p-ISSN: 2301-5373
e-ISSN: 2654-5101

Acquisition Of Digital Evidence In Online Scam Cases (CyberCrime) On *WhatsApp* Chat Application Using NIST Method

Gede Agus Surya Atmaja[a1], I Komang Ari Mogi[a2]

[a]Informatics Department, Faculty of Math and Science, Udayana University
Bali, Indonesia
[1]agussurya435@gmail.com
[2]arimogi@cs.unud.ac.id

Abstract

Cybercrime usually happen on internet. There are many type of cybercrime such as Cyberbullying, Online Scams, Malware, etc. WhatsApp is a chatting application that is easy to use and many of its users. Because of many users that used WhatsApp chatting application not infrequently many crimes occur there. Especially Online Scams, the perpetrator usually sell something online and make their target use WhatsApp to contact them and their transaction begin there. In this research using NIST steps, those steps are Identification, collect data, analyze data and report the result. This research also focusing on WhatsApp data extraction to obtain evidence from perpetrator Smartphone. The end of the research

Keywords: *CyberCrime, WhatsApp, Forensic, Online Scam, NIST*

1. Introduction

The Internet is a place to find all things that user want and need. There is benefit user can get from internet such as search for information, news, communicate with others and shop online. The Internet can be access from computer and smartphone. With smartphone the user can access the internet and make their work easier. According to We Are Social in 2018 the internet users pass more than 4 billion people around the world. Smartphone can be use for communication with social media application such as *WhatsApp*, LINE, Instagram, Telegram, etc. Although there is so much good things that user get from the internet. The internet can be a tool for evil or bad things such as Cybercrime. Cybercrime is rife on internet these days such as Online Scams, Cyberbullying, *Phising,* Malware etc. One of the cybercrimes that often occur is Online scam. In Indonesia, Online Scam occupy the top position in 2019. Indonesia Police received 1.617 reports of online scam. Judging from the disadvantages, online scam via website reached 73 billion in this case especially in the case of online shopping and this mode was mostly reported as many as 351 reports [1].

Online Scam usually take place on online shop or an email or short message that the target win prize, the perpetrator pretend sale things and looks convincing so that the victim believes. One of the popular chat applications is *WhatsApp Application*. *WhatsApp Application* is easier to use and user-friendly. According to We Are Social *WhatsApp* reach 1.6 billion users active in 2019. Because of its popularity *WhatsApp* can be used for Online scam. Usually after the perpetrator get the money they will disappear and can’t be contacted. Therefore to prevent this happening requires caution so as not to get caught up in the perpetrator’s trick. The police will do an investigation, track the perpetrator down and chase the perpetrator. So begin the examination and collecting the evidence from the suspect. One of the things that can be done in solving the digital crime problem is digital forensics.

Digital Forensics is an appropriate step for investigating digital evidence. The main purpose of this research is to extract *WhatsApp* database to get evidence from perpetrator’s *Smartphone.* In this research, the researchers will conduct forensics on *WhatsApp* application which uses forensics steps from NIST.

1.1. Literature Review

The previous research related to this research is as follows:

The research conducted by Ayubi Wirara et al (2020) is about "Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan '*WhatsApp*' ". The research discusses crimes on the *WhatsApp* application. In their research they acquisition the digital evidence and they analyzed it. The tool that they used are XRY version 8.0.0 and Encase Mobile Forensic version 9.09.00.192. The Result they got from their research are the digital evidence that they extracted from the smartphone [2].
Research conducted by Hussein Abed Ghannam (2020) is about "Forensic Anaysis of Artifacts of Giants Instant Messaging "*WhatsApp*" in Android Smarphone".his research discusses about how the researcher acquire data from *WhatsApp* from it database. Decrypt and extract the database without rooting the smartphone and collect digital evidence as much as possible. The tools used in this research are Whatcrypt to decrypt the database, SQLite to view the database, UFED cellbrite to recover the deleted message. In the end of the research, the researcher succeeded in getting data from extracting and analyzing these data [3].
Research conducted by Muhammad Irwan Syahib et al (2018) entitled " Analisis Forensic Digital Aplikasi *BEETALK* untuk Pengamanan *Cybercrime* Menggunakan Metode NIST ". Their research discusses the analysis of *BEETALK* applications using the NIST method. In the data acquisition process, the beetalk smartphone application must be rooted first using the Kingroot tools. After that, take data from the smartphone, but the data from the smartphone must be backed up first using the *MOBILedit* Forensic tool, then Examination using OXYGEN Forensic which is used to acquire data that has been backed up by *MOBILedit* [4].
Research conducted by Muhammad Iqbal Ramadhan and Imam Riadi (2019) entitled "Forensic *WhatsApp* based Andorid using National Institute of Standard Technology (NIST) Method". Their research discusses about acquisition the data from rooted and non-rooted smartphones. The researchers using following tools *FTK Imager, ProDiscover Basic*, *WhatsApp* DB Extractor. *TWRP* and *WhatsApp Viewer*. The result from the research are they successfully raised evidence from the smartphones [5].
Research conducted by Dr. Iyobor Egho-Promise et al (2020) entitled "A Forensic Analysis of *WhatsApp* on Andorid Smart phone". Their research is about how to extract valuable information from *WhatsApp* and from similar mobile applications installed on the Android platform and focus on extraction and analysis data user from volatile and non-volatile memory of an Android Device [6].

