International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 89-97
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001

Forensic Analysis of Android-based WhatsApp Messenger Against Fraud Crime Using The National Institute of Standard and Technology Framework

Helmy Trisnasenjaya [1], Imam Riadi[2]
[1] *Departement of Informatics, Universitas Ahmad Dahlan*, Yogyakarta, Indonesia
[2] *Department of Information System, Universitas Ahmad Dahlan*, Yogyakarta, Indonesia
(helmy1400018177@webmail.uad.ac.id, imam.riadi@is.uad.ac.id)

ABSTRACT

Mobile devices developed very rapidly along with the development of technology. Improved service users instant messenger applications such as WhatsApp would be very susceptible to crime. Some crimes such as pornography, premeditated murder and fraud, in the case involving technologies that serve as the digital evidence in court, either in the form of conversations, pictures, video recordings, and other chat messages originating from the application WhatsApp. The method used in this study using National Institute of Standards and Technology (NIST). The NIST method has four stages as a reference for the analysis of evidence, namely the collection, examination, analisis and reporting. Stages are used to process the data security of the physical evidence found and to prove the perpetrator. Analysis of the NIST investigation process has stages that have been modified so that it can adjust to the investigation procedure initiated on the seizure of evidence until the discovery process digital data from the evidence in the case of fraudulent crimes using WhatsApp application. The study produced the information stored in the database in the form of data artifacts that the contents of the conversation chat messages, log history of delivery, phone number, and a conversation then based on these data to get items of digital evidence which subsequently became a reference in the proceedings to determine the punishment for the perpetrators of fraud

Keywords: *WhatsApp, Android, Forensic, Mobile,* NIST

I. INTRODUCTION

Mobile devices are experiencing rapid growth along with technological developments. Mobile devices are slowly beginning to replace the role of computers with the increasing number of features and applications available on mobile devices, until February 2016, there are 1 billion active users per month. The number has increased compared to the number of What users in January 2015 which as many as 700 million active users each month. WA every day serving the delivery of messages as much as 42 Billion [1]·

WhatsApp also provides security holes for the privacy of users one of which is tapping a conversation that involves both devices smartphones and computers.The handling of crimes involving digital devices should be emphasized so as to assist the judicial process for its effects. The Digital Forensics investigation contributes to the abuse of WhatsApp Instant messaging service features such as the investigation of the handling of the WhatsApp conversation tapping through a series of standard steps in accordance with digital forensics procedures [2].

The supporting framework used to perform forensic mobile analysis of the evidence is by NIST framework (National Institute of Standards Technology).The NIST framework has four stages for the analysis of evidence with stages of collection, examination, analysis, reporting [3]. The framework used can indeed produce the required data, but in obtaining an information cannot define the encryption used in the WhatsApp message [4].

II. LITERATURE REVIEW

2.1 Digital Forensics

Forensics is an activity to conduct investigations and establish facts relating to criminal activity and other legal matters. Forensics is part of the science that encompasses the discovery and investigation of data found on digital devices (computers, handphones, smartphones, tablets, storage and the like), in which case digital forensics can be divided into computer-related forensics (host, server), applications (including databases), and devices (digital devices). Each of them has its own deepening [5].

Digital forensics can be said to be a scientific framework in system development to identify, locate, retrieve, and analyze evidence from computers, computer storage media, and other electronic devices and present the findings in a court case. Digital forensics can also be interpreted as the collection and analysis of data from various computers of computer power including computer systems, computer networks, communication lines, and appropriate storage media to be presented in court [6].

2.2 WhatsApp Messenger Forensics

Live memory has different goals and needs while doing forensic activities.This framework can get forensic information when an event has ended or can be categorized as we search for information with the help of log/history database of WhatsApp application.Using this framework is very easy and requires only log/history database written in the smartphone with the help of tools. In Figure 1 shows illustrates the Forensic WhatsApp frameworkology using Live Memory [4].

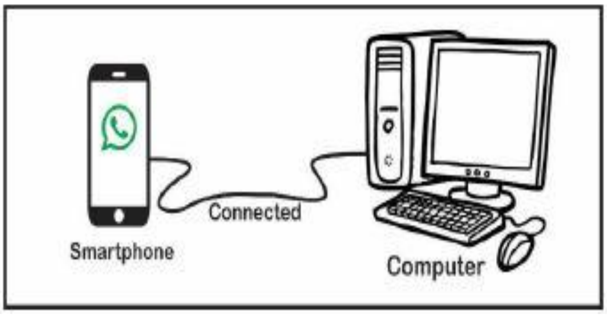


Figure 1 Forensic WhatsApp Framework Using Live Memory.

The simulation design of WhatsApp conversational tapping described the WhatsApp application testing scheme as in this case concerning the existence of digital evidence after interception occurred. In Figure 2 shows the response to each application between WhatsApp on Smartphone to WhatsApp.

