Forensic Mobile Drug Trafficking WhatsApp Services using National Standard of Technology Method

Afif Alhusaini
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Nowadays technology has developed very rapidly. The impact of the rapid development of technology is to increase the use of social media. One of the instant messaging applications that is currently popular and growing is WhatsApp. WhatsApp is a cross-platform instant messaging service for smartphones that use the internet to send messages. Due to the high number of Whatsapp users, there are more and more criminal acts, one of which is narcotics transactions. This research was conducted by creating conversation scenarios containing narcotics transactions carried out through the-based WhatsApp application mobile. This study aims to restore evidence of conversations containing deleted narcotics transactions by applying the forensic stages of the National Institute of Standards and Technology. The process of searching for digital evidence uses three tools forensic,MOBILedit Forensic Express, Magnet Axiom, and SysTools SQLite Viewer. Based on measurements the percentage of index numbers from each tool in the process of finding evidence, conversation data obtained a percentage of 100%, details of the time and date messages were sent and received by 67%, smartphone contact by 100%, and pictures by 33%. will be given to the court to assist in the process of enforcement and decision on lawsuits to uncover criminal cases of drug trafficking or narcotics transactions.

Keywords

Forensics, WhatsApp, Smartphone, Android, Narcotics,
Drug trafficking, NIST

1. INTRODUCTION

Today technology has experienced very rapid developments. fast. Especially during the Pandemic that is sweeping the world today, people are more active using Smartphones and Desktops to go to school or work from home. And the impact that occurs from distance schooling and working from home is to increase the use of social media. These applications have the potential to be used for a crime by using services, user data and hacking, because social media is used for various needs [1]. One of the instant messaging applications that is currently popular and growing is WhatsApp. WhatsApp is a cross-platform instant messaging service for smartphones that use the internet to send messages [2]. This application also makes it possible to send unlimited messages to contacts stored on smartphones because WhatsApp has anfeature auto syncto phone addresses [3]. This application can be used on devices with Android, iOS, Windows Phone, Windows NT, macOS, and Linux operating systems[4].App WhatsApp messenger has a positive impact, but also has a negative impact, Indonesia is one of the users of theapplication WhatsApp messengers quite a lot ofand of course will bring up irresponsible people, the sophistication of WhatsApp Many misused to commit crimes such as buying and selling drugs. The research will be carried out using the NIST (National Institute of Standards and Technology). In solving and investigatingcases Cyber Crime that occur, themethod can be used National Institute of Standards and Technology (NIST). This stage will help investigators carry out digital forensic analysis in order to obtain digital evidence on WhatsApp [5].

2. STUDY LITERATURE

2.1 Previous Study

The first previous research entitled "Forensic Analysis of Android-Based Instant Messaging Applications" in this study discusses how to get WA application data, from encrypted data into readable data which is then analyzed to be used as evidence. This study uses the SQLite Studio application to read the extracted files and see the communication that occurs in the WA application [6].

The previous study the second is entitled "Method Nist For Forensic Analysis of Digital Evidence On Android Devices" that contains a process to recover digital evidence has been erased, this process uses tools Wondersharedr.Fone For android, Oxygen Forensic Suite 2014 by using The National Institute of Standards and Technology and the results obtained are expected to be used as evidence in court trials [7].

The third previous research is entitled "Digital Forensic Analysis of Telegram Applications on Android-Based Smartphones" which has a discussion of digital forensic analysis to obtain digital evidence incases cybercrime. With digital evidence, it is hoped that it can assist in the law enforcement process to uncover responsible digital crimes in court [8].

The fourth previous study, entitled "Facebook Lite Social Media Analysis with Forensic tools using the NIST Method" in this study discussed the removal of digital evidence for the Facebook Lite application on smartphones with the Toolkit. MOBILedit Forensic Pro using themethod National Institute of Standards Technology (NIST) and digital evidence produced in the form of perpetrator accounts, audio, conversations, and images [9].

The latest previous research is entitled "Forensic Analysis of Kakaotalk Applications Using the National Institute Standard Technology Method" which discusses the analysis of digital forensic evidence to obtain digital evidence in the form of conversation histories, pictures, documents, and videos. This research uses thetool MOBILEedit Forensic and themethod National Institute of Standards Technology (NIST). The results that have been obtained are expected to help in the law enforcement process in court[10].

2.2 Digital Forensic

forensics is an activity to investigate data and determine criminal events obtained from digital devices such as computers, smartphones, tablets, PDAs, net-working devices, storage, and others [11].Digital forensics analyzes files or data in the form of audio, video, and others by obtaining from examining electronic devices to assist legal processes [12]. According to[13]digital forensics is divided into several types, namely Active data, Archival data and latent data.

2.3 Android

Android is adevice hybrid that can work as a cellphone or work as a computer but in a portable form with a display that is simpler and easier to understand [14]. Android is a mobile device with a Linux-based operating system [15].On android devices there is an Android Market that contains uploaded applications developed by developers, users can download applications in the Android Market and then install heon smartphones [16].The Google company has developed Android as an open operating system that aims to provide freedom for hardware developers and mobile operators to develop applications and operating systems. Android is designed for touch screen mobile devices such as smartphones and tablets.

2.4 Mobile Forensic

Mobile Forensics is a derivative of digital forensic science related to the recovery of digital evidence from smartphones. A smartphone is generally a term referring to cellular phones, but it can also be associated with digital devices with internal memory and communication capabilities [17].On mobile devices there is a lot of information that is used for crimes and is very useful in various legal matters, administration to investigations [7].

2.5 Digital Evidence

is the evidentiary value of stored or transmitted in digital form [18]. Digital evidence is data that is sent and stored via a mobile device or computer which can later become a tool to deny, support and provide clues to a particular crime. Retrieval of digital evidence has several steps that must pay attention to digital media as evidence, integrity and authenticity, storage location, using WriteProtect, hashes, and others. Evidence can only be accessed by certain people[7]. The process of proving evidence is a very decisive stage in a case because the results of the evidence can be known whether or not the indictment is true[19].

