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 Instantapplication 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 FTKtool 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 usingthe 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 theMethod 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 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 MOBILedit 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 fourthresearch entitled "Comparative Analysis of Digital Evidence for 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 proofor 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, andtelecommunications 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 itIMO 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.

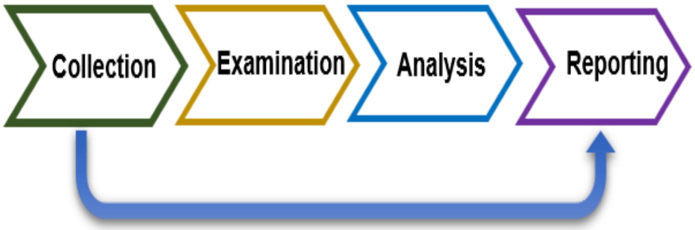


Figure 1. Stages of NIST Method

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.

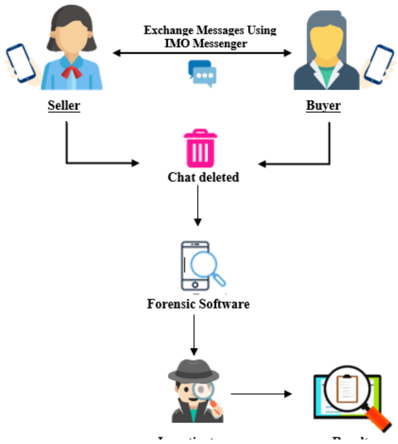


Figure 2. Simulation of the Research Scenario on IMO Messenger

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.

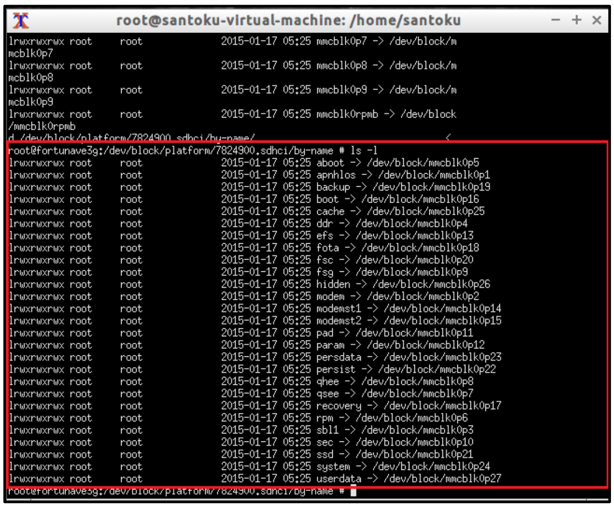
2.2.1 *Collection*

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.

Table 1. Physical Evidence Found

No	Name	Image	Description
1	The smartphone perpetrator' sfront view		The Samsung Galaxy Grand Prime brand is on, connected to the network, and in a root state
2	The smartphone perpetrator looks back		
3	Data Cable		Cable/Micro USB is the link between the smartphone and the laptop for data acquisition.