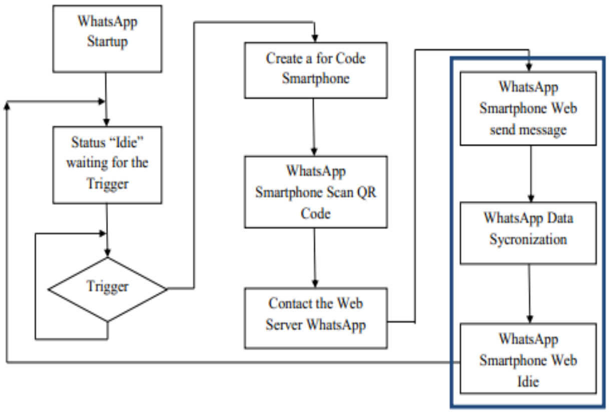

WhatsApp Startup
Status "Idle" waiting for the Trigger
Trigger
Create a for Code Smartphone
WhatsApp Smartphone Scan QR Code
Contact the Web Server WhatsApp
WhatsApp Smartphone Web send message
WhatsApp Data Sycronization
WhatsApp Smartphone Web Idie

Figure 2 WhatsApp Attack Workflow [2]

WhatsApp conversation intercepts from Image above are focused on synchronizing data on WhatsApp data on a smartphone or on a web browser, then the two applications can access each other simultaneously and identically.

2.3 Mobile Forensics

Mobile forensic devices data taken from the phone by itself can be used as evidence.This evidence can be the foundation when investigating a case by law enforcement agencies. There is some evidence that can be extracted from the phone. The types of evidence that can be extracted from the phone include contact numbers, call logs, SMS messages, audio files, emails, and internet history. These artifacts can be extracted by either logical or physical frameworks. Logically it is extracted with the device using some special tools. Software or tools that can extract these artifacts are very limited. So forensic investigators will find it difficult to carry out this work in a timely fashion [7].

2.4 Digital Evidence

Digital evidence is information stored or sent in a binary form that can be judged in court. These can be found on computer hard drives, mobile phones, personal digital assistants (PDA), CD, and flash card on digital cameras, among other places. Digital evidence is generally fraught with digital or electronic crimes, such as pornography, prostitution, identity theft, phishing, or fraud in the form of credit cards or ATM. However, digital evidence is now used to prosecute all types of crimes, not just digital crimes [9].

2.5 Android

Android is an operating system (OS) developed by open handset alliance (OHA). The basic architecture of Android is shown to be built based on Linux 2.6 kernel. With Linux in flash, however, a flash transition layer provides system device functionality. A Memory Technology Device is required to provide an interface between a Linux OS and a physical flash device [10].

2.6 User Acceptance Testing (UAT)

User Acceptance Testing is used to indicate the final use of software testing performed before new information is introduced to an organization. The main purpose of the UAT is to replace the new system doing what it is set to do and meet the requirements that the business has [11].

2.7 Cybercrime

Another definition of cybercrime is a crime that uses information technology as an instrument or target and forensic digital essentially answers the question of when, what, who, where, how, and why related to digital crime [12]. There is a lot of cyberspace in the cyber world, including cyberbullying, the term refers to the use of information technology to bully people to send or post the text in order to intimidate or threaten others [13].

III. RESEARCH METHOD

The framework used to perform analysis of digital evidence or stages to obtain information from the digital evidence is by the National Institute of Standards and Technology (NIST) framework [3].The framework recommends a basic stage in the forensic process as shown in Figure 3.

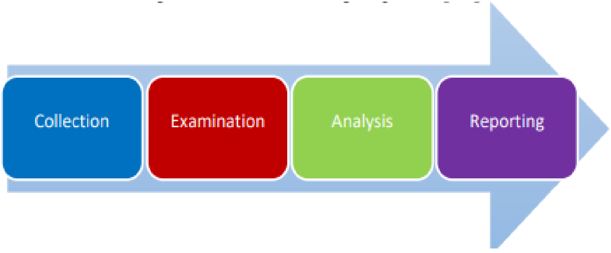


Figure 3 Stages of Frameworks National Institute of Standards and Technology (NIST) [8].

Stages of research are the stage where simulations can be performed from a case research to try to locate a criminal on WhatsApp application based on chat message conversations.With a variety of simulations and stages conducted aiming to perform mobile forensic implementation of the analysis results in identifying the perpetrators in a criminal case using WhatsApp then it can be conclude the perpetrator who sent the chat message [14].

The National Institute of Standards and Technology (NIST) framework recommends a basic stage in the forensic process, namely collection, examination, analysis, and reporting [15].

a) Collection. The first phase in the process is to identify, label, record, and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections, as well as losing data from battery-powered device

b) Examination. Examinations involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest, while preserving the integrity of the data.

c) Analysis. The next phase of the process is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

d) Reporting. The final phase is reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation

IV. RESULTS AND DISCUSSION

At the first stage forensic mobile is done to find evidence (evidence) including the smartphone by the perpetrator. Then for the next stage, for the next stage can be described as follows:

1) Collection

In this phase is the initial stage of the search, data collection, and documentation of evidence, furthermore, in this research, the sample of evidence analyzed in the form of a smartphone that is the scenario as evidence in a criminal case of fraud through the WhatsAap Messenger application. Table 1 shows the result of documentation and specifications of evidence

Table 1 Evidence Specification Table (Evidence)

Brand	Series	Model number	Imei	OS Version
Evercros	SANZDWKB6RG 7TTGSOV8	A28A	3576730 823619	4.4.4
Huawei	Honor 4C	CHM-001	8667780 2020131 9	5.1.1

On a smartphone to get the desired digital artifact with the condition of WhatsApp aplication in the condition of a smartphone that is already in the root with inactive screen security feature. Because to allow users to have full access to the system so that it will have more control for the settings, but for smartphones that are rooted should not be permanently at risk of altering evidence and may result in deleted data [16].