2.6 WhatsApp

WhatsApp is an instant messaging application whose traffic platform is smartphones. In the WhatsApp application, users can also send images, videos, locations, word documents, excel, PDF, telephone, video calls, and create stories [3]. In the WhatsApp application users can create shared chat rooms or chat groups but there is a maximum of members. WhatsApp itself is a lightweight, fast, no ads and free application. Users can use the WhatsApp application on smartphones or computers.

2.7 Cybercrime

Cybercrime is all forms of crime or the actions of someone who violates the law that utilizes the development of internet technology[20]. An action such as cybercrime can be grouped based on several types based on the motive of the activity and the modus operandi of the perpetrator. According to [21]cybercrime which can be grouped based on the mode include Unauthorized access, illegal content, virus spread, forgery, cyber espionage, cyberstalking, carding, hacking and cracker, cybersquatting and typosquatting, hijacking, infringements of privacy, an offense against intellectual property, defacing,phishing, spamming, snooping, sniffing, spoofing, pharming and malware.

2.8 Narcotic

Narcotics are drugs or substances and not classified into the types of foods that if taken, suctioned or injected can cause loss of consciousness, loss of taste, eliminate pain, and can lead to dependence [22]. According to the Narcotics Law No. 35 of 2009 narcotics are divided into three groups, namely:

"Narcotics Group I" are narcotics that can only be used for the purpose of developing science and are not used in therapeutic treatment, and have a very high potential which can lead to dependence. Types of narcotics included in Group I include: Heroin, Cocaine, Cocaine Leaves, Marijuana, and Opium.

"Narcotics Group II" is Narcotics that have efficacy for the purpose of treatment, therapy and are used as a last resort or for the purpose of developing science and have a high potential to cause dependence. Types of narcotics included in Group II include: Morphine, Pethidine and Fentanyl.

"Narcotics Group III" is Narcotics that have efficacy in the field of medicine or for the purpose of developing science and have a low potential to cause dependence. Types of narcotics included in Group III include: Codeine, Ethylmorphine, and Nicocodina.

2.9 National Institute of Standard Technology

National institute of standard technology (NIST) is a method that has standards and work policies that ensure examiners follow the same workflow until the work is documented and the results can be repeated is also maintained [5]. According to[9]in the NIST method, there are various stages of forensics, the following is an explanation of the flow of the National Institute of Standard Technology (NIST):

1. Collection
   This stage is the stage for collecting all information from data sources while maintaining data integrity.

2. Examination
   At this stage, check the processing of data that has been obtained at thestage collection automatically or manually while maintaining data integrity.

3. Analysis
   The next stage is to analyze the results of thestage Examination using methods that are legally correct and obtain reliable information.

4. Reporting
   The last stage is the reporting stage of the results of the analysis, namely describing the results of the research, the tools used, and the stages that have been carried out.

3. METHODOLOGY

3.1 Research Scenario

Article 112 of the Criminal Code stipulates that the original case or case may not be used for scientific research, because the record of a crime case is strictly confidential. Therefore, the research will be conducted using a research scenario.

This scenario is designed to illustrate how to carry out various stages of the forensic process. In this research scenario, the suspect or perpetrator uses the WhatsApp application to carry out the act of buying and selling drugs online using a cellphone or smartphone which is used as evidence in the crime case. The smartphone that became evidence was acquired using a forensic application. The suspect made a drug sale and purchase transaction, then after the transaction was successful, the perpetrator deleted the message to remove traces of the drug sale and purchase transaction. The identification of digital evidence shown in figure 1 which explains how investigators collect evidence fromdevices smartphone.

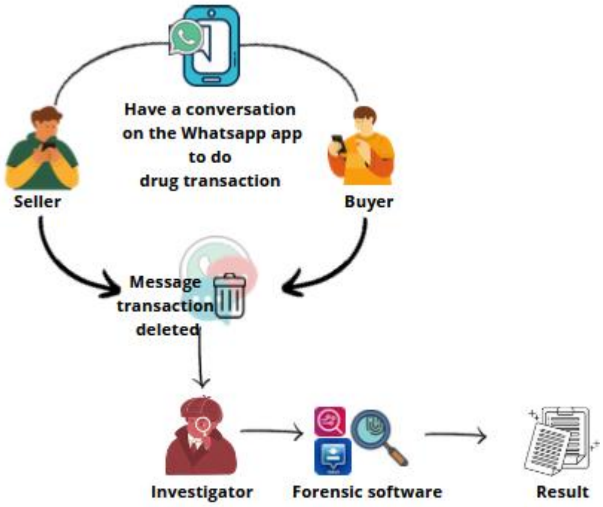


Figure 1. Research Case Simulation

In Figure 1 this case scenario uses a smartphone that has the WhatsApp Messenger application installed, which describes the perpetrators who are transacting drugs through the WhatsApp Messenger application. After transacting, the perpetrator then deletes the transaction chat so as not to leave a trace. Examination of evidence using the MOBILEdit forensic software aims to restore text messages and images that have been deleted by the perpetrator.

This case is scenariod to see how the perpetrators communicate via social media, then make transactions face-to-face somewhere. Then people who feel aggrieved by the incident report to the authorities so that can be processed immediately.

3.2 Research Stages

At the implementation stage, it is the stage where investigators carry out the forensic process according to applicable procedures. The application of the stages that are in accordance with the procedures for obtaining digital evidence in the form of forensic data will have an impact of success up to 100% [23]. The search for digital evidence refers to the Steps formulated by NIST (National Institute of Standard Technology) [24].