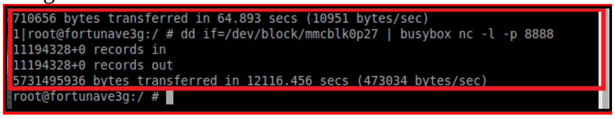
The next stage is to perform a data backup process on a smartphone with a physical image using the DD Command acquisition technique for the santoku Linux operating system. The stages of the process Collection use the DD (Disk Definition) Command which is a Linux command to make a copy or backup of one 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.



```
root@santoku-virtual-machine: /home/santoku
lrwxrwxrwx root     root              2015-01-17 05:25 mmcblk0p7 -> /dev/block/m
mcblk0p7
lrwxrwxrwx root     root              2015-01-17 05:25 mmcblk0p8 -> /dev/block/m
mcblk0p8
lrwxrwxrwx root     root              2015-01-17 05:25 mmcblk0p9 -> /dev/block/m
mcblk0p9
lrwxrwxrwx root     root              2015-01-17 05:25 mmcblk0rpmb -> /dev/block
/mmcblk0rpmb
d /dev/block/platform/7824900.sdhci/by-name/                            <
root@fortunave3g:/dev/block/platform/7824900.sdhci/by-name # ls -l
lrwxrwxrwx root     root              2015-01-17 05:25 aboot -> /dev/block/mmcblk0p5
lrwxrwxrwx root     root              2015-01-17 05:25 apnhlos -> /dev/block/mmcblk0p1
lrwxrwxrwx root     root              2015-01-17 05:25 backup -> /dev/block/mmcblk0p19
lrwxrwxrwx root     root              2015-01-17 05:25 boot -> /dev/block/mmcblk0p16
lrwxrwxrwx root     root              2015-01-17 05:25 cache -> /dev/block/mmcblk0p25
lrwxrwxrwx root     root              2015-01-17 05:25 ddr -> /dev/block/mmcblk0p4
lrwxrwxrwx root     root              2015-01-17 05:25 efs -> /dev/block/mmcblk0p13
lrwxrwxrwx root     root              2015-01-17 05:25 fota -> /dev/block/mmcblk0p18
lrwxrwxrwx root     root              2015-01-17 05:25 fsc -> /dev/block/mmcblk0p20
lrwxrwxrwx root     root              2015-01-17 05:25 fsg -> /dev/block/mmcblk0p9
lrwxrwxrwx root     root              2015-01-17 05:25 hidden -> /dev/block/mmcblk0p26
lrwxrwxrwx root     root              2015-01-17 05:25 modem -> /dev/block/mmcblk0p2
lrwxrwxrwx root     root              2015-01-17 05:25 modemst1 -> /dev/block/mmcblk0p14
lrwxrwxrwx root     root              2015-01-17 05:25 modemst2 -> /dev/block/mmcblk0p15
lrwxrwxrwx root     root              2015-01-17 05:25 pad -> /dev/block/mmcblk0p11
lrwxrwxrwx root     root              2015-01-17 05:25 param -> /dev/block/mmcblk0p12
lrwxrwxrwx root     root              2015-01-17 05:25 persdata -> /dev/block/mmcblk0p23
lrwxrwxrwx root     root              2015-01-17 05:25 persist -> /dev/block/mmcblk0p22
lrwxrwxrwx root     root              2015-01-17 05:25 qhee -> /dev/block/mmcblk0p8
lrwxrwxrwx root     root              2015-01-17 05:25 qsee -> /dev/block/mmcblk0p7
lrwxrwxrwx root     root              2015-01-17 05:25 recovery -> /dev/block/mmcblk0p17
lrwxrwxrwx root     root              2015-01-17 05:25 rpm -> /dev/block/mmcblk0p6
lrwxrwxrwx root     root              2015-01-17 05:25 sbl1 -> /dev/block/mmcblk0p3
lrwxrwxrwx root     root              2015-01-17 05:25 sec -> /dev/block/mmcblk0p10
lrwxrwxrwx root     root              2015-01-17 05:25 ssd -> /dev/block/mmcblk0p21
lrwxrwxrwx root     root              2015-01-17 05:25 system -> /dev/block/mmcblk0p24
lrwxrwxrwx root     root              2015-01-17 05:25 userdata -> /dev/block/mmcblk0p27
root@fortunave3g:/dev/block/platform/7824900.sdhci/by-name #
```

Figure 3. Blocks of Internal Memory Data that Will be Made Image Files

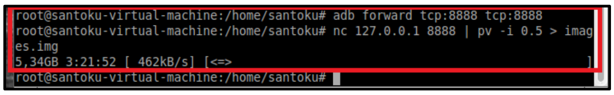
From Figure 3 it can be seen that 27 blocks are used for the system and data stored in internal memory. The data block in internal memory is located in USERDATA which is stored in /dev/block/mmcblk0p27. This block of data will be copied to the host computer's hard disk in the form of an image file using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



```
710656 bytes transferred in 64.893 secs (10951 bytes/sec)
1|root@fortunave3g:/ # dd if=/dev/block/mmcblk0p27 | busybox nc -l -p 8888
11194328+0 records in
11194328+0 records out
5731495936 bytes transferred in 12116.456 secs (473034 bytes/sec)
root@fortunave3g:/ #
```

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.



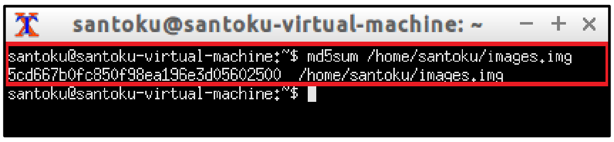
```
root@santoku-virtual-machine:/home/santoku# adb forward tcp:8888 tcp:8888
root@santoku-virtual-machine:/home/santoku# nc 127.0.0.1 8888 | pv -i 0.5 > imag
es.img
5,34GB 3:21:52 [ 462kB/s] [<=>                                              ]
root@santoku-virtual-machine:/home/santoku#
```

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

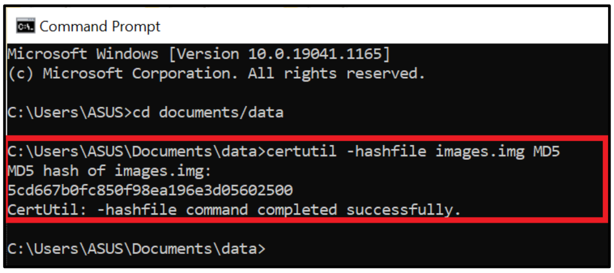
This stage is the process of protecting the evidence from damage and knowing the integrity of the data that the evidence has not been changed or modified. One way to protect the data is by hashing. Hashing is a method to perform integrity,harm to cause activities checks, which is to compare the results 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.



```
santoku@santoku-virtual-machine: ~
santoku@santoku-virtual-machine:~$ md5sum /home/santoku/images.img
5cd667b0fc850f98ea196e3d05602500  /home/santoku/images.img
santoku@santoku-virtual-machine:~$
```

