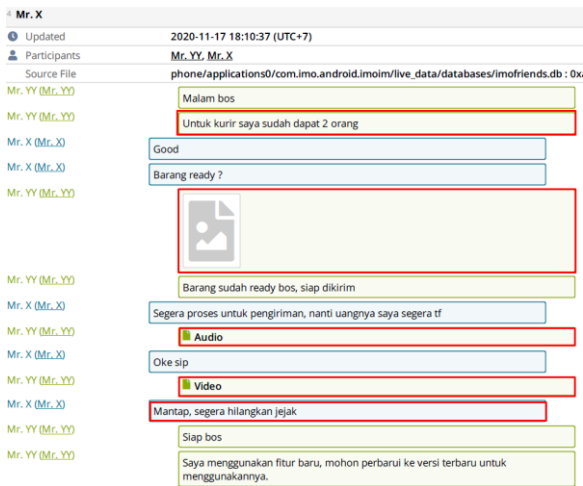


Figure 9. The appearance of the chat that the perpetrator deleted

Figure 10 shows other evidence files in the form of media files, namely images, audio, and video that can also be recovered and captured on the MOBILedit report tools page.

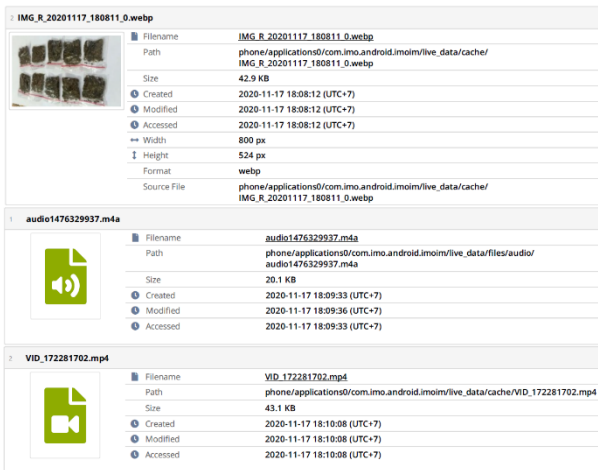


Figure 10. Display of image, audio, and video media files

### 2.2.3.2 DB Browser for SQLite

The process of analyzing evidence in the DB Browser for SQLite tools begins by opening the database file extracted from the data using the MOBILedit tools. The database file can be seen in Figure 11.

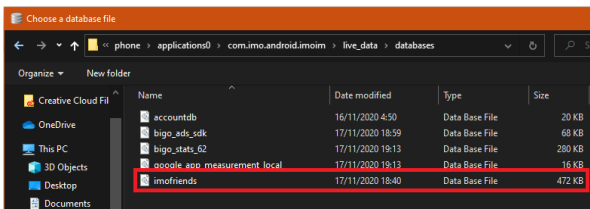


Figure 11. Display the database file "imofriends"

The next process is to open the database file "imofriends" with the DB Browser for SQLite tools which can be seen in Figure 12.

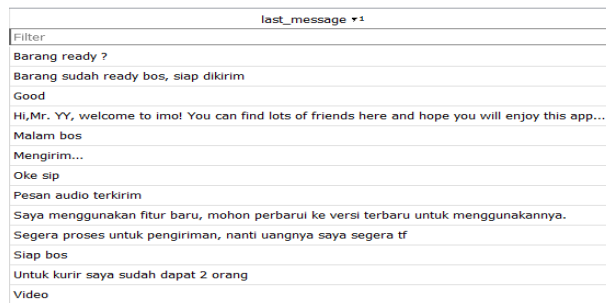


Figure 12. Display the contents of the database file "imofriends"

Figure 12 shows the appearance of the conversations carried out by the perpetrators listed in the table messages.

### 2.2.3.3 AccessData FTK Imager

DataThe process of data acquisition on the FTK Imager tool is done by opening the physical image file that has been created using the MOBILedit tools. The next process is to find the keywords used by the perpetrator on the Find menu as shown in Figure 13.