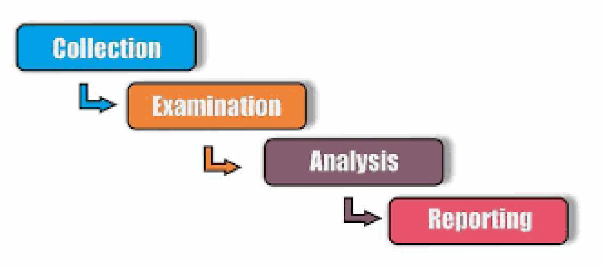


Figure 2. National Institute of Standard Technology Stage

In Figure 2 is the NIST stage consisting of the stages of collection, examination, analysis and reporting [25].

3.2.1 Collection

collection of digital evidence using the help of several tools forensicto get the desired data or files on a smartphone. There are several pieces of evidence that were successfully confiscated by the police during the investigation process, which can be seen in Table 1.

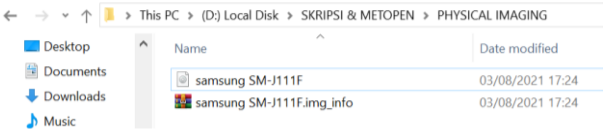
Table. 1Physical Evidence Found

No	Name of evidence	picture	description
1.	Smartphone 1		Smartphone 1 brand Samsung Galaxy J1 Ace, connected to the network, in root condition
2.	Data cable		Data cable/ Micro USB is used to connect smartphone with laptop
3.	Smartphone 2		Smartphone 2brand iphone 6s, connected to the network, not rooted

Table 1 is evidence that was confiscated by the police and will be carried out for forensics by investigators.

3.2.1.1 Collection Smartphone

The stages of theprocess smartphone collection using the MOBILedit Forensic Express Pro tools are to create a physical image that aims to perform imaging files. The results of the imaging can be seen in Figure 3.


This PC > (D:) Local Disk > SKRIPSI & METOPEN > PHYSICAL IMAGING
Desktop
Documents
Downloads
Music

Name	Date modified
samsung SM-J111F	03/08/2021 17:24
samsung SM-J111F.img_info	03/08/2021 17:24

Figure 3. The Results of the Imaging Files

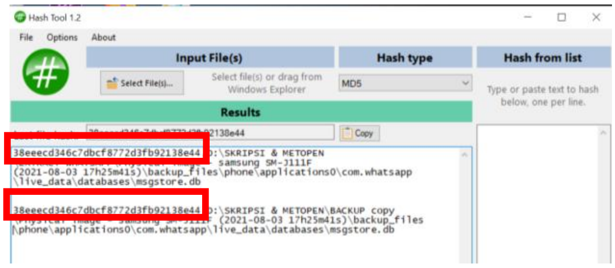
Figure 3 is a display of the results of the imaging files from the Smartphone in the root and stored in the selected directory.

3.2.2 *Examination*

This stage is the stage to prove the integrity of the data. The examination is a process to protect evidence from damage and also to find out that digital evidence has not been damaged by an irresponsible party, one way to protect the evidence from being damaged is by hashing thedata that has beenbacked up previously. The way it works is to match the data in the initial hashing result with the finalresult hashing. Theprocess of Hashing in this study will use theapplication Hash Tool. the initial stage is to copy the original folder from the backup data.

3.2.2.1 *Examination Smartphone*

Process Hashing This research carried out the results on the "" database file**msgstore**on the Smartphone which was successfully obtained during theprocess collection using the Hash Tool application.



Hash type: MD5

```
38eeecd346c7dbcf8772d3fb92138e44 D:\SKRIPSI & METOPEN
                                   samsung SM-J111F
(2021-08-03 17h25m41s)\backup_files\phone\applications0\com.whatsapp
\live_data\databases\msgstore.db

38eeecd346c7dbcf8772d3fb92138e44 D:\SKRIPSI & METOPEN\BACKUP copy
                                   F (2021-08-03 17h25m41s)\backup_files
\phone\applications0\com.whatsapp\live_data\databases\msgstore.db
```

Figure 4.The Result of Hashing the File Database

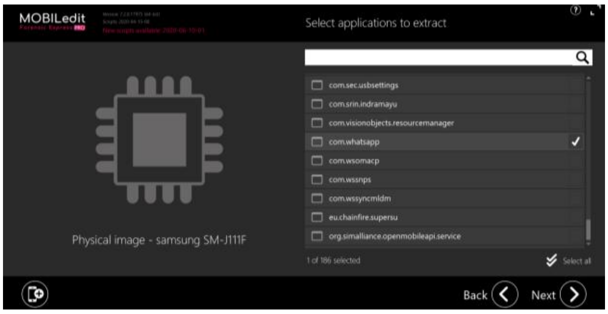
Figure 4 shows the hashed result of the MOBILEdit Forensic Express database. The red color indicates the encryption code for the file. Judging from the written file encryption code words that are displayed remain unchanged, it shows that there are no changes to the database.

3.2.3 *Analysis*

At this stage is the stage to find and collect evidence that has been collected in one case. The process of searching for evidence in the form of conversation history, pictures, videos, audio, documents, and others. Analyze the results of the examination using tools forensicsuch as MOBILedit forensic express pro, Magnet Axiom, and SysTools SQLite Viewer.

3.2.3.1 *MOBILedit Forensic Express*

The analysis process will begin by opening the tool MOBILedit Forensic Express. In this analysis process,use theoption imported data image file obtained at thestage collection. then the investigator chooses Application analysis to extract data on a particular application to be analyzed on a Smartphone. Then checklist **com.whatsappshown**, asin Figure 5.