Figure6. 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 Figure7.



```
Command Prompt
Microsoft Windows [Version 10.0.19041.1165]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ASUS>cd documents/data

C:\Users\ASUS\Documents\data>certutil -hashfile images.img MD5
MD5 hash of images.img:
5cd667b0fc850f98ea196e3d05602500
CertUtil: -hashfile command completed successfully.

C:\Users\ASUS\Documents\data>
```

Figure7. Hashing Check Terminal Display on Windows

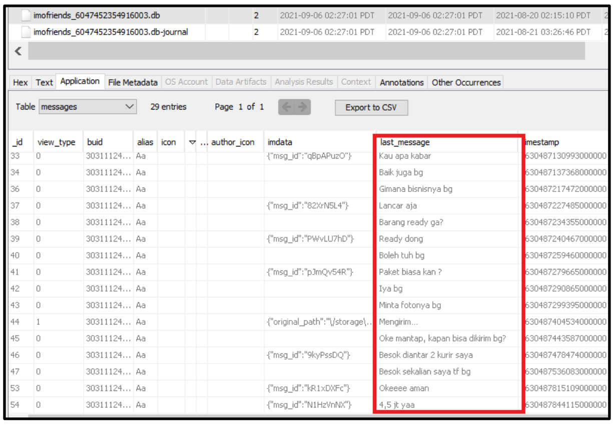
In Figures 6 and 7, it can be concluded that the results of the encryption code from the Linux operating system data acquisition file with the Windows operating system are the same, meaning that no data changes occur.

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.



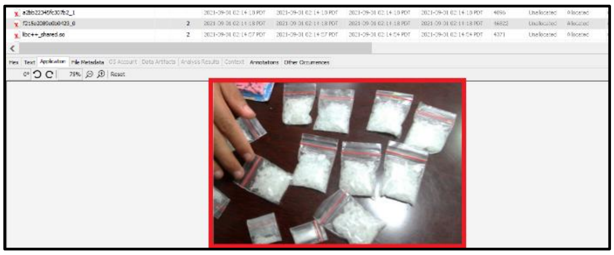
imofriends_6047452354916003.db	2	2021-09-06 02:27:01 PDT	2021-09-06 02:27:01 PDT	2021-08-20 02:15:10 PDT
imofriends_6047452354916003.db-journal	2	2021-09-06 02:27:01 PDT	2021-09-06 02:27:01 PDT	2021-08-21 03:26:46 PDT

Table messages 29 entries Page 1 of 1

_id	view_type	buid	alias	icon	▽	…	author_icon	imdata	last_message	imestamp
33	0	30311124…	Aa					{"msg_id":"qBpAPuzO"}	Kau apa kabar	630487130993000000
34	0	30311124…	Aa						Baik juga bg	630487137368000000
36	0	30311124…	Aa						Gimana bisnisnya bg	630487217472000000
37	0	30311124…	Aa					{"msg_id":"82XrN5L4"}	Lancar aja	630487227485000000
38	0	30311124…	Aa						Barang ready ga?	630487234355000000
39	0	30311124…	Aa					{"msg_id":"PWvLU7hD"}	Ready dong	630487240467000000
40	0	30311124…	Aa						Boleh tuh bg	630487259460000000
41	0	30311124…	Aa					{"msg_id":"pJmQv54R"}	Paket biasa kan ?	630487279665000000
42	0	30311124…	Aa						Iya bg	630487290865000000
43	0	30311124…	Aa						Minta fotonya bg	630487299395000000
44	1	30311124…	Aa					{"original_path":"\/storage\…	Mengirim…	630487404534000000
45	0	30311124…	Aa						Oke mantap, kapan bisa dikirim bg?	630487443587000000
46	0	30311124…	Aa					{"msg_id":"9kyPssDQ"}	Besok diantar 2 kurir saya	630487478474000000
47	0	30311124…	Aa						Besok sekalian saya tf bg	630487536083000000
53	0	30311124…	Aa					{"msg_id":"kR1xDXFc"}	Okeeee aman	630487815109000000
54	0	30311124…	Aa					{"msg_id":"N1HzVnNX"}	4,5 jt yaa	630487844115000000

Figure8. IMO Application Database Messenger

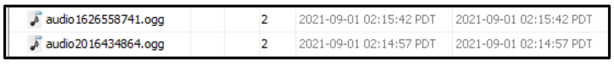
In Figure8 are the chat findings that have been deleted by the perpetrator on the IMO Messenger application on the messages table.