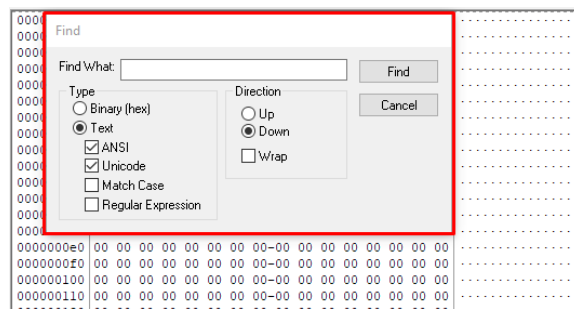


Figure 13. Display of conversation text search using the Find menu

The text search will be detected and appear if the entered keywords match one of the chats conducted by the perpetrator such as which can be seen in Figure 14.

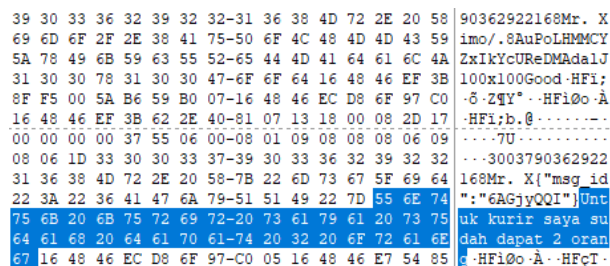


Figure 14. Display of text that has been successfully detected based on the entered keywords

Figure 14 shows the results of the searched text read on the FTK Imager tool. The text is one of the conversations carried out by the perpetrator.

### 2.2.3.4 Belkasoft Evidence Center

The data acquisition process in the tools is carried out by analyzing the physical image folders generated by the MOBILedit tools. Figure 15 shows the analysis process on the physical image folder.

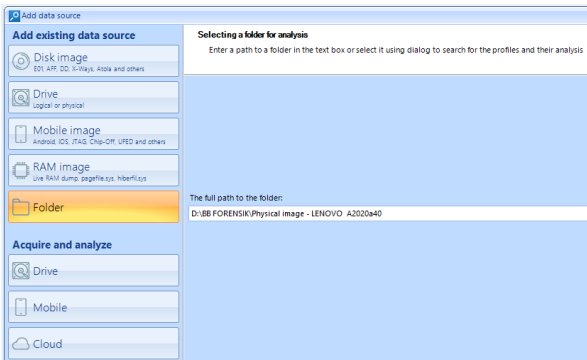


Figure 15. Display of physical image analysis

After the analysis process is complete, Belkasoft tools will display the results of the report on the dashboard page which can be seen in Figure 16.

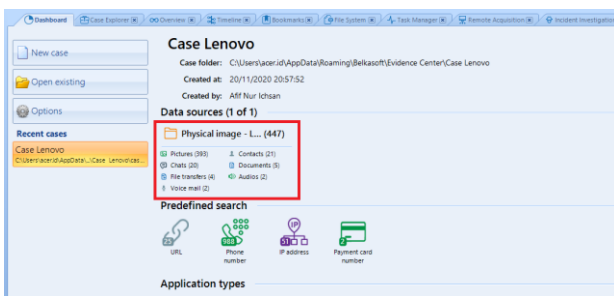


Figure 16. Display of report results on the dashboard page

More detailed data extraction results can be seen on the case explorer page where this page displays data that has been recovered in the form of conversation files, audio files, and files that have been deleted by the perpetrator as seen in Figure 17.

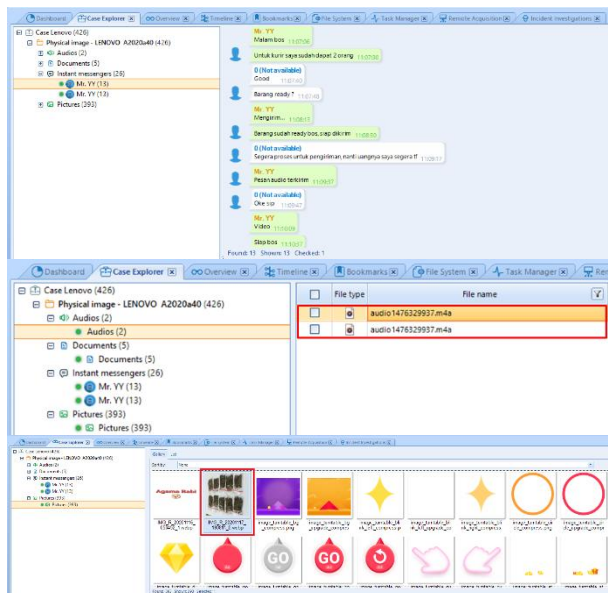


Figure 17. Display of conversation files, audio, and images

### 2.2.4 Hashing

Hashing is used to determine the authenticity of the data from the evidence obtained by matching the initial hashing result and the final hashing result using the Hash Tool. Evidence

obtained in the form of a conversation file is used as a sample of several other evidence files obtained during the data extraction process. The hashing process in the conversation file begins by looking for the source file contained in the PDF file reporting results using the MOBILedit tool which can be seen in Figure 18.