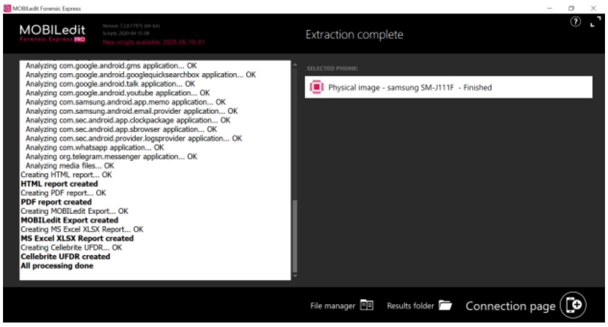

MOBILedit
Forensic Express PRO
Select applications to extract
Physical image - samsung SM-J111F
Back
Next
Select all

- ☐ com.sec.usbsettings
- ☐ com.srin.indramayu
- ☐ com.visionobjects.resourcemanager
- ☐ com.whatsapp ✓
- ☐ com.wsomacp
- ☐ com.wssnps
- ☐ com.wssyncmldm
- ☐ eu.chainfire.supersu
- ☐ org.simalliance.openmobileapi.service

1 of 186 selected

Figure 5. The Directory List on the Smartphone

will then appear the extraction process, as Figure 6.



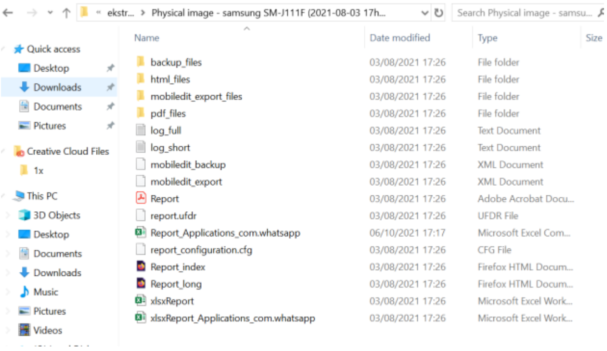
Version: 7.2.0.17975 (64-bit)
Scripts: 2020-04-15-00
New scripts available: 2020-06-10-01

Physical image - samsung SM-J111F - Finished

```
  Analyzing com.google.android.gms application... OK
  Analyzing com.google.android.googlequicksearchbox application... OK
  Analyzing com.google.android.talk application... OK
  Analyzing com.google.android.youtube application... OK
  Analyzing com.samsung.android.app.memo application... OK
  Analyzing com.samsung.android.email.provider application... OK
  Analyzing com.sec.android.app.clockpackage application... OK
  Analyzing com.sec.android.app.sbrowser application... OK
  Analyzing com.sec.android.provider.logsprovider application... OK
  Analyzing com.whatsapp application... OK
  Analyzing org.telegram.messenger application... OK
  Analyzing media files... OK
Creating HTML report... OK
HTML report created
Creating PDF report... OK
PDF report created
Creating MOBILedit Export... OK
MOBILedit Export created
Creating MS Excel XLSX Report... OK
MS Excel XLSX Report created
Creating Cellebrite UFDR... OK
Cellebrite UFDR created
All processing done
```

Figure 6.Display of the Extraction Process is Complete.

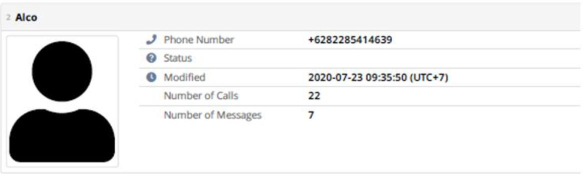
After the process is complete, the results of data extraction on the smartphone will be saved automatically in the storage folder selected by the investigator.



Name	Date modified	Type	Size
backup_files	03/08/2021 17:26	File folder	
html_files	03/08/2021 17:26	File folder	
mobiledit_export_files	03/08/2021 17:26	File folder	
pdf_files	03/08/2021 17:26	File folder	
log_full	03/08/2021 17:26	Text Document	
log_short	03/08/2021 17:26	Text Document	
mobiledit_backup	03/08/2021 17:26	XML Document	
mobiledit_export	03/08/2021 17:26	XML Document	
Report	03/08/2021 17:26	Adobe Acrobat Docu...	
report.ufdr	03/08/2021 17:26	UFDR File	
Report_Applications_com.whatsapp	06/10/2021 17:17	Microsoft Excel Com...	
report_configuration.cfg	03/08/2021 17:26	CFG File	
Report_index	03/08/2021 17:26	Firefox HTML Docum...	
Report_long	03/08/2021 17:26	Firefox HTML Docum...	
xlsxReport	03/08/2021 17:26	Microsoft Excel Work...	
xlsxReport_Applications_com.whatsapp	03/08/2021 17:26	Microsoft Excel Work...	

Figure 7. Extracted Data Folder

Extracted fromFigure 7 is the result of the data extraction process, there are several types of files including, backup files, exel files, folder html, files,mobileditt export files, Txtfile, XML document, CFG file, HTML document, MS excel worksheet, PDF files.

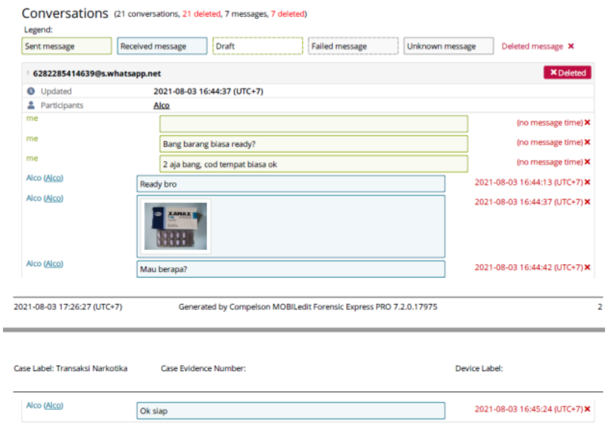


2 Alco

Phone Number	+6282285414639
Status	
Modified	2020-07-23 09:35:50 (UTC+7)
Number of Calls	22
Number of Messages	7

Figure 8. Display of Contact Information

Figure 8 shows the display ofinformation contact suspected of being the seller of the drug which contains information on the seller's name, phone number, and others.