2) Examination

In the acquisition, a stage is done imaging process which where each smartphone will be a different way of process imaging in accordance with the operating system and mobile devices used and different characteristics.

a) Early Smartphone Detection with FTK Imager application

In Table 2 shows smartphone 1 and 2 are already in root condition, but which can be detected by FTK Imager only smartphone 1 by activating USB Debugging and the smartphone is detected on ADB.

Table 2 Preliminary Process of Smartphone Detection with FTK Imager using USB

	Password Protection	Security Screen	Protocol Transfer	Eksternal Memory	Internal Memory
Smartphone 1	No	No	MTP	Detected	Detected
Smartphone 2	No	No	MTP	Not Detected	Not Detected

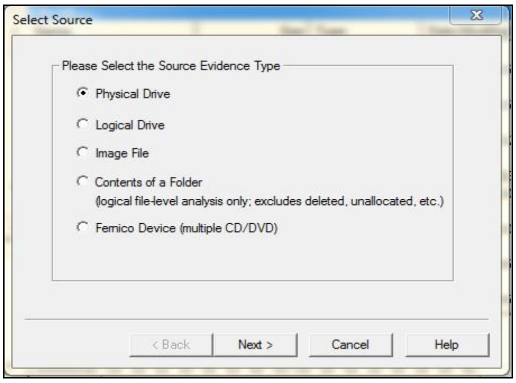
While on smartphone 2 can’t be detected in ADB, but can enable USB Debugging. This is due to the condition of smartphones and root privileges of smartphones and the less supportive types of vendors.

b) Imaging process smartphone

In this process imaging using a tool one of them is tools FTK Imager as a tool for the process of copying data on the smartphone and one way to secure the evidence so that the data we analyzed can be compared with the original in addition to FTK. To do imaging all the files residing in the smartphone but to get more smartphone permissions must be in the root state.

i. Imaging process on smartphone 1 using FTK Imager

Process in Figure 4 shows determine the file to be in imaging.



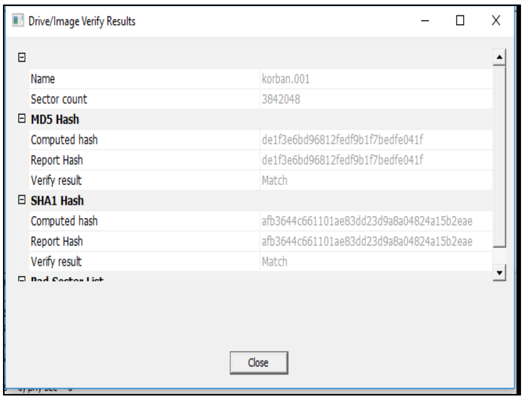
Select Source

Please Select the Source Evidence Type

● Physical Drive
○ Logical Drive
○ Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Femico Device (multiple CD/DVD)

Figure 4 Selection Process Source File to be in Imaging

There are 5 choices of source files. The investigator selects the selected source file of the Physical Drive because it is in the form of a flash or can be said to drive physically. In Figure 5 shows the result of SHA1 Hash.



Drive/Image Verify Results

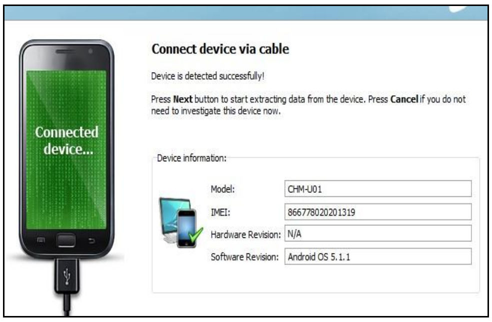
Name korban.001
Sector count 3842048
MD5 Hash
Computed hash de1f3e6bd96812fedf9b1f7bedfe041f
Report Hash de1f3e6bd96812fedf9b1f7bedfe041f
Verify result Match
SHA1 Hash
Computed hash afb3644c661101ae83dd23d9a8a04824a15b2eae
Report Hash afb3644c661101ae83dd23d9a8a04824a15b2eae
Verify result Match

Figure 5 Result of Hash File Imaging

Value where the value is used as a reference to match the hash value in the original file when it is done imaging so that when we analyze the file already in the same imaging with the original file of the evidence.

ii. Imaging process on smartphone 2 using Oxygen Forensic Suite

After completion of the device search process will then appear the device information is connected as shown on Figure 6.



Connect device via cable

Device is detected successfully!

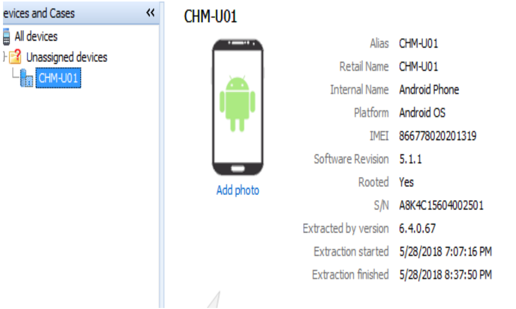
Press **Next** button to start extracting data from the device. Press **Cancel** if you do not need to investigate this device now.

Device information:

Model: CHM-U01
IMEI: 866778020201319
Hardware Revision: N/A
Software Revision: Android OS 5.1.1

Figure 6 Information Tool

The investigator can match the authenticity of imaging data with smartphone evidence by looking at the IMEI code contained in the smartphone Figure 7 shows the image result using the Oxygen Forensic Suite.