a2bb22345fc307b2_1		2021-09-01 02:14:10 PDT	2021-09-01 02:14:10 PDT	2021-09-01 02:14:10 PDT	2021-09-01 02:14:10 PDT	4096	Unallocated	Allocated
f215e2080a0b0423_0	2	2021-09-01 02:14:18 PDT	2021-09-01 02:14:18 PDT	2021-09-01 02:14:18 PDT	2021-09-01 02:14:18 PDT	16822	Unallocated	Allocated
libc++_shared.so	2	2021-09-01 02:14:57 PDT	2021-09-01 02:14:57 PDT	2021-09-01 02:14:54 PDT	2021-09-01 02:14:54 PDT	4371	Unallocated	Allocated

Figure9. Proof of the Deleted Image Autopsy

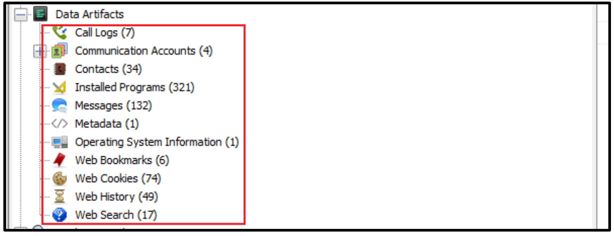
In Figure9 is found an image that has been deleted by the perpetrator on the IMO application Messenger.



audio1626558741.ogg	2	2021-09-01 02:15:42 PDT	2021-09-01 02:15:42 PDT
audio2016434864.ogg	2	2021-09-01 02:14:57 PDT	2021-09-01 02:14:57 PDT

Figure10. Proof of the Deleted Audio Autopsy

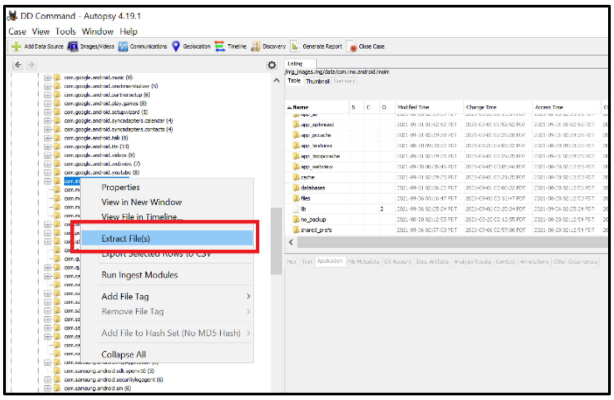
Figure10 shows the results obtained other than images that have been deleted, namely audio that has been deleted.



Data Artifacts
- Call Logs (7)
- Communication Accounts (4)
- Contacts (34)
- Installed Programs (321)
- Messages (132)
- Metadata (1)
- Operating System Information (1)
- Web Bookmarks (6)
- Web Cookies (74)
- Web History (49)
- Web Search (17)

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* Autopsyfound 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, *file*s 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.



DD Command - Autopsy 4.19.1

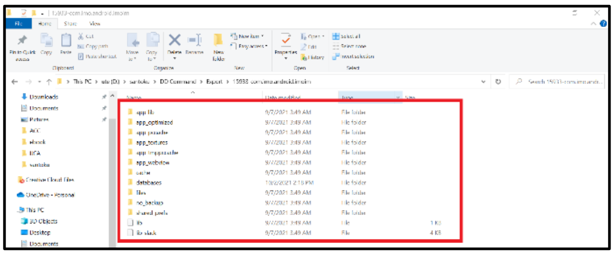
/img_images.img/data/com.imo.android.imoim

com.google.android.music (8)
com.google.android.onetimeinitializer (5)
com.google.android.partnersetup (6)
com.google.android.play.games (8)
com.google.android.setupwizard (5)
com.google.android.syncadapters.calendar (4)
com.google.android.syncadapters.contacts (4)
com.google.android.talk (8)
com.google.android.tts (11)
com.google.android.videos (8)
com.google.android.webview (7)
com.google.android.youtube (8)
com.samsung.android.sdk.spenv10 (3)
com.samsung.android.securitylogagent (6)
com.samsung.android.sm (6)

Name	S	C	O	Modified Time	Change Time	Access Time
app_optimized				2021-09-01 01:52:52 PDT	2021-09-01 01:52:52 PDT	2021-09-01 01:52:52 PDT
app_pccache				2021-09-01 02:29:28 PDT	2021-09-01 02:29:28 PDT	2021-09-01 02:29:25 PDT
app_textures				2021-08-20 09:03:22 PDT	2021-08-20 09:03:22 PDT	2021-08-20 09:03:22 PDT
app_tmppccache				2021-09-01 02:29:25 PDT	2021-09-01 02:29:25 PDT	2021-09-01 02:29:25 PDT
app_webview				2021-09-05 00:05:46 PDT	2021-09-05 00:05:46 PDT	2021-08-20 02:12:55 PDT
cache				2021-09-01 02:29:25 PDT	2021-09-01 02:29:25 PDT	2021-08-20 02:12:53 PDT
databases				2021-09-01 02:06:22 PDT	2021-09-01 02:00:22 PDT	2021-08-20 02:12:53 PDT
files				2021-09-06 03:16:47 PDT	2021-09-06 03:16:47 PDT	2021-08-20 02:12:53 PDT
lib			2	2021-09-06 02:25:24 PDT	2021-09-06 02:25:24 PDT	2021-09-06 02:25:24 PDT
no_backup				2021-08-20 02:12:55 PDT	2021-08-20 02:12:55 PDT	2021-08-20 02:12:54 PDT
shared_prefs				2021-09-06 02:57:00 PDT	2021-09-06 02:57:00 PDT	2021-08-20 02:12:54 PDT