Conversations (21 conversations, 21 deleted, 7 messages, 7 deleted)

Legend:

6282285414639@s.whatsapp.net ✖Deleted

Updated 2021-08-03 16:44:37 (UTC+7)

Participants Alco

me		(no message time) ✖
me	Bang barang biasa ready?	(no message time) ✖
me	2 aja bang, cod tempat biasa ok	(no message time) ✖
Alco (Alco)	Ready bro	2021-08-03 16:44:13 (UTC+7) ✖
Alco (Alco)		2021-08-03 16:44:37 (UTC+7) ✖
Alco (Alco)	Mau berapa?	2021-08-03 16:44:42 (UTC+7) ✖

2021-08-03 17:26:27 (UTC+7) Generated by Compelson MOBILedit Forensic Express PRO 7.2.0.17975 2

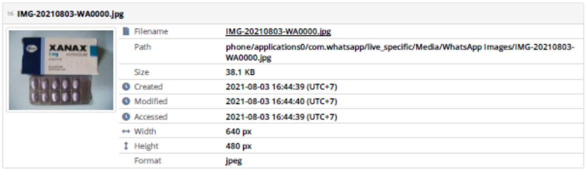
Case Label: Transaksi Narkotika Case Evidence Number: Device Label:

Alco (Alco)	Ok siap	2021-08-03 16:45:24 (UTC+7) ✖

Figure 9. View of Deleted Conversations

Figure 9 shows sent messages (green box) that have been deleted and received messages (blue boxes) that have been deleted. In addition, there is information on the time when the resulting conversation also appears on the right side of the header, in the description of the time using UTC+7 (Uoordinated Universal Time) which is the same as WIB (Western Indonesian Time).

Another file obtained is in the form of an image file that can help strengthen that the two perpetrators actually committed a narcotics transaction crime as shown in Figure 10.



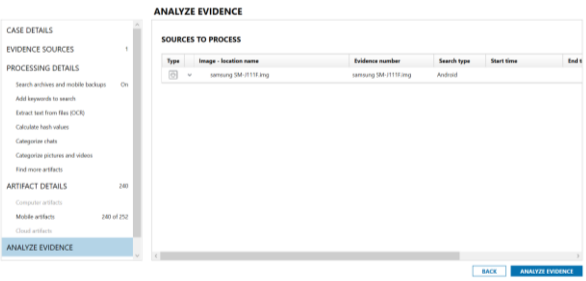
16 IMG-20210803-WA0000.jpg

Filename	IMG-20210803-WA0000.jpg
Path	phone/applications0/com.whatsapp/live_specific/Media/WhatsApp Images/IMG-20210803-WA0000.jpg
Size	38.1 KB
Created	2021-08-03 16:44:39 (UTC+7)
Modified	2021-08-03 16:44:40 (UTC+7)
Accessed	2021-08-03 16:44:39 (UTC+7)
Width	640 px
Height	480 px
Format	jpeg

Figure 10.Image Files that Have Been Deleted

3.2.3.2 *Magnet Axiom*

The analysis phase using the Magnet Axiom Process tools is carried out by analyzing the processed folders backup data smartphone obtained from theprocess physical image using the MOBILedit forensic express tool . first select the image file to be analyzed, the file to be analyzed is located in the "D:\SKRIPSI & METOPEN\PHYSICAL IMAGING" folder with the file name "Samsung SM-J111F.img", which can be seen in the Figure 11.



ANALYZE EVIDENCE

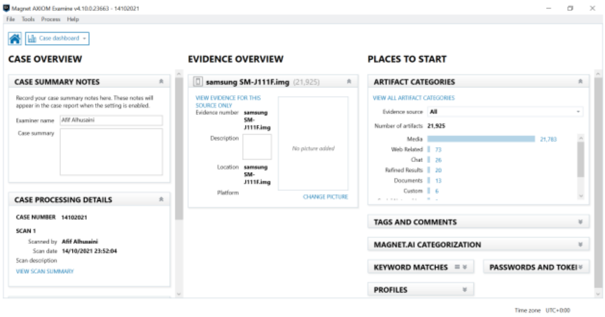
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR)
Calculate hash values
Categorize chats
Categorize pictures and videos
Find more artifacts
Computer artifacts
Mobile artifacts 240 of 252
Cloud artifacts

SOURCES TO PROCESS

Type	Image - location name	Evidence number	Search type	Start time	End t
	samsung SM-J111F.img	samsung SM-J111F.img	Android		

Figure 11. Display AnalyzeEvidence of Magnet Axiom

Analyze after the analysis process is complete, it will be transferred to thesection magnetic axiom examination to view reports on evidence obtained in the analysis process in the magnet axiom process.The display after the analysis process is complete can be seen in Figure 12.



Magnet AXIOM Examine v4.10.0.23663 - 14102021

Record your case summary notes here. These notes will appear in the case report when the setting is enabled.

Examiner name Afif Alhusaini

Case summary

CASE NUMBER 14102021

SCAN 1

Scanned by Afif Alhusaini

Scan date 14/10/2021 23:52:04

Scan description

samsung SM-J111F.img (21,925)

Evidence number samsung SM-J111F.img

Description

Location samsung SM-J111F.img

Platform

No picture added

Evidence source All

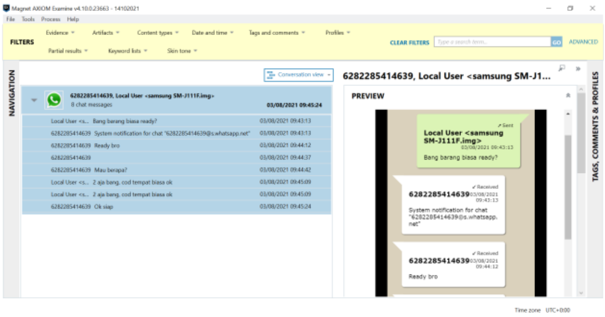
Number of artifacts 21,925

Media	21,783
Web Related	73
Chat	26
Refined Results	20
Documents	13
Custom	6

Time zone UTC+0:00

Figure 12. Display Magnet Axiom Examination

After the results of the analysis process are saved automatically into the storage folder, which is in the directory that has been selected by the investigator. Conversations that have been deleted have been successfully restored bytools Magnet Axiom, and there is also information about user numbers, conversation times, and conversation dates. Conversations that have been successfully recovered along with a description of the time the messages were sent and received are shown in Figure 13.



