Forensic Mobile on IMO Messenger Services for Drug Trafficking using National Institute of Standard Technology Method

Whuty Meidilla Vadice
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
Information technology is currently developing very rapidly in the community. With the development of information technology, there are many positive or negative impacts from the use of technology. The IMO application provides data transmission in real-time over the internet, allowing users to send group chat text messages, share photos, videos, and audio calls. Criminals also use the Instant application Messenger for activities illegal such as activity hacker, fraud, drug trafficking, and crimes cyber other. This study was conducted to obtain digital evidence to reveal a criminal case of narcotics transactions that occurred in the IMO application Messenger using the stages National Institute of Standards and Technology (namely, collection, examination, analysis, and reporting). The data collection process uses the data acquisition technique DD Command that runs on the santoku Linux system. Autopsy and FTK Imager tools are used to extract physical images from the data acquisition technique DD Command. The results of data acquisition obtained from the Autopsy tool are exported in CSV format, to make it easier to read the file using a simple program created, namely CSV Reader. Based on the results of the study using the DD Command acquisition technique running on the santoku Linux system, it is possible to find the folder structure and its contents in the IMO application Messenger. Calculation of the percentage of index numbers from evidence obtained on smartphones using Autopsy tools is 100% and FTKImager there is 20% and 80% is not found in the evidence of information data in images, audio, call logs, and contacts. The Autopsy tool, which is used to extract physical images from the DD Command, can find deleted chats, images, and audio that can be used as information to help uncover crime cases on social media, while the FTK tool Imager can only find the text of the perpetrator's conversation.

Keywords
Forensics, Mobile, IMO Messenger, Cybercrime, NIST

1. INTRODUCTION
Information technology is currently developing very rapidly in society. With the development of information technology, there are many positive or negative impacts from the use of technology. The rapid development of technology is accompanied by the increasing use of social media. Social media is a means to share personal information, communicate with each other, share stories, post articles, pictures, or videos [1]. The social media that are widely used today are Instagram, Facebook, Twitter, Tiktok, and IMO Messenger. IMO as one of the Instant Messengers also has the potential to be used as a means of crime such as cyberstalking (use of the internet/electronic devices to harass a person, group of people, or certain organizations), sextortion (sexual blackmail in cyberspace), drug trafficking (drug trafficking crimes). [2]. To reveal a criminal case of drug trafficking that occurs at the application IMO Messenger stage using the National Institute of Standards and Technology (NIST) to the stages of collection, examination, analysis, and reporting.

1.1 Study Literature
1.1.1 Previous Study
This study refers to five previous studies conducted as a comparison with the current research with the previous one. The first research entitled “Analysis of Forensic Cyberbullying Investigations on Whatsapp Messenger Using the Method National Institute of Standards Technology”. In this study, data collection on WhatsApp messenger uses a tool that is often used in investigations, namely oxygen forensics. The text data that has been obtained will be analyzed using the cosine similarity method to help find texts that identify actions that are involved in cyberbullying with many words contained in the message text in the message. WhatsApp. The analysis of the forensic investigation of cyberbullying on WhatsApp uses the method of the National Institute of Standards Technology method to assist the process of removing evidence from the perpetrators of cyberbullying[3].

The second research entitled “Application of the National Institute of Standards Technology Method in Digital Forensic Analysis for handling Cybercrime”. The forensic tool used to find digital evidence on the perpetrator's device is KingRoot. This study resulted in forensic procedures in investigating the WhatsApp application to obtain previously deleted evidence in the form of conversation sessions, a list of contact numbers, profile photos of victims, and others. By applying the method, the National Institute of Standards and Technology will make it easier for researchers to find evidence of digital crimes on smartphones that can be used as evidence of criminal acts by following the steps contained in the National Institute of Standards and Technology method [4].

The third research entitled “Forensic Analysis of Kakaotalk Applications Using the National Institute of Standards Technology Method”. In this study, the process of removing digital evidence from the Kakaotalk application using the MOBIEdit Forensic Tool software. Digital evidence that is expected from the appointment process and forensic analysis can help the process of investigating a digital crime [5].