CHM-U01

Alias CHM-U01
Retail Name CHM-U01
Internal Name Android Phone
Platform Android OS
IMEI 866778020201319
Software Revision 5.1.1
Rooted Yes
S/N A8K4C15604002501
Extracted by version 6.4.0.67
Extraction started 5/28/2018 7:07:16 PM
Extraction finished 5/28/2018 8:37:50 PM

Figure 7 Imaging Results using Oxygen Forensic Suite Tools

Phase Examination is performed examination of the data processing and the results of the imaging process to then be explored to obtain or find the required evidence is WhatsApp database stored in the storage device smartphone without changing data integrity.

a) Smartphone Data Extraction from Imaging Results

In the extraction of imaging results here is divided into two between smartphone 1 and smartphone 2 adapts to the imaging tools used.

i. The Imaging Results on Smartphone 1 Imaging uses the Autopsy

In smartphone 1 to open the imaging file using Autopsy, actually using FTK Imager can be used to extract the imaging result and its result is the same. Here the author tries to compare from both tools to open the imaging file format .dd.

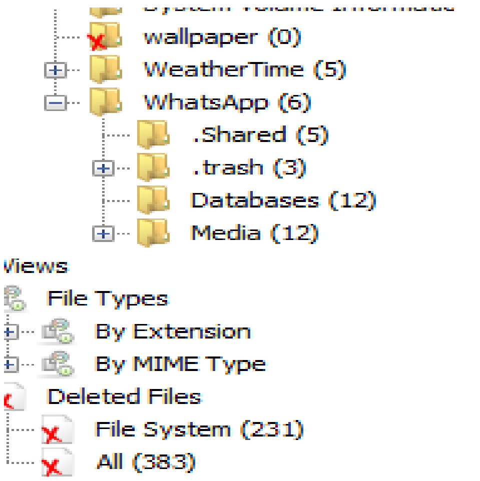
ii. Extract Imaging Results on Smartphone 2 using Oxygen Forensic Suite

In Oxygen Forensic Suite is slightly different from FTK Imager or Autopsy. Because the folders are shown do not all appear on the start page, but are merged into a single data folder.

b) Exploration of Imaging Data Extraction Results

i. Exploration on smartphone 1

Figure 8 shows the database file in the WhatsApp folder is in the tools whose data comes from the extracted .dd file in the open case then the result can be directly open to the location of a file in G: \ / EVERCROSS [FAT16] / [root] / WhatsApp/ database.



wallpaper (0)
WeatherTime (5)
WhatsApp (6)
.Shared (5)
.trash (3)
Databases (12)
Media (12)
Views
File Types
By Extension
By MIME Type
Deleted Files
File System (231)
All (383)

Figure 8 WhatsApp Smartphone Database Folder Structure 1

ii. Exploration on smartphone 2

Exposure has done on smartphone 2 get fairly complete results, because the findings of extracts of imaging results there is a fairly complete file and on forensic oxygen, tools can read all existing data in the smartphone with root conditions in order to provide more access rights in exploring the data and we can see more complate data on smartphone 2.

3) Analysis

This analysis phase aims to reveal and analyze the results of the Examination stage to obtain data related to WhatsApp application.

a) WhatsApp Database Decryption on Both Smartphones

i. Database decryption WhatsApp Smartphone 1

From Figure 9 shows the decrypted database file with a 340 KB file size. Then the file is opened using the WhatsApp Viewer application to see what the contents contained in the WhatsApp database

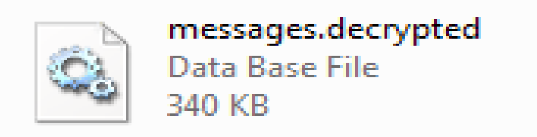
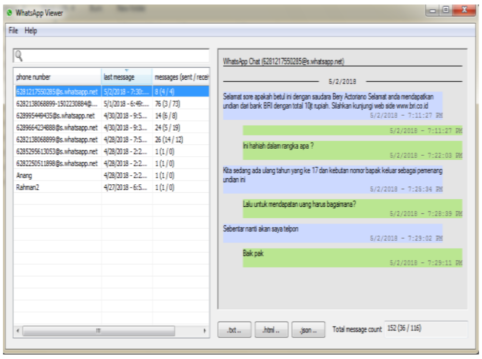

messages.decrypted
Data Base File
340 KB

Figure 9 The Decrypted Database File on Smartphone 1

In Figure 10 shows the contents of the database on smartphone 1 that has been decrypted.



phone number	last message	messages (sent / recei
6281217550285@s.whatsapp.net	5/2/2018 - 7:30:...	8 (4 / 4)
6282138068899-1502230884@...	5/1/2018 - 6:49:...	76 (3 / 73)
628995449435@s.whatsapp.net	4/30/2018 - 9:5...	14 (6 / 8)
6289664234888@s.whatsapp.net	4/30/2018 - 9:3...	24 (5 / 19)
6282138068899@s.whatsapp.net	4/28/2018 - 7:5...	26 (14 / 12)
6285295613053@s.whatsapp.net	4/28/2018 - 2:2...	1 (1 / 0)
6282250511898@s.whatsapp.net	4/28/2018 - 2:2...	1 (1 / 0)
Anang	4/28/2018 - 2:2...	1 (1 / 0)
Rahman2	4/27/2018 - 6:5...	1 (1 / 0)