Magnet AXIOM Examine v4.10.0.23663 - 14102021

6282285414639, Local User <samsung SM-J111F.img>
8 chat messages 03/08/2021 09:45:24

Local User <s...	Bang barang biasa ready?	03/08/2021 09:43:13
6282285414639	System notification for chat "6282285414639@s.whatsapp.net"	03/08/2021 09:43:13
6282285414639	Ready bro	03/08/2021 09:44:12
6282285414639		03/08/2021 09:44:37
6282285414639	Mau berapa?	03/08/2021 09:44:42
Local User <s...	2 aja bang, cod tempat biasa ok	03/08/2021 09:45:09
Local User <s...	2 aja bang, cod tempat biasa ok	03/08/2021 09:45:09
6282285414639	Ok siap	03/08/2021 09:45:24

6282285414639, Local User <samsung SM-J1...

Sent
Local User <samsung SM-J111F.img> 03/08/2021 09:43:13
Bang barang biasa ready?

Received
6282285414639 03/08/2021 09:43:13
System notification for chat "6282285414639@s.whatsapp.net"

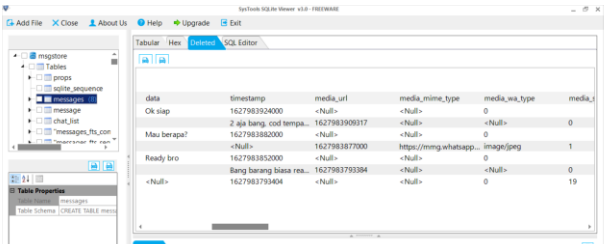
Received
6282285414639 03/08/2021 09:44:12
Ready bro

Time zone UTC+0:00

Figure 13. The Conversation was Successfully Restored

3.2.3.3 *SysTools SQLite Viewer*

The analysis process was carried out to obtain evidence contained in thesmartphone perpetrator'susing thetool SysTools SQLite Viewer by analyzingfiles database and databases journals that were stored during theprocess data backup. the next step is to select the "**Messages"**to display the conversations between the perpetrator and the victim, the conversations that have been successfully displayed are shown in Figure 14.



SysTools SQLite Viewer v3.0 - FREEWARE

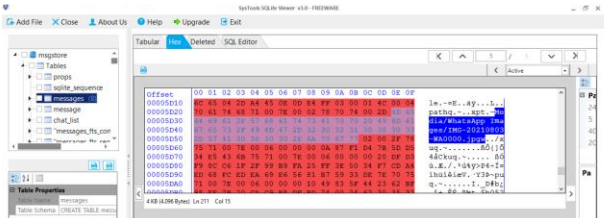
Table Name messages

Table Schema CREATE TABLE mess

data	timestamp	media_url	media_mime_type	media_wa_type	media_s
Ok siap	1627983924000	<Null>	<Null>	0	
	2 aja bang, cod tempa...	1627983909317	<Null>	<Null>	0
Mau berapa?	1627983882000	<Null>	<Null>	0	
	<Null>	1627983877000	https://mmg.whatsapp...	image/jpeg	1
Ready bro	1627983852000	<Null>	<Null>	0	
	Bang barang biasa rea...	1627983793384	<Null>	<Null>	0
<Null>	1627983793404	<Null>	<Null>	0	19

Figure 14.Display of Deleted Conversations

Other digital evidence found in the form of the location of deleted images contained in smartphone, such as Figure 15.


SysTools SQLite Viewer v3.0 - FREEWARE

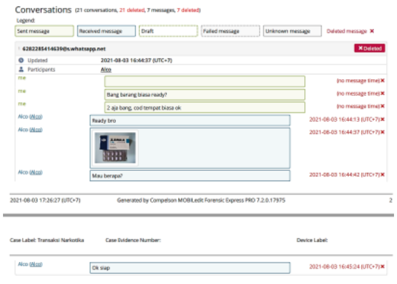
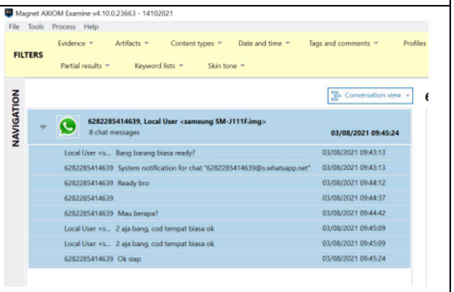
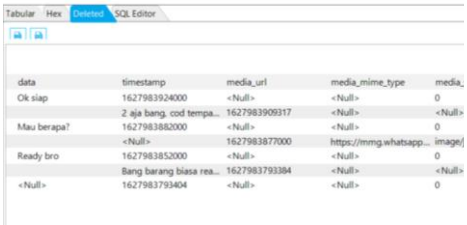
```
Offset    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00005D10  6C 65 04 2D A4 45 0E 0D E4 FF 03 00 01 4C 00 04   le.-¤E..äÿ...L..
00005D20  70 61 74 68 71 00 7E 00 02 78 70 74 00 2D 4D 65   pathq.~..xpt.-Me
00005D30  64 69 61 2F 57 68 61 74 73 41 70 70 20 49 6D 61   dia/WhatsApp Ima
00005D40  67 65 73 2F 49 4D 47 2D 32 30 32 31 30 38 30 33   ges/IMG-20210803
00005D50  2D 57 41 30 30 30 30 2E 6A 70 67 77 02 00 2F 78   -WA0000.jpgw../x
00005D60  75 71 00 7E 00 06 00 00 00 0A 87 F1 D4 7B 5D D5   uq.~.......ñÔ{]Õ
00005D70  34 E5 43 6B 75 71 00 7E 00 06 00 00 00 20 DF D3   4åCkuq.~..... ßÓ
00005D80  F9 8C C6 1F 2F 99 B9 FA 25 FF 3E 50 34 F7 CD A4   ù.Æ./.¹ú%ÿ>P4÷Í¤
00005D90  ED 68 FC ED EA 69 E6 56 81 B7 59 33 DE 7E 70 75   íhüíêiæV.·Y3Þ~pu
00005DA0  71 00 7E 00 06 00 00 00 10 49 63 5F 44 23 62 BF   q.~......Ic_D#b¿
4 KB (4,096 Bytes)  Ln 211  Col 15
```