The fourth research entitled “Comparative Analysis of Digital Evidence from InstantApplications Messenger on Android”. In this study, the tools that will be used are King root and FTK Imager. The results of network forensic investigations carried
out on the IM application did not get relevant data to be used as digital evidence, but at least get information about the IP address of the server and the communication protocol used by each IM application when a simulation is done. The LINE application is the best application for maintaining chat privacy and protecting data from forensic investigators because deleted messages or calls on LINE cannot be recovered. LINE also uses end-to-end encryption for communication between smartphones and servers[6].

The fifth research entitled "Identification of Conversation Evidence for Dual Apps Whatsapp Applications on Xiaomi Phones Using the the National Institute of Standards Technology Mobile Forensics Method". In this study, the extraction process using Andriller on an object in the form of a Xiaomi Mi5 cellphone did not obtain digital evidence in the form of a database or other file. Andriller used to extract digital evidence contained in the Xiaomi Mi5 mobile phone is the latest version at the time of this research (version 2.6.40). Since the extraction results using Andriller and Laron could not find digital evidence of WhatsApp conversations in their entirety, both the original version and Dual Apps, extraction was carried out using the manual method through ADB by observing the rules of the National Institute of Standards Technology Mobile Forensics[7].

1.1.2 Digital Forensics
Forensics is an activity to investigate and establish the truth or facts related to criminal events and other legal cases[8]. In the field of technology, forensic analysis of digital or electronic evidence is called digital forensics or computer forensics [9]. The purpose of forensic science is to determine the value of an item of evidence. Digital proof or electronics consisting of valuable information and data stored or transmitted by digital devices[10].

1.1.3 Mobile Forensics
is the branch of digital forensics that deals with the recovery of digital data or evidence from mobile devices, but may also involve digital devices with internal storage and communication skills [11]. Mobile Forensics can extract data from mobile phones, which in turn can be used as digital evidence. This evidence can be an ethical basis for law enforcement to investigate the case[12]. Several types of evidence can be extracted from cellphones, namely, contact numbers, call logs, SMS messages, files, audio, email, and internet history [13].

1.1.4 Digital Evidence
Digital evidence is any evidentiary information stored or distributed in digital form that can be used for examination in court. Digital evidence is very important for proving computer crime cases involving storage media devices [14]. Digital evidence is evidence that is retrieved or recovered from electronic evidence [15]. Digital evidence has been recognized in Indonesia by the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions[16].

1.1.5 Android
Android is an operating system for mobile phones based on Linux. Android provides an open platform for developers to create their applications. It was originally developed by Android Inc, a newcomer company that makes software for mobile phones which were later purchased by Google Inc. For its development, the formed Open Handset Alliance (OHA) was, a consortium of 34 hardware, software, and telecommunications companies including Google, HTC, Intel, Motorola, Qualcomm, T-Mobile, and Nvidia[17].

1.1.6 IMO Messenger
IMO messenger is a chat application which is where users can send videos, photos, texts, to each other stickers & emoticons, and at the same time make audio and video calls to fellow IMO users around the world for free. According to its developers, the service has more than 200 million users, and more than 50 million messages per day are sent through it 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, Vkontakte, and even Steam[18].

1.1.7 Cybercrime
Cybercrime can be interpreted as an unlawful activity carried out by using a computer network as a medium/tool or a computer as an object, to cause or not harm other parties [18]. Cybercrime is a crime that uses information technology as a crime target and digital forensics answers the questions: when, what, who, where, how, and why related to digital crime [20]. There are two categories of cybercrime, the first category of violence/potential violence is a computer device that causes a physical impact on another person. The second category of non-violence is computer equipment that does not have a direct physical impact but provides systemic harm to a person[21].

1.1.8 Drug Trafficking
Terminologically in the Big Indonesian Dictionary, drugs are drugs that can calm nerves, relieve pain, cause drowsiness or a sense of stimulation [21]. The black market is used to buy and sell illegal drugs online. Some drug traffickers use encrypted messaging tools to communicate with drug suppliers[22]. Based on Law Number 35 of 2009 concerning Narcotics, it is stated that every act that is without rights is directly or indirectly related to narcotics is part of a narcotics crime. The use of narcotics can only be used for the benefit of medicine as well as science and technology. If it is known that there is an act outside the interests mentioned above, then the act is classified as a narcotics crime [23].