Figure12. Extract File on Autopsy

In Figure12 is extracting the IMO file Messenger using the tool Autopsy.



15933-com.imo.android.imoim

This PC > ata (D:) > santoku > DD Command > Export > 15933-com.imo.android.imoim

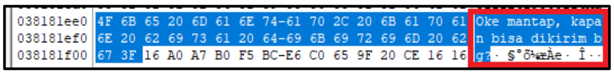
Name	Date modified	Type	Size
app lib	9/7/2021 3:49 AM	File folder	
app_optimized	9/7/2021 3:49 AM	File folder	
app pccache	9/7/2021 3:49 AM	File folder	
app_textures	9/7/2021 3:49 AM	File folder	
app tmppccache	9/7/2021 3:49 AM	File folder	
app_webview	9/7/2021 3:49 AM	File folder	
cache	9/7/2021 3:49 AM	File folder	
databases	10/2/2021 2:16 PM	File folder	
files	9/7/2021 3:49 AM	File folder	
no_backup	9/7/2021 3:49 AM	File folder	
shared prefs	9/7/2021 3:49 AM	File folder	
lib	9/7/2021 3:49 AM	File	1 KB
lib slack	9/7/2021 3:49 AM	File	4 KB

Figure 13. Extract File Results

Figure13 is the result of extracting the IMO application data file Messenger stored inD:\santoku\IMO*Messenger*\Export\15933com.IMO.android.imoim.

2.2.3.2 FTK Imager

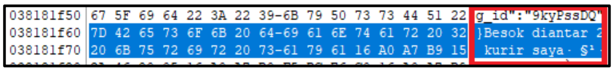
The next analysis process uses FTK Imager. The results of data acquisition using DD Command carried out a data search extraction process on the FTK Imager which aims to find information and data from the crimes committed by the perpetrators. FTK Imager can be used to analyze the acquisition results with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



```
038181ee0  4F 6B 65 20 6D 61 6E 74-61 70 2C 20 6B 61 70 61  Oke mantap, kapa
038181ef0  6E 20 62 69 73 61 20 64-69 6B 69 72 69 6D 20 62  n bisa dikirim b
038181f00  67 3F 16 A0 A7 B0 F5 BC-E6 C0 65 9F 20 CE 16 16  g?·§°õ¼æÀe· Î··
```

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.



```
038181f50  67 5F 69 64 22 3A 22 39-6B 79 50 73 73 44 51 22  g_id":"9kyPssDQ"
038181f60  7D 42 65 73 6F 6B 20 64-69 61 6E 74 61 72 20 32  }Besok diantar 2
038181f70  20 6B 75 72 69 72 20 73-61 79 61 16 A0 A7 B9 15   kurir saya·§¹·
```

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 inFigure16.

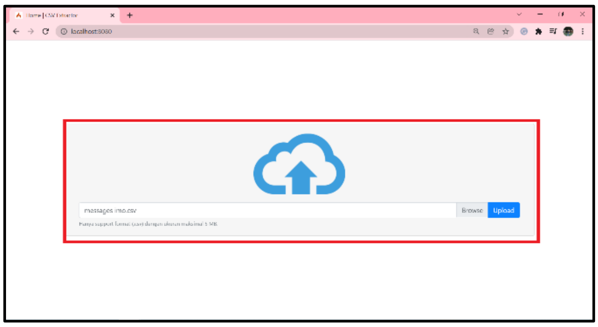
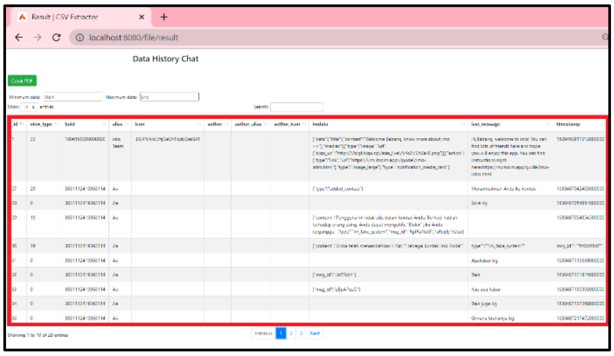