WhatsApp Chat (6281217550285@s.whatsapp.net)

5/2/2018

Selamat sore apakah betul ini dengan saudara Bery Actoriano Selamat anda mendapatkan undian dari bank BRI dengan total 10jt rupiah. Silahkan kunjungi web side www.bri.co.id
5/2/2018 - 7:11:27 PM

5/2/2018 - 7:11:27 PM

Ini hahiah dalam rangka apa ?
5/2/2018 - 7:22:03 PM

Kita sedang ada ulang tahun yang ke 17 dan kebutan nomor bapak keluar sebagai pemenang undian ini
5/2/2018 - 7:25:34 PM

Lalu untuk mendapatan uang harus bagaimana?
5/2/2018 - 7:28:39 PM

Sebentar nanti akan saya telpon
5/2/2018 - 7:29:02 PM

Baik pak
5/2/2018 - 7:29:11 PM

Total message count 152 (36 / 116)

Figure 10 The Contents of a Decrypted Database on Smartphon 1

ii. Database decryption WhatsApp Smartphone 2

The smartphone 2 for different sizes with smartphone 1, smartphone 1 has a file size of 340 KB while smartphone 2 has a file size of 2.90 MB. That's because how much the contents of the messages stored in the database, then also counted from how many sending files in the form of Photos, Videos, Voice Note, etc. that will affect the size of the database file. The decrypted database shown on Figure 11.

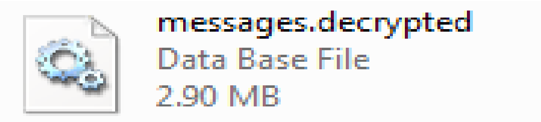
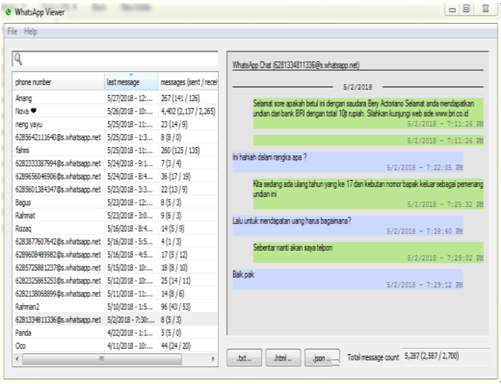

messages.decrypted
Data Base File
2.90 MB

Figure 11 The Decrypted Database File on Smartphone 2

Figure 12 shows the content of the conversation that has been decrypted there is a database of smartphone chat message conversations 2.



phone number	last message	messages (sent / recei
Anang	5/27/2018 - 12:...	267 (141 / 126)
Nova ❤	5/26/2018 - 10:...	4,402 (2,137 / 2,265)
neng yayu	5/25/2018 - 11:...	23 (14 / 9)
6285642111640@s.whatsapp.net	5/25/2018 - 1:3...	8 (8 / 0)
fahmi	5/25/2018 - 11:...	260 (125 / 135)
6282333387994@s.whatsapp.net	5/24/2018 - 9:1...	7 (3 / 4)
6289656046906@s.whatsapp.net	5/24/2018 - 8:4...	36 (17 / 19)
6285601384347@s.whatsapp.net	5/23/2018 - 3:3...	22 (13 / 9)
Bagus	5/23/2018 - 12:...	8 (5 / 3)
Rahmat	5/23/2018 - 3:0...	9 (6 / 3)
Rozaq	5/16/2018 - 8:4...	14 (5 / 9)
6283877607642@s.whatsapp.net	5/16/2018 - 5:5...	4 (1 / 3)
6289608489982@s.whatsapp.net	5/16/2018 - 4:5...	17 (5 / 12)
6285725881237@s.whatsapp.net	5/15/2018 - 10:...	18 (8 / 10)
6282325865253@s.whatsapp.net	5/12/2018 - 10:...	25 (14 / 11)
6282138068899@s.whatsapp.net	5/11/2018 - 11:...	14 (8 / 6)
Rahman2	5/10/2018 - 1:5...	96 (43 / 53)
6281334811336@s.whatsapp.net	5/2/2018 - 7:30:...	8 (5 / 3)
Panda	4/22/2018 - 1:1...	5 (5 / 0)
Oco	4/11/2018 - 10:...	44 (24 / 20)

WhatsApp Chat (6281334811336@s.whatsapp.net)

5/2/2018

Selamat sore apakah betul ini dengan saudara Bery Actoriano Selamat anda mendapatkan undian dari bank BRI dengan total 10jt rupiah. Silahkan kunjungi web side www.bri.co.id
5/2/2018 - 7:11:26 PM

5/2/2018 - 7:11:26 PM

Ini hahiah dalam rangka apa ?
5/2/2018 - 7:22:05 PM

Kita sedang ada ulang tahun yang ke 17 dan kebutan nomor bapak keluar sebagai pemenang undian ini
5/2/2018 - 7:25:32 PM

Lalu untuk mendapatan uang harus bagaimana?
5/2/2018 - 7:28:40 PM

Sebentar nanti akan saya telpon
5/2/2018 - 7:29:02 PM

Baik pak
5/2/2018 - 7:29:12 PM

Total message count 5,287 (2,587 / 2,700)