Figure 18. Display of the conversation source file

Figure 18 shows the information from the conversation that was deleted by the perpetrator with the source file located at the database file "imofriends.db" which can be seen in Figure 19.

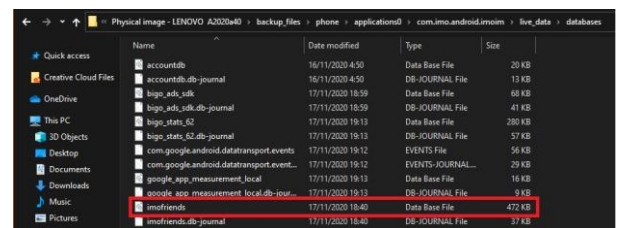


Figure 19. Display of the conversation database file

The next process is to look for the hash file information contained in the Excel file "fileHashes" as a result of data extraction using MOBILedit forensic tools which can be seen in Figure 20.

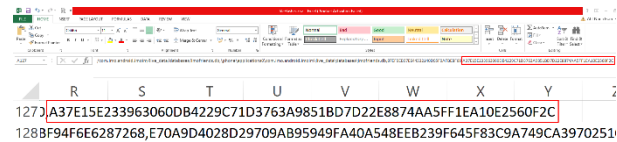


Figure 20. Display of the database hash file in the excel file

The next step is to show the hashing results in the database file "imofriends.db" using the Hash Tool software with the SHA-256 algorithm as shown in Figure 21.

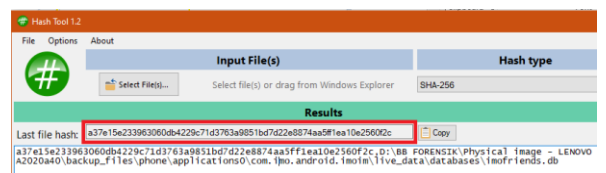


Figure 21. Display of conversation hash file results

Figure 21 shows the hashing results have the same or match with Excel file "fileHashes" with the algorithm code "a37e15e233963060db4229c71d3763a9851bd7d22e8874aa5ff1ea10e2560f2c".

### 2.2.5 Results

Data extraction process on a root condition smartphone using MOBILedit forensics express, DB Browser for SQLite, AccessData FTK Imager, and Belkasoft evidence center obtained differences in results. Evidence obtained on the perpetrator's smartphone with root conditions includes chat

files, image files, audio files, and video files that have been deleted by the perpetrator, and several other additional files which can be seen in table 3.

**Table 3. The Results Data Extraction**

| Results Obtained | Forensic Tools      |                       |            |                           |
|------------------|---------------------|-----------------------|------------|---------------------------|
|                  | MOBIL edit forensic | DB Browser for SQLite | FTK Imager | Belkasoft evidence center |
| Chat             | ✓                   | ✓                     | ✓          | ✓                         |
| Image            | ✓                   | x                     | x          | ✓                         |
| Audio            | ✓                   | x                     | x          | ✓                         |
| Video            | ✓                   | x                     | x          | x                         |
| Chat Time        | ✓                   | x                     | x          | ✓                         |
| Doer Account     | ✓                   | ✓                     | ✓          | ✓                         |

Based on table 3, percentage The index number from the evidence obtained on the smartphone at the root using MOBILedit forensic express tools is 100%, DB Browser for SQLite is 33.33%, AccessData FTK Imager is 33.33% and Belkasoft evidence center is 83.33%. Smartphones with non-rooted conditions do not get results because the imaging file process cannot be carried out to extract data on the smartphone.