1.1.9 National Institute of Standard Technology
National Institute of Standards and Technology is a method used to perform forensic analysis [24]. Forensic stages that have policy work guidelines and standards to ensure that each examiner follows the same workflow so that work is documented and the results are repeatable and can be defended. The stages in NIST are collection, examination, analysis, and reporting [25]. The stages can be seen in Figure 1.

Figure 1. Stages of NIST Method
1. Collection
The collection is labeling, identification, recording, and retrieval of data from relevant data sources with the following procedure to maintain data integrity.

2. Examination
The examination is a process to protect evidence from damage and determine the integrity of the data that the evidence has not been changed or modified.

3. Analysis
The analysis is an analysis of the results of the examination using technically and legally justified steps.

4. Reporting
Reporting is reporting the results of the analysis of the investigation process and the data obtained from the investigation.

2. METHODOLOGY

2.1 Research Scenario
This scenario aims to discuss the flow of the stages of the mobile forensics process. This research scenario uses two smartphones that interact with each other on the IMO application Messenger, to interact and serve as evidence to uncover cases of cybercrime, namely narcotics transactions. At this stage, the process of identifying evidence as shown in Figure 2 will explain how an investigator is in the process of investigating evidence from a Smartphone device.

![Figure 2. Simulation of the Research Scenario on IMO Messenger](image)

Mobile forensic scenario As shown in Figure 2, a simulation of a criminal case, cybercrime namely narcotics transactions through the IMO application Messenger, starting from the perpetrators using smartphones exchanging messages. The smartphone used by the suspect becomes evidence for imaging using a forensic application. Investigators will take over the mobile phones of both users to examine messages that have been deleted by the perpetrators relating to narcotics transactions to the victim. The process of getting digital evidence begins with rooting, the root process using the Odin software. Furthermore, data collection on smartphones is carried out by extracting data or carrying out imaging processes to find out data that has been deleted and data recovery is carried out for the investigation process using the DD Command santoku Linux operating system and extracted using Autopsy tools and FTK Imager.

2.2 Research Stages
The search for digital evidence refers to the stages formulated by the National Institute of Standard Technology (NIST). These stages are described as follows.

2.2.1 Collection
At this stage, data collection is carried out. Data collection is the stage carried out by investigators to find and collect digital evidence. The evidence is one smartphone and one for the data cable or micro USB which is used to connect the smartphone with the laptop to carry out the data acquisition process. The following items of evidence collected by investigators can be seen in Table 1.

| No | Name | Image | Description |
|----|------|-------|-------------|
| 1  | The smartphone perpetrator’s front view | ![Image](image) | The Samsung Galaxy Grand Prime brand is on, connected to the network, and in a root state |
| 2  | The smartphone perpetrator looks back | ![Image](image) |
| 3  | Data Cable | ![Image](image) | Cable/Micro USB is the link between the smartphone and the laptop for data acquisition. |

The next stage is to perform a data backup process on a smartphone with a physical image using the DD Command acquisition technique for the santoku Linux operating system. The stages of the process Collection use the DD (Disk Definition) Command which is a Linux command to make a copy or backup of one partition to another storage media. When copying or backing up partitions to other media, not all data on the internal storage contains the required information, so it is necessary to select the data most likely to contain the required information. Data is usually stored in data blocks in internal memory.
Figure 3. Blocks of Internal Memory Data that Will be Made Image Files

From Figure 3 it can be seen that 27 blocks are used for the system and data stored in internal memory. The data block in internal memory is located in USERDATA which is stored in /dev/block/mmcblk0p27. This block of data will be copied to the host computer’s hard disk in the form of an image file using the DD command.

Figure 4. Data Transmission using The DD Command

Figure 4 is to read the physical disk and send data over the network (port 8888) and use Netcat (nc) to accept connections on port 8888. Next, set the connection routing between the workstation and smartphone using the command “adb forward tcp:8888 tcp: 8888”, it will forward all data from port 8888 between smartphone and workstation. Once connected, the data from the smartphone will be transferred to the images.img file, as shown in Figure 5.

Figure 5. Data Acquisition Process using The DD Command

This process takes a long time to create an image file from this data block because it has a large enough capacity of about 5.3 GB, and the result is that the physical image is stored in a directory home/santoku with the name images.img.