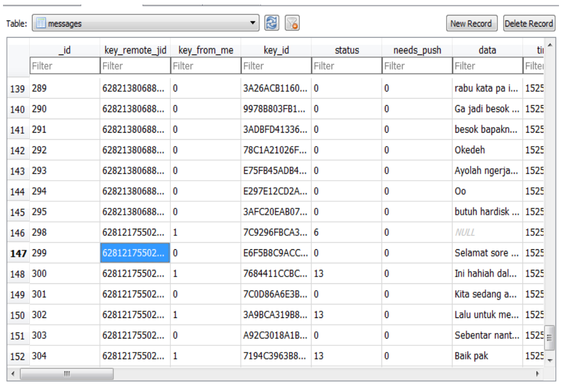
Figure 12 The Contents of a Decrypted Database on Smartphone 2

b) WhatsApp Database Exploration

In exploring the WhatsApp database here using the DB Browser For SQLite, the tools can provide information in the form of database structures, phone numbers connected with WhatsApp, sending id notes, conversation message quotes, etc.

i. Exploring WhatsApp Database on Smartphone 1

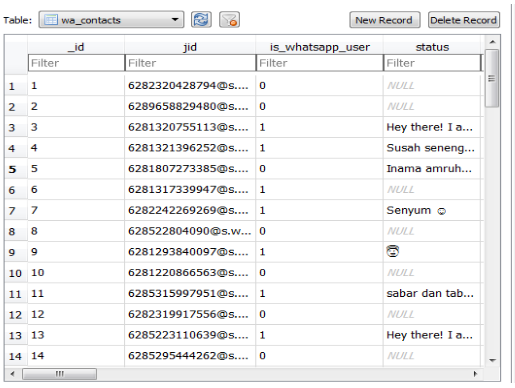
For Figure 13 is the contents in the messages.dcrypted.db file there are several columns that are filled with id, key_remote_jid, key_id, status etc.



	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	ti
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
139	289	62821380688...	0	3A26ACB1160...	0	0	rabu kata pa i...	1525
140	290	62821380688...	0	9978B803FB1...	0	0	Ga jadi besok ...	1525
141	291	62821380688...	0	3ADBFD41336...	0	0	besok bapakn...	1525
142	292	62821380688...	0	78C1A21026F...	0	0	Okedeh	1525
143	293	62821380688...	0	E75FB45ADB4...	0	0	Ayolah ngerja...	1525
144	294	62821380688...	0	E297E12CD2A...	0	0	Oo	1525
145	295	62821380688...	0	3AFC20EAB07...	0	0	butuh hardisk ...	1525
146	298	62812175502...	1	7C9296FBCA3...	6	0	NULL	1525
147	299	62812175502...	0	E6F5B8C9ACC...	0	0	Selamat sore ...	1525
148	300	62812175502...	1	7684411CCBC...	13	0	Ini hahiah dal...	1525
149	301	62812175502...	0	7C0D86A6E3B...	0	0	Kita sedang a...	1525
150	302	62812175502...	1	3A9BCA319B8...	13	0	Lalu untuk me...	1525
151	303	62812175502...	0	A92C3018A1B...	0	0	Sebentar nant...	1525
152	304	62812175502...	1	7194C3963B8...	13	0	Baik pak	1525

Figure 13 The contents of the messages.dcrypted.db file on Smartphone1

The Figure 14 shows information that we can catch the column which is in the file wa.db contains contact phone numbers connected with WhatsApp or un-connected, the existing column in the wa.db file consists of id, jid, is_WhatsApp_user,status,status_timestamp, number.

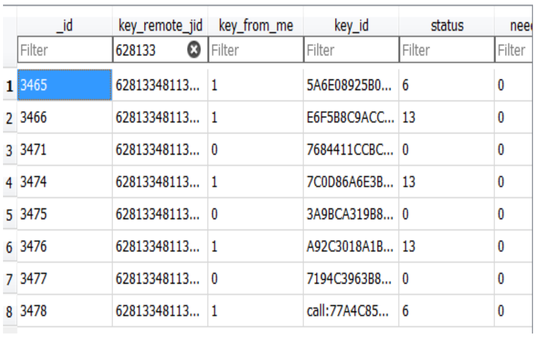


	_id	jid	is_whatsapp_user	status
	Filter	Filter	Filter	Filter
1	1	6282320428794@s....	0	NULL
2	2	6289658829480@s....	0	NULL
3	3	6281320755113@s....	1	Hey there! I a...
4	4	6281321396252@s....	1	Susah seneng...
5	5	6281807273385@s....	0	Inama amruh...
6	6	6281317339947@s....	1	NULL
7	7	6282242269269@s....	1	Senyum ☺
8	8	628522804090@s.w...	0	NULL
9	9	6281293840097@s....	1	☺
10	10	6281220866563@s....	0	NULL
11	11	6285315997951@s....	1	sabar dan tab...
12	12	6282319917556@s....	0	NULL
13	13	6285223110639@s....	1	Hey there! I a...
14	14	6285295444262@s....	0	NULL

Figure 14 File Contents wa.db on Smartphone 1

ii. Exploring WhatsApp Database on Smartphone 2

In Figure 15 which is the contents of the file has a column consisting of id (To Record Message Number), key_id(Unique Messag Identification), key_remote_jid (ID WhatsApp from Communication Partners), key_from_me (Message Direction : '0' = Signed in, '1' = Exit) .