### 3. CONCLUSION

The data acquisition process carried out at the collection stage using forensic tools produces findings of digital evidence in the form of chat files, images, audio, video, the perpetrator's account and chat time that has been deleted from a smartphone device in root condition. Smartphones with non-root conditions do not get the evidence they are looking for because the imaging file process cannot be carried out to extract data on the smartphone. The calculation of the percentage index number from the evidence obtained on the smartphone at the root using the MOBILedit forensic express tool is 100%, DB Browser for SQLite is 33.33%, AccessData FTK Imager is 33.33% and Belkasoft evidence center is 83.33%. This research is expected to provide insight into the general public about the mobile forensic process so that they can be careful in using social media to avoid crime.

### 4. REFERENCES

[1] Hootsuite, "Digital 2019: Indonesia," *Glob. Digit. Insights*, p. 77, 2019.

[2] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Comparative Analysis of Forensic Tools on Twitter Applications Using the Digital Forensics Research Workshop Method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, 2020.

[3] Muhammad Kukuh Tri Haryanto, "Forensics Analysis of the SQLite Database in the Android-Based IMO Application," 2018.

[4] M. Nur Faiz, W. Adi Prabowo, and M. Fajar Sidiq, "Study Comparison of Digital Forensic Investigation on Crime," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 1, pp. 63–70, 2018.

[5] Andri Puspo Heriyanto, *Mobile phone forensics: theory mobile phone forensics dan security series*, 1st ed.

Yogyakarta, 2016.

[6] M. S. Asyaky, "Analysis and Comparison of Digital Evidence on Instant Messenger Applications on Android," *J. Penelit. Tek. Inform.*, vol. Vol. 3 No, no. 1, pp. 220–231, 2019.

[7] W. A. Mukti, S. U. Masruroh, D. Khairani, and B. Forensik, "Analysis and Comparison of Forensic Evidence on Social Media Applications Facebook and Twitter on Android Smartphones," vol. 10, no. 1, 2017.

[8] A. L. Suryana, R. El Akbar, and N. Widiyasono, "Investigating Email Spoofing Using the Digital Forensics Research Workshop (DFRWS) Method," *J. Edukasi dan Penelit. Inform.*, vol. 2, no. 2, pp. 111–117, 2016.

[9] T. D. Larasati and B. C. Hidayanto, "Live Forensics Analysis for Comparison of Instant Messenger Applications on the Windows 10 Operating System," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.

[10] Z. Akbar, B. Nugraha, and M. Alaydrus, "Whatsapp Forensics on Android Smartphones: a Survey," *Sinergi*, vol. 20, no. 3, p. 207, 2016.

[11] S. RACHMIE, "The Role of Forensic Digital Science on Investigating Website Hacking Cases," *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020.

[12] E. Army, *Electronic Evidence in Judicial Practice*, 1st ed. Jakarta: Sinar Grafika, 2020.

[13] A. P. Heriyanto, *Mobile Phone Forensics: Theory: Mobile Phone Forensics and Security Series*, 1st ed. Yogyakarta: ANDI, 2016.

[14] C. Handoko, "The Position of Digital Evidence in Proving Cybercrime in Court," *J. Jurisprud.*, vol. 6, no. 1, p. 1, 2017.

[15] D. Oktavianto, *Log Analysis For Forensic Digital Investigation*, 4th ed. TIM Redaksi CDEF, 2018.

[16] W. Komputer, *Tips and Tricks Caring for Android-Based Cell Phones*. Jakarta: PT Elex Media Komputindo, 2012.

[17] E. Ketaren, "Cybercrime, Cyber Space, and Cyber Law," *Times*, vol. 5, no. 2, pp. 35–42, 2016.

[18] S. Sunardi, I. Riadi, and M. H. Akbar, "Steganalysis of Digital Evidence on Storage Media Using the Static Forensics Method," *J. Nas. Teknol. dan Sist. Inf.*, vol. 6, no. 1, pp. 1–8, 2020.

[19] Wardana, *Learning Programming, and Hacking Using Python*. Jakarta: PT Elex Media Komputindo, 2019.

[20] Y. Anugrah, M. Hannats, H. Ichsan, and A. Kusyanti, "Implementation of the SHA-256 Algorithm Using the MQTT Protocol in Ornamental Fish Cultivation," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 4, pp. 4066–4074, 2019.

[21] D. Kurniawan, *Android Hacking*. Jakarta: PT Elex Media Komputindo, 2016.