2. Reseach Methods

The main purpose of this research is to do forensic WhatsApp data and extract the data with
Smartphone Forensic System and view the extracted data in *WhatsApp Viewer* using NIST
Method. The scenario that will be carried out in this research is that the perpetrator and victim communicate with *WhatsApp* then the victim sends money and confirms to the perpetrator and the perpetrator runs away ad cannot be contacted again

2.1. NIST

This research use forensics method from National Institute of Standards and Technology (NIST). The steps are:

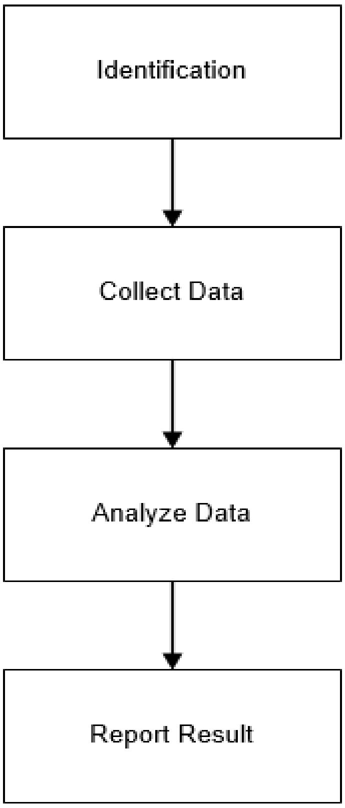


Figure 1. *National Institute of Standards and Technology Method (NIST)*

a. Identify/Identification
In identify or identification, we will acquire data and protect data related to a specific event. In this research the event is about online scams. The data that we acquire is digital evidence is smartphone. The smartphone contain the data that we need for this research.

b. Collect Data
In this step the researchers start to collect the data and extract relevan pieces of information from it. From this step to collect and extract the data we need from evidence, the researchers
start use tools, the tool is *MOBILedit*. In this case we need *WhatsApp* Data from the evidence smartphone.

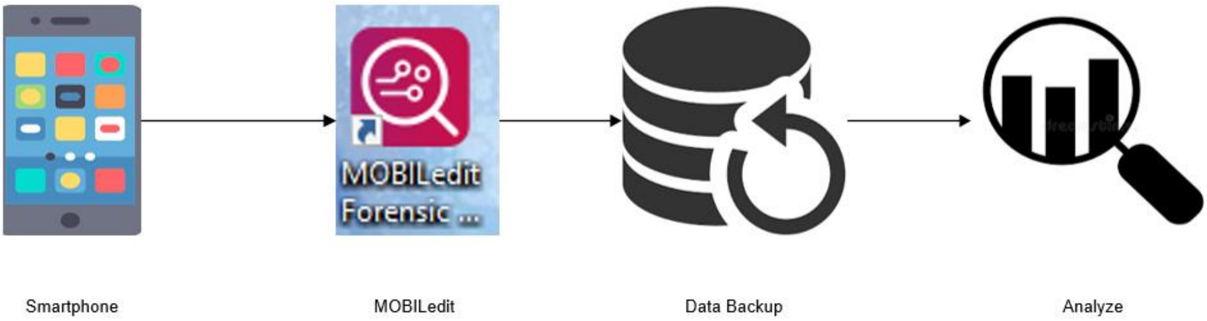


Figure 2. Acquisition Process

c. Analyzed Data
After we get the extracted data, we analyze the data. From *WhatsApp* data we get from Collect Data Steps. In this step, we will analyzed the database from *WhatsApp*.

WhatsApp Databases are Encrypted after backup. The way to decrypt it is to find the key or downgrade the *WhatsApp* on smartphone and backup the data again, because the older version *WhatsApp* does not use encryption.