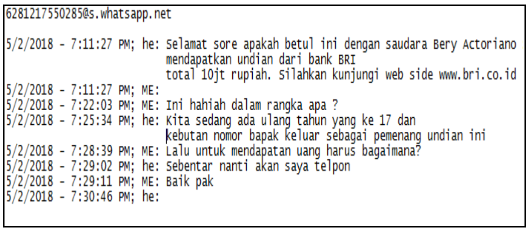


	_id	key_remote_jid	key_from_me	key_id	status	nee
	Filter	628133	Filter	Filter	Filter	Filter
1	3465	62813348113...	1	5A6E08925B0...	6	0
2	3466	62813348113...	1	E6F5B8C9ACC...	13	0
3	3471	62813348113...	0	7684411CCBC...	0	0
4	3474	62813348113...	1	7C0D86A6E3B...	13	0
5	3475	62813348113...	0	3A9BCA319B8...	0	0
6	3476	62813348113...	1	A92C3018A1B...	13	0
7	3477	62813348113...	0	7194C3963B8...	0	0
8	3478	62813348113...	1	call:77A4C85...	6	0

Figure 15 Content messages.decrypted.db file on Smartphone 2

c) Results Both Smartphone Analysis

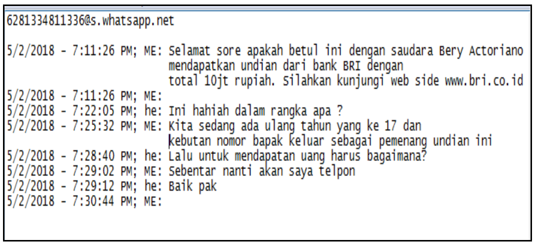
In the conversation, there is an element of conversation that is notification information winning contents of the lottery and ends with a fraudulent action on behalf of an agency. In Figure 16 and Figure 17 shows the content of a conversation between two smartphones with the number of each registered or logged in using the phone number on the smartphone used.



```
6281217550285@s.whatsapp.net

5/2/2018 - 7:11:27 PM; he: Selamat sore apakah betul ini dengan saudara Bery Actoriano
                           mendapatkan undian dari bank BRI
                           total 10jt rupiah. Silahkan kunjungi web side www.bri.co.id
5/2/2018 - 7:11:27 PM; ME:
5/2/2018 - 7:22:03 PM; ME: Ini hahiah dalam rangka apa ?
5/2/2018 - 7:25:34 PM; he: Kita sedang ada ulang tahun yang ke 17 dan
                           kebutan nomor bapak keluar sebagai pemenang undian ini
5/2/2018 - 7:28:39 PM; ME: Lalu untuk mendapatan uang harus bagaimana?
5/2/2018 - 7:29:02 PM; he: Sebentar nanti akan saya telpon
5/2/2018 - 7:29:11 PM; ME: Baik pak
5/2/2018 - 7:30:46 PM; he:
```

Figure 16 Conversation Contents on Smartphone 1



```
6281334811336@s.whatsapp.net

5/2/2018 - 7:11:26 PM; ME: Selamat sore apakah betul ini dengan saudara Bery Actoriano
                           mendapatkan undian dari bank BRI dengan
                           total 10jt rupiah. Silahkan kunjungi web side www.bri.co.id
5/2/2018 - 7:11:26 PM; ME:
5/2/2018 - 7:22:05 PM; he: Ini hahiah dalam rangka apa ?
5/2/2018 - 7:25:32 PM; ME: Kita sedang ada ulang tahun yang ke 17 dan
                           kebutan nomor bapak keluar sebagai pemenang undian ini
5/2/2018 - 7:28:40 PM; he: Lalu untuk mendapatan uang harus bagaimana?
5/2/2018 - 7:29:02 PM; ME: Sebentar nanti akan saya telpon
5/2/2018 - 7:29:12 PM; he: Baik pak
5/2/2018 - 7:30:44 PM; ME:
```

Figure 17 Conversation Contents on Smartphone 2

Both conversations above are the result of exporting the WhatsApp Viewer file into a .txt format. When we look from the picture 20 and 21 at the top of the picture there is a phone number, phone number is the phone number owned by smartphone 2 and vice versa phone number is phone number owned by smartphone 1. That is smartphone 1 receive a message sent by smartphone 2, by looking at the message (ME) which indicates even that is the outgoing message da (he) indicates the incoming message.

When viewing the contents of messages.decrypted.db file then we will find the sender of the message that is from the side of the phone number with no id for smartphone 1 of id 299 -304 is on the smartphone 2 no id starting from id 3465-3478 as shown in Figure 13 and Figure 14. From the data we can also see who sends the message and who receives the message by latching on the column key_from_me in the column contains the contents of '0' and '1', for '0' means incoming message and '1' means outgoing message, data the key_form_me column will also get the contents of the message sent by the sender to the recipient.

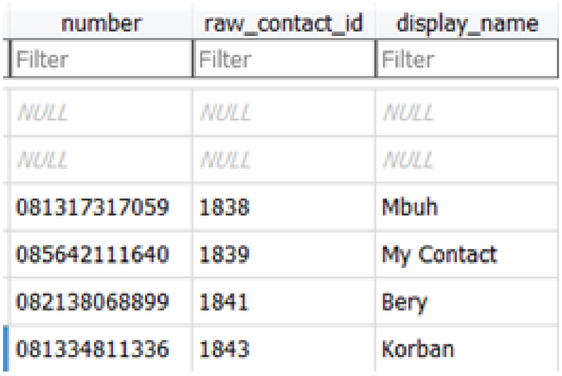
4) Reporting

After doing the analysis of evidence in the form of two smartphones. With the above findings can be concluded by using the mobile forensic process and the NIST groove on the Android platform, digital artifacts related to the evidence required and obtained. In the artifacts include conversations, photos, voice notes, call history and others, but in this research researchers only focus on conducting analysis on conversations stored in the database only. the discovery of artifacts of evidence or evidence in the form of two smartphones as shown on Table 3.