Figure16. Initial View of The CSV Reader Program

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



Result | CSV Extractor

localhost:8080/file/result

Data History Chat

Cetak PDF

Minimum date: Start Maximum date: End

Show 10 entries Search:

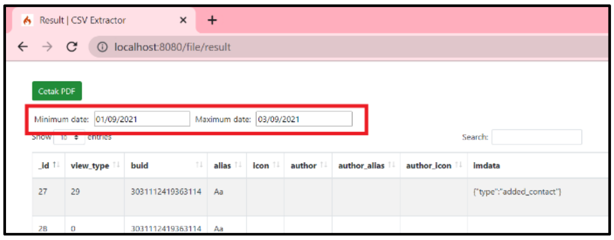
_id	view_type	buid	alias	icon	author	author_alias	author_icon	imdata	last_message	timestamp
1	33	1006160000000000	imo Team	[illegible]				{"data":{"title":{"content":"Welcome Babang, know more about imo >>"},"medias":[{"type":"image","url": [illegible]	Hi Babang, welcome to imo! You can find lots of friends here and hope you will enjoy this app. You can find instructions right here [illegible]	[illegible]
27	29	3031112419363114	Aa					{"type":"added_contact"}	Menambahkan Anda ke kontak	[illegible]
28	0	3031112419363114	Aa						Sore bg	[illegible]
29	19	3031112419363114	Aa					{"content":"Pengguna ini tidak ada dalam kontak Anda. Berhati-hatilah terhadap orang asing. Anda dapat mengklik "Blokir" jika Anda terganggu.","type":"im_fake_system","msg_id": [illegible]		[illegible]
30	19	3031112419363114	Aa					{"content":"Anda telah menambahkan \"Aa\" sebagai kontak imo Anda"	type":"im_fake_system"	msg_id": [illegible]
31	0	3031112419363114	Aa						Apakabar bg	[illegible]
32	0	3031112419363114	Aa					{"msg_id": [illegible]}	Baik	[illegible]
33	0	3031112419363114	Aa					{"msg_id": [illegible]}	Kau apa kabar	[illegible]
34	0	3031112419363114	Aa						Baik juga bg	[illegible]
35	0	3031112419363114	Aa						Gimana bisnisnya bg	[illegible]

Showing 1 to 10 of 29 entries

Previous 1 2 3 Next

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. ToThe 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.



Result | CSV Extractor

localhost:8080/file/result

Cetak PDF

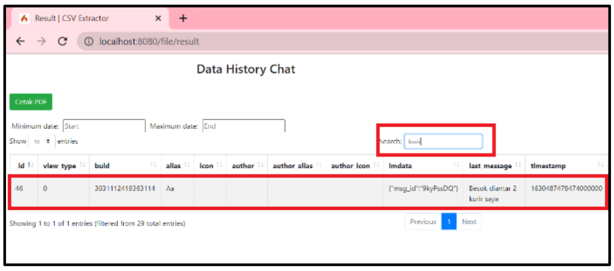
Minimum date: 01/09/2021 Maximum date: 03/09/2021

Show 10 entries Search:

_id	view_type	buid	alias	icon	author	author_alias	author_icon	imdata
27	29	3031112419363114	Aa					{"type":"added_contact"}
28	0	3031112419363114	Aa					

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 Figure19.



Result | CSV Extractor

localhost:8080/file/result

Data History Chat

Cetak PDF

Minimum date: Start Maximum date: End

Show 10 entries Search: kurir

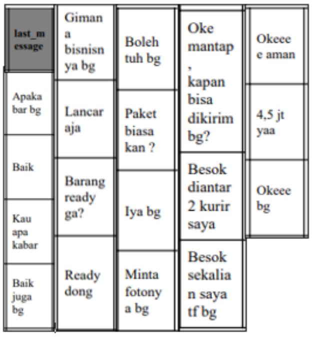
_id	view_type	buid	alias	icon	author	author_alias	author_icon	imdata	last_message	timestamp
46	0	3031112419363114	Aa					{"msg_id":"9kyPssDQ"}	Besok diantar 2 kurir saya	1630487478474000000

Showing 1 to 1 of 1 entries (filtered from 29 total entries)

Previous 1 Next

Figure19. Search Feature on CSV Reader

In Figure19the 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 inFigure20.



last_message	Gimana bisnisnya bg	Boleh tuh bg	Oke mantap , kapan bisa dikirim bg?	Okeeee aman
Apakabar bg	Lancar aja	Paket biasa kan ?	Besok diantar 2 kurir saya	4,5 jt yaa
Baik	Barang ready ga?	Iya bg	Besok sekalian saya tf bg	Okeee bg
Kau apa kabar	Ready dong	Minta fotonya bg		
Baik juga bg				

Figure20. Print PDF from CSV Reader

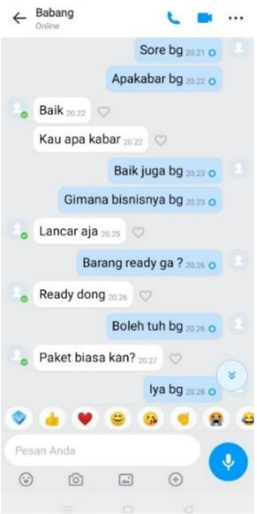
Figure20 is the output that was successfully printed on the CSV reader application in pdf format.