2.2.2 Examination

This stage is the process of protecting the evidence from damage and knowing the integrity of the data that the evidence has not been changed or modified. One way to protect the data is by hashing. Hashing is a method to perform integrity check to cause activities checks, which is to compare the results imaging whether they are the same as the original. The original hashing is done in terminal Santoku Linux with the command md5sum /location of files/file names, such as in Figure 6.

Figure 6. Visible Terminal Testing Hashing in Linux

After the images.img file was transferred to the Windows operating system, it must be integrity checked using command prompt (CMD) in windows, with the command certutil -hash file (filename) MD5, as in Figure 7.

Figure 7. Hashing Check Terminal Display on Windows

In Figures 6 and 7, it can be concluded that the results of the encryption code from the Linux operating system data acquisition file with the Windows operating system are the same, meaning that no data changes occur.

2.2.3 Analysis

This analysis stage is carried out after obtaining the desired data from the previous process. Analysis of the results of data acquisition with DD Command using the tool Autopsy.

2.2.3.1 Autopsy

From the results of the acquisition using the DD Command, the Images.img file is obtained which is a copy of the data block from the device smartphone. The result of data acquisition using DD Command has carried out the data search extraction process at autopsy. From the results of the acquisition DD Command extracted using autopsy, the files containing data and information are found in the /data/com.IMO.android.imoim folder. The results were obtained from the physical image of the DD Command of the IMO Messenger application, namely the IMO application database.

Figure 8. IMO Application Database Messenger
In Figure 8 are the chat findings that have been deleted by the perpetrator on the IMO Messenger application on the messages table.

Figure 9. Proof of the Deleted Image Autopsy

In Figure 9 is found an image that has been deleted by the perpetrator on the IMO application Messenger.

Figure 10. Proof of the Deleted Audio Autopsy

Figure 10 shows the results obtained other than images that have been deleted, namely audio that has been deleted.

Figure 11. Traces of Call logs, Contacts, Messages, Web Cookies, and Web History

In Figure 11 is other important information obtained from the IMO Messenger application, namely traces of call logs, contacts, and messages, web history, web cookies which can be used as information to help uncover criminal cases even though they are not directly related to the IMO application Messenger being researched. Call logs contain information about incoming and outgoing calls, when the call occurred, who made the call and received the call. Messages contain communication via text messages that have been done. While contacts contain phone numbers stored in the sim card or storage machines connected via the internet. The results of data extraction using the tool Autopsy found information related to the IMO application Messenger. After the acquisition process is carried out, the extraction results in the IMO application Messenger show that there are several folders: lib folder, cache folder, database folder, files folder, no-backup folder, and shared-pref folder. The results of the discovery of several folders of the evidence are shown in detail. Next, extract data from the file IMO Messenger using the tool Autopsy. As seen in Figure 12.

Figure 12. Extract File on Autopsy

In Figure 12 is extracting the IMO file Messenger using the tool Autopsy.

Figure 13. Extract File Results

Figure 13 is the result of extracting the IMO application data file Messenger stored in D:santoku\IMOMessenger\Export\15933com.IMO.android.imoim.

2.2.3.2 FTK Imager

The next analysis process uses FTK Imager. The results of data acquisition using DD Command carried out a data search extraction process on the FTK Imager which aims to find information and data from the crimes committed by the perpetrators. FTK Imager can be used to analyze the acquisition results with img format. Search results with the keyword “sent” can be found, which is shown in Figure 14.

Figure 14. First Search Results for FTK Imager

Figure 14 is a chat from the buyer to the seller, by asking for the delivery of goods.

Figure 15. Second Search Results for FTK Imager

In Figure 15 is a reply from the seller, by informing the delivery will be made tomorrow and delivered by 2 couriers.

2.2.3.3 CSV Reader

CSV Reader is a simple program to open data acquisition results obtained from the Autopsy tool by extracting data in CSV format. To make it easier to read the file, you can use a simple CSV Reader program. The initial view of the CSV Reader is shown in Figure 16.
Figure 16. Initial View of The CSV Reader Program

Figure 16 is the initial display for entering the file CSV to be read.