Figure 15. Location of Deleted Images

3.2.4 Reporting

Reporting is the final stage which aims to show data from the collection, examination, and analysis processes that have been found by investigators. Digital evidence collection reports were generated from the MOBILedit Forensic Express Pro tools, Magnet Axiom, and SysTools SQLite Viewer. Each tool has different results. The findings of digital evidence can be seen in table 2.

Table. 2The Findings of Digital Evidence

NO	Digital Evidence Finding	
1	Tool MOBIL edit forensic express	 Conversations (21 conversations, 21 deleted, 7 messages, 7 deleted) Legend: Sent message · Received message · Draft · Failed message · Unknown message · Deleted message × 6282285414639@s.whatsapp.net ✖ Deleted Updated 2021-08-03 16:44:37 (UTC+7) Participants Alco me — (no message time) × me — Bang barang biasa ready? — (no message time) × me — 2 aja bang, cod tempat biasa ok — (no message time) × Alco (Alco) — Ready bro — 2021-08-03 16:44:13 (UTC+7) × Alco (Alco) — 2021-08-03 16:44:37 (UTC+7) × Alco (Alco) — Mau berapa? — 2021-08-03 16:44:42 (UTC+7) × 2021-08-03 17:26:27 (UTC+7) Generated by Compelson MOBILedit Forensic Express PRO 7.2.0.17975 2 Case Label: Transaksi Narkotika Case Evidence Number: Device Label: Alco (Alco) — Ok siap — 2021-08-03 16:45:24 (UTC+7) ×
2	Tool Magnet Axiom	 Magnet AXIOM Examine v4.10.0.23663 - 14102021 6282285414639, Local User <samsung SM-J111F.img> — 8 chat messages — 03/08/2021 09:45:24 Local User <s... Bang barang biasa ready? 03/08/2021 09:43:13 6282285414639 System notification for chat "6282285414639@s.whatsapp.net" 03/08/2021 09:43:13 6282285414639 Ready bro 03/08/2021 09:44:12 6282285414639 03/08/2021 09:44:37 6282285414639 Mau berapa? 03/08/2021 09:44:42 Local User <s... 2 aja bang, cod tempat biasa ok 03/08/2021 09:45:09 Local User <s... 2 aja bang, cod tempat biasa ok 03/08/2021 09:45:09 6282285414639 Ok siap 03/08/2021 09:45:24
3	Tool SysTool SQLite Viewer	 data · timestamp · media_url · media_mime_type · media_ Ok siap · 1627983924000 · <Null> · <Null> · 0 · 2 aja bang, cod tempa... · 1627983909317 · <Null> · <Null> Mau berapa? · 1627983882000 · <Null> · <Null> · 0 · <Null> · 1627983877000 · https://mmg.whatsapp... · image/ Ready bro · 1627983852000 · <Null> · <Null> · 0 · Bang barang biasa rea... · 1627983793384 · <Null> · <Null> <Null> · 1627983793404 · <Null> · <Null> · 0

From the table above, the findings of evidence in the form of deleted conversations were successfully obtained from the forensic process carried out by investigators that matched the evidence conversation from the victim, which later the digital evidence will be used as supporting evidence in the court process by adding other evidence findings.

3.2.5 The Results

after testing with various forensic tools, a comparison of the results of digital evidence can be obtained which can be seen in Table 3.

Table. 3Comparison of The Findings of The Digital Evidence

Tools	Result of Digital Evidence			
	Deleted conversation	Image	Time and date the message was sent and received	Smartphone contact
MOBILedit Forensic Express	✓	✓	✓	✓
Magnet Axiom	✓	×	✓	✓
SysTools SQLite Viewer	✓	×	×	✓

The comparison table aims to see the final results obtained from the research process using several tools and the differences in the results of the goods evidence of the two smartphones perpetrators'. Basically the results of several forensic tools used are thetool Mobiledit Forensic Express which successfully generates evidence of conversation, location, time, user info, contacts and pictures.Tool Axiom's Magnet managed to get proof of the conversation that had been deleted but was unable to restore the sent image.tool SysTools SQLite Viewer that successfully generates evidence of conversation, image url and location of the storage folder suspected as evidence of a crime. This will be used as support for digital evidence in criminal cases to increase sanctions in court.

4. CONCLUSION

The digital forensic process carried out on drug trafficking crimes or illegal narcotics transactions on mobile-based WhatsApp services has succeeded in obtaining digital evidence in the form of deleted text conversations on Smartphones using the MOBILedit Forensic Express tools, Magnet Axiom, and SysTools SQLite Viewer. The process of finding evidence in the research carried out refers to the NIST (National Institute of Standard and Technology) stage with four stages in it, namely collection, examination, analysis, and reporting. Proofwas obtained using three forensic tools and obtained different results. Smartphones byrooting get complete digital evidence results. Based on the measurement of the percentage index number of each tool in the process of finding evidence, the conversation data got a percentage of 100%, the details of the time and date of messages sent and received by 67%, smartphone contact by 100%, and images by 33%. The digital evidence will be used as supporting evidence in the court process by adding other evidence findings.