2.2.4 *Reporting*

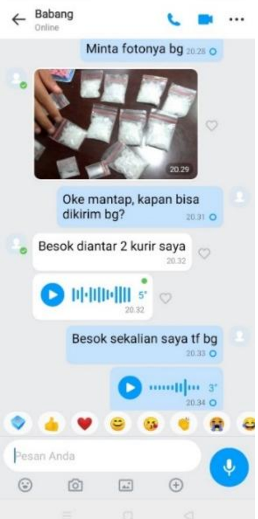
The final stage is reporting, which is reporting the results of the analysis of the investigation process and the data obtained. The report contains the results of the identification of *imaging* evidence of *smartphone* conditions in the root. The result of repotting using *DD Command* results in a *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.

Tabel 2.Findings and Evidence from Victims

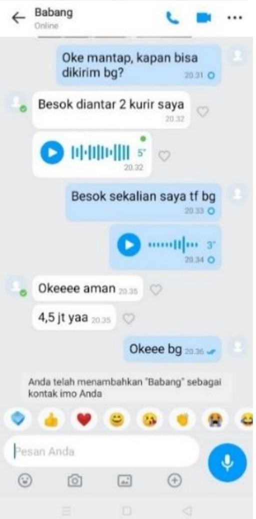
Evidence from the buyer's smartphone	Results Evidence found from the seller's smartphone



Sore bg 20.21
Apakabar bg 20.22
Baik 20.22
Kau apa kabar 20.22
Baik juga bg 20.23
Gimana bisnisnya bg 20.23
Lancar aja 20.25
Barang ready ga ? 20.26
Ready dong 20.26
Boleh tuh bg 20.26
Paket biasa kan? 20.27
Iya bg 20.28

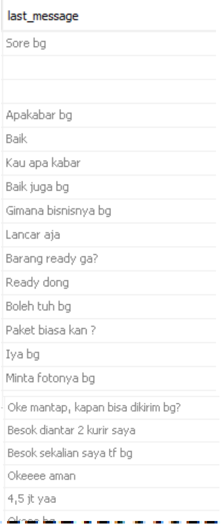


Minta fotonya bg 20.28
Oke mantap, kapan bisa dikirim bg? 20.31
Besok diantar 2 kurir saya 20.32
5" 20.32
Besok sekalian saya tf bg 20.33
3" 20.34

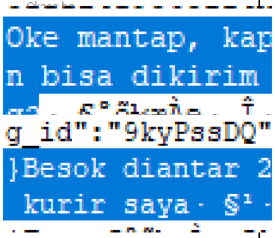


Oke mantap, kapan bisa dikirim bg? 20.31
Besok diantar 2 kurir saya 20.32
5" 20.32
Besok sekalian saya tf bg 20.33
3" 20.34
Okeeee aman 20.35
4,5 jt yaa 20.35
Okeee bg 20.36
Anda telah menambahkan "Babang" sebagai kontak imo Anda

Text Message



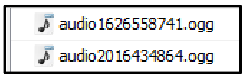
last_message
Sore bg
Apakabar bg
Baik
Kau apa kabar
Baik juga bg
Gimana bisnisnya bg
Lancar aja
Barang ready ga?
Ready dong
Boleh tuh bg
Paket biasa kan ?
Iya bg
Minta fotonya bg
Oke mantap, kapan bisa dikirim bg?
Besok diantar 2 kurir saya
Besok sekalian saya tf bg
Okeeee aman
4,5 jt yaa
Okeee bg



```
Oke mantap, kap
n bisa dikirim
g_id":"9kyPssDQ"
}Besok diantar 2
 kurir saya· §¹·
```

Image

Audio



audio1626558741.ogg
audio2016434864.ogg

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 IMOconversation *Messenger* on the buyer's smartphone. It can be shown that digital evidence obtained has similar results, such as having the same text, image, and audio messages as the IMOconversation 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.

Table 3. Comparison of ResultsObtained from Several Tools

Data Information	Software	
	Autopsy	FTK Imager
Chat	✓	✓
Images	✓	×
Audio	✓	×
Call Logs	✓	×
Contacts	✓	×

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 FTKImager 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.teknikunkris.ac.id/index.php/semnastek2019/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.*

inf., vol. 4, no. 1, p. 29–39, 2020, doi:10.22373/cj.v4i1.7241.