Figure 17. The Results of Importing CSV Data

In Figure 17, the contents of the data file that have been successfully inputted are the contents of the chat from the IMO application Messenger. The feature in the CSV Reader is the data filtering feature using the date, by filling in the boxes in the available columns, so investigators can easily search data according to the data sought. As shown in Figure 18.

Figure 18. The Filtering Data on CSV Reader

Figure 18 is filtering data, filtered from 01 September 2021 to 03 September 2021, the data will appear on the selected date. Furthermore, in the CSV Reader, there is a search feature for the data you want to find, by typing the word you are looking for, it will look like Figure 19.

Figure 19. Search Feature on CSV Reader

In Figure 19 the word you are looking for is the word "courier", then the data will appear as you are looking for. Furthermore, to make it easier for investigators to make reports, investigators can use the print feature which is useful for retrieving the required data, the data will automatically appear, as shown in Figure 20.

Figure 20. Print PDF from CSV Reader

Figure 20 is the output that was successfully printed on the CSV Reader application in pdf format.

2.2.4 Reporting

The final stage is reporting, which is reporting the results of the analysis of the investigation process and the data obtained. The report contains the results of the identification of imaging evidence of smartphone conditions in the root. The result of reporting using DD Command results in a physical image in the form of an img format which is extracted using the tools Autopsy and FTK Imager. The application analyzed for the research case is the IMO Messenger application installed on the Samsung Grand Prime smartphone. Case simulations made for research purposes are in the form of case simulations to obtain digital evidence in the form of deleted conversations. The evidence found in this study will be matched with the evidence owned by the buyer, which can be seen in Table 2.

Table 2. Findings and Evidence from Victims

| Evidence from the buyer's smartphone | Results Evidence found from the seller's smartphone |
|--------------------------------------|---------------------------------------------------|

27
Evidence of the conversation history on the buyer's smartphone is used as a reference to determine the person suspected of being the seller is the same person. From the table, it can be said that it is suspected that the seller is the same person who narrated the IMO conversation history Messenger on the buyer's smartphone.

2.2.5 Results

We can conclude the comparison results obtained from the physical image using a DD Command in a format IMG performed the extraction process using Tool autopsy and FTK Imager can be seen in the comparison Table 3.

| Data Information | Autopsy | FTK Imager |
|------------------|---------|------------|
| Chat             |         | ✓          |
| Images           | ✓       | x          |
| Audio            | ✓       | x          |
| Call Logs        | ✓       | x          |
| Contacts         |         | x          |

Table 3 is a comparison of the results found that uploads pictures that have been sent by the offender, conversation actors, audio, call logs, and contacts were found in tools autopsy and while the tools FTK Imager only found text conversation between perpetrator and victim.

3. CONCLUSION

Data acquisition technique using DD Command running on santoku Linux system can find the folder structure and its contents in the IMO application Messenger. Not only that, the results of Physical images using DD Command, other important information he gets are traces of call logs, contacts, and messages, web history, web cookies which can be used as information to help uncover criminal cases even though they are not directly related to the IMO application Messenger being researched. The autopsy tool used to extract the physical image from the DD Command can find databases with deleted chats, images and audio, while the tool FTK Imager can only find the text of the perpetrator's conversation. Further research can use smartphones with different operating systems such as IOS. This study uses the DD acquisition technique Command on Linux santoku, for further research it can use different and new acquisition techniques.

4. REFERENCES

[1] FS Mutma, "Description of Understanding Cyberbullying in Social Media in Students," J. Komun., vol. 13, no. 2, p. 165–182, 2019, doi:10.21107/communication.v13i2.5928.

[2] Muhammad Kukuh Tri Haryanto, “Forensics Analysis of SQLite Database on Android-Based IMO Applications,” p. 17, 2018.

[3] P. Widiandana, I. Riadi, and Sunardi, "Analysis of Forensic Investigations of Cyberbullying on Whatsapp Messenger Using the NIST Method," Semin. Nas. Technol. Fac. Engineering Univ. Krisnadwipayana, p. 488–493, 2019, [Online]. Available at: https://jurnal.teknikunikus.ac.id/index.php/seminastek2019/article/view/308.

[4] M. Fitriana, KA AR, and JM Marsya, "Application of the National Institute of Standards and Technology (Nist) Methods in Digital Forensic Analysis for Handling Cyber Crime," Cybersp. J. Educator. Technol.