5. REFERENCES

[1] A. Fauzan, I. Riadi, and A. Fadlil, “Digital Forensics Analysis on Line Messenger for Cybercrime Handling,” vol. 2, no. 1, pp. 159–163, 2016.

[2] N. Anwar and I. Riadi,“Forensic Investigation Analysis of WhatsApp Messenger Smartphones Against Web-Based WhatsApp,” *J. Ilm. Tech. Electrical Computing. and Information.*, vol. 3, no. 1, p. 1, 2017, doi:10.26555/jiteki.v3i1.6643.

[3] Y. N. Kunang and A. Khristian, “Implementation of Forensic Procedures for Whatsapp Artifact Analysis on

Android Phones," vol. 2, no. 1, pp. 59–68, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[4] I. G. Ngurah, G. Wicaksana, and I. K. G. Suhartana, "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method," vol. 8, no. 4, pp. 381–385, 2020.

[5] P. Widiandana, I. Riadi, and Sunardi,"Forensic Investigation Analysis of Cyberbullying on Whatsapp Messenger Using the NIST Method," *Semin. Nas. Teknol. Fak. Tekinik Univ. Krisnadwipayana*, pp. 488–493, 2019, [Online]. Available: https://jurnal.teknikunkris.ac.id/index.php/semnastek2019/article/view/308.

[6] G. M. Zamroni, R. Umar, and I. Riadi, "Forensic Analysis of Android-Based Instant Messaging Applications," vol. 2, no. 1, pp. 102–105, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[7] R. Umar and Sahiruddin, , "Nist Method For Forensic Analysis of Digital Evidence on Android Devices,"*Pros. SENDU_U_2019*, pp. 978–979, 2019.

[8] I. S. Wijaya, H. Riadi, "Digital Forensic Analysis of Telegram Applications,"*Semantikom*, pp. 95–98, 2017.

[9] R. A. Bintang, R. Umar, and A. Yudhana,"Facebook Lite Social Media Analysis with Forensic tools using the NIST Method," *Techno (Journal of Faculty of Technology, Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.

[10] R. Y. Prasongko, A. Yudhana, and A. Fadil,"Forensic analysis of kakaotalk application using national institute standard technology method," *Semin. Nas. Inform. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328*, vol. 2018, no. November, pp. 129–133, 2018.

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

[12] R. Adijisman and I. Riadi, "An Overview of Digital Forensics," vol. 183, no. 29, pp. 41–48, 2021.

[13] N. Anggraini *et al.*, "Forensic Analysis of Whatsapp Messenger on Android Smartphones," vol. XII, no. 1, pp. 83–100, 2020.

[14] I. Z. Yadi and Y. N. Kunang, "2014 National Conference on Computer Science (KONIK) Forensic Analysis on the Android Platform,"*Konf. Nas. Ilmu Komput.*, p. 142, 2014, [Online]. Available: http://eprints.binadarma.ac.id/2191/.

[15] S. M. Dusu, "Mobile Forensic of Facebook Services using National Institute of Standard Technology (NIST) Method," vol. 183, no. 33, pp. 9–15, 2021.

[16] I. Riadi, A. Yudhana, and M. Al Barra, "Mobile Forensics on LinkedIn Social Media Services,"*JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 6, no. 1, p. 9, 2021, doi: 10.14421/jiska.2021.61-02.

[17] S. Pambayun and I. Riadi, "Investigation on Instagram Android-based using Digital Forensics Research Workshop Framework," *Int. J. Comput. Appl.*, vol. 175, no. 35, pp. 15–21, 2020, doi: 10.5120/ijca2020920904.

[18] D. A. Putri, "Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method," vol. 183, no. 30, pp. 1–8, 2021.

[19] C. Handoko, "The Position of Digital Evidence in Cybercrime Evidence in Court," *J. Jurisprud.*, vol. 6, no. 1, p. 1, 2017, doi: 10.23917/jurisprudence.v6i1.2992.

[20] M. Rifauddin and A. N. Halida, , "Cybercrime Alerts and Hoax Information on Facebook Social Media,"*Khizanah al-Hikmah J. Ilmu Perpustakaan, Informasi, dan Kearsipan*, vol. 6, no. 2, p. 98, 2018, doi: 10.24252/kah.v6i2a2.

[21] E. Ketaren, "Cybercrime, Cyber Space, dan Cyber Law," *Times*, vol. 5, no. 2, pp. 35–42, 2016, [Online]. Available: http://stmik-time.ac.id/ejournal/index.php/jurnalTIMES/article/viewFile/556/126.

[22] B. P. Hariyanto, "Prevention and Eradication of Drug Trafficking in Indonesia," *J. Daulat Huk.*, vol. 1, no. 1, pp. 201–210, 2018, doi: 10.30659/jdh.v1i1.2634.

[23] R. Sistem *et al.*, "Journal of rest," vol. 1, no. 10, pp. 820–828, 2021.

[24] M. I. Syahib, I. Riadi, and R. Umar, "Acquisition of Digital Evidence for Viber Applications Using the National Institute of Standards Technology (NIST) Method,"*J-SAKTI (Jurnal Sains Komput. dan Inform.*, vol. 4, no. 1, p. 170, 2020, doi: 10.30645/j-sakti.v4i1.196.

[25] S. D. Utami, C. Carudin, and A. A. Ridha,"Live Forensic Analysis on Whatsapp Web for Proof Electronic Transaction Fraud Cases,"*Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[26] C. K. Herawati, "Forensic Browser on Facebook Services using National Institute of Standards Technology Method," vol. 183, no. 30, pp. 17–24, 2021.