Table 3 Information on Findings of Evidence from Both Smartphones at Can

Information	*Smartphone 1*	*Smartphone 2*
Mobile phone number	+6281334811336	+6281217550285
username	Berry	Helmy
Contact	72	285
Conversation	9	20
Encrypted Databases	9	7

From the results of the above analysis has been expressed that the message sent by smartphone 2 contains the notification of the winner of the present and smartphone 1 is the recipient of the message. So for the perpetrator in this scenario is smartphone 2 because that sends messages first and contains elements of fraud Because of the name of the agency. Proof that smartphone 2 is the perpetrator of the crime of fraud shown on Figure 18.



number	raw_contact_id	display_name
Filter	Filter	Filter
NULL	NULL	NULL
NULL	NULL	NULL
081317317059	1838	Mbuh
085642111640	1839	My Contact
082138068899	1841	Bery
081334811336	1843	Korban

Figure 18 Contact Information on Smartphone 2

The column display_name containing the name of the victim with number 081334811336 number is the number on smartphone 1. So it can be concluded that the perpetrators of this fraud case scenario are smartphone2 with phone number +628121755028 on behalf of the Helmy owner.

5) User Acceptance Test (UAT)
From the testing results, the percentage of FTK Imager is (60%), Autopsy is (52%), Oxygen Forensic Suite is (44%) the percentage is taken from the highest value in the column. Based on liker's interpretation of the distance category between 41% - 60% belonging to a fairly high interpretation, the assessment for the forensic tools and applications includes quite appropriate and can be used as a tool for analyzing forensic investigations in finding digital evidence.

V. CONCLUSION

Based on the stages of Mobile Forensic and the flow of the NIST framework conducted in this research succeeded in producing information presented in the form of disclosure of fraudulent criminals from findings in the form of evidence artifacts in the form of chat message conversation sessions, user telephone numbers, message sending id numbers, and account owner identities. WhatsApp and get other media files that can be used as evidence and also the most important encrypted database backup files.

VI. REFERENCES

1. G. M. Zamroni, R. Umar, and I. Riadi, “Forensic Analysis Instant Messaging Aplication Based on Android,” *Annu. Res. Semin.*, vol. 2, no. 1, pp. 102–105, 2016.

2. Nuril anwar and I. Riadi, “WhatsApp Messenger Smartphone Forensic Investigation Analysis on Web-based WhatsApp,” *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, pp. 1–10, 2017.

3. K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,” 2006.

4. Z. Akbar, B. Nugraha, and M. Alaydrus, “WhatsApp Forensics on Android Smartphone : a Survey,” *Sinergi*, vol. 20, no. 3, p. 207, 2016.

5. B. Raharjo, “Overview of Digital Forensics,” *Overview of Digital Forensics. J. Sosioteknologi Ed.*, vol. 29, no. 12, pp. 384–387, 2013.

6. Ruci Meiyanti and Ismaniah, “Digital Forensic Development,” *J. Kaji. Ilmial UBJ*,

vol. 15, no. September 2015, 2015.

7. I. Z. Yadi and Y. N. Kunang, “Forensic Analysis on the Android Platform,” *Konf. Nas. ilmu Komput.*, pp. 141–148, 2014.

8. I. Riadi, A. Yudhana, M. Caesar, and F. Putra, “Digital Recovery Proof Analysis Instagram Messenger Using National Institute of Standards and Technology (NIST) Method,” *Semin. Nas. Teknol. Inf. dan Komun. - Semant.*, pp. 161–166, 2017.

9. I. Riadi, Sunardi;, and A. Firdonsyah, “Forensic Investigation Technique on Android’s Blackberry Messenger using NIST Framework,” *Int. J. Cyber-Security Digit. Forensics*, vol. 16, no. 4, pp. 198–205, 2017.

10. V. Rao and A. S. N. Chakravarthy, “Survey on Android Forensic Tools and Frameworkologies,” *Int. J. Comput. Appl.*, vol. 154, no. 8, pp. 975–8887, 2016.

11. B. Hambling and P. van Goethem, *User Acceptance Testing: a Step by Step Guide*. 2013.

12. I. Riadi, J. Eko, A. Ashari, and S. -, “Internet Forensics Framework Based-on Clustering,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 12, pp. 115–123, 2013.

13. Hariani and I. Riadi, “Detection Of Cyberbullying On Social Media Using Data Mining Techniques,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 3, pp. 244–250, 2017.

14. Y. N. Kunang *et al.*, “Implementation of Forensic Procedures for the WhatsApp Application on Android Phones,” vol. 11, no. Thakur 2013, 2017.

15. A. A. Anton Yudhana , Rusydi Umar, “Google Drive Acquisition and Analysis on Android Smartphone,” 2017.

16. M. Z. Shuaibu and Alhassan Bala, “Global Journal of Advanced Engineering Technologies and Sciences,” vol.2,no. 8, pp. 33–38, 2015.