[5] RY Prasongko, A. Yudhana, and A. Fadil, "Forensic analysis of kakaotalk applications using the national institute standard technology method," *Semin. Nas. information. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328*, vol. 2018, no. November, p. 129–133, 2018.

[6] MS Asyaky, "Analysis and Comparison of Digital Evidence of Instant Messenger Applications on Android," *J. Researcher. Tech. information.*, vol. Vol. 3 No., No. 1, p. 220–231, 2019.

[7] D. Hariyadi and IY Pasa, "Dual Whatsapp Apps on Xiaomi Phones," *J. INTEK*, vol. 1, p. 1–7, 2018.

[8] ATB SITUNGKIR, "Juridical Review of Digital Forensics in Analyzing Digital Evidence in Criminal Acts Proof because of Law No. 11 of 2008 Junto Law N0 19 of 2016 concerning Information and Electronic Transactions, vol. 53, no. 9, p. 1689–1699, 2013.

[9] B. Raharjo, "An Overview of Digital Forensics," *J. Sociotechnology*, vol. 12, no. 29, p. 384–387, 2013, doi:10.5614/sostek.itbj.2013.12.29.3.

[10] R. Montasari, "Review and Assessment of the Existing Digital Forensic Investigation Process Models," *Int. J. Comput. app.*, vol. 147, no. 7, p. 41–49, 2016, doi:10.5120/ijca2016911194.

[11] I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, and A. Al-Omari, "Mobile Forensics," *Pract. inf. Secure.*, Thing. 297–308, 2018, doi:10.1007/978-3-319-72119-4_13.

[12] S. Madiyanto, H. Mubarok, and N. Widiyasono, "Mobile Forensics Investigation Mobile Forensics Investigation Process on IOS-Based Smartphones," *J. Rekayasa Sist. eng.*, vol. 4, no. 01, p. 93–98, 2017, doi:10.25124/jrsi.v4i01.149.

[13] IZ Yadi and YN Kunang, "National Conference on Computer Science (KONIK) 2014 Forensic Analysis on the Android Platform," *Conf. Nas. Computer Science.*, Thing. 142, 2014, [Online]. Available at: http://eprints.binadarma.ac.id/2191/.

[14] MR Setyawan, A. Yudhana, and A. Fadlil, "Identification of Skype Digital Evidence on Android Smartphones Using the National Institute Of Justice (NIJ)" *MethodSemnastek*, p. 565–570, 2019.

[15] BY Prasetyo and I. Riadi, "Investigation Cyberbullying on Kik Messenger using National Institute of Standards Technology Method," *Int. J. Comput. app.*, vol. 174, no. 17, p. 34–41, 2021, doi:10.5120/ijca2021921060.

[16] S. Lasmadi, "Arrangement of Evidence in Cybercrimes," *J. Ilmu Huk. Jambi*, vol. 5, no. 2, p. 43274, 2014.

[17] S. Gumuda, "Dynamics of the process of changes in concentration of methane in the air of ventilation currents in mines.," vol. 2, no. 2, p. 13–21, 1978.

[18] AN Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *Int. J. Comput. app.*, vol. 174, no. 18, p. 34–40, 2021, doi: 10.5120/ijca2021921076.

[19] DA Arifah, "CYBERCRIME CASE IN INDONESIA Indonesia's Cybercrime Case," *J. Bisnis and Ekon.*, vol. 18, no. 2, p. 185–195, 2011.

[20] V. Retno and G. Leri, "Data Search for Pornographic Content on Twitter Services using National Institute of Standard and Technology (NIST) Method," vol. 183, no. 24, p. 25–31, 2021.

[21] A. P. Utami, "Mobile Forensics Analysis of Line Messenger on Illegal Drug Transaction Case using National Institute of Standard Technology (NIST) Method," vol. 183, no. 32, hal. 23–33, 2021.

[22] SG Mukri, "Educational Measures for Handling Drug Abuse," *'Is*, vol. 3, no. 1, p. 25–30, 2019, doi:10.15408/is.v3i1.10983.

[23] AG Gani, "Cybercrime (Computer Based Crime)," *J. Sist. inf.*, vol. 5, no. 1, p. 16–29, 2018./article/view/18.

[24] WM Yolandi, "Legal Aspects of Narcotics Trading Transactions in the Border Areas Between the Republic of Indonesia and Malaysia," *Dedik. J. Mhs.*, vol. 1, no. 1, p. 232–249, 2020.

[25] Mustafa, I. Riadi, and R. Umar, "E-mail Forensic Investigation Design with the National Institute of Standards and Technology (NIST)," *Method9th Snst*, vol. 9, p. 121–124, 2018,

[26] MI Syahib, I. Riadi, and R. Umar, "Digital Forensic Analysis of Beetalk Applications for Cybercrime Handling Using the NIST Method," *Semin. Nas. information.*, vol. 2018, no. November, p. 134, 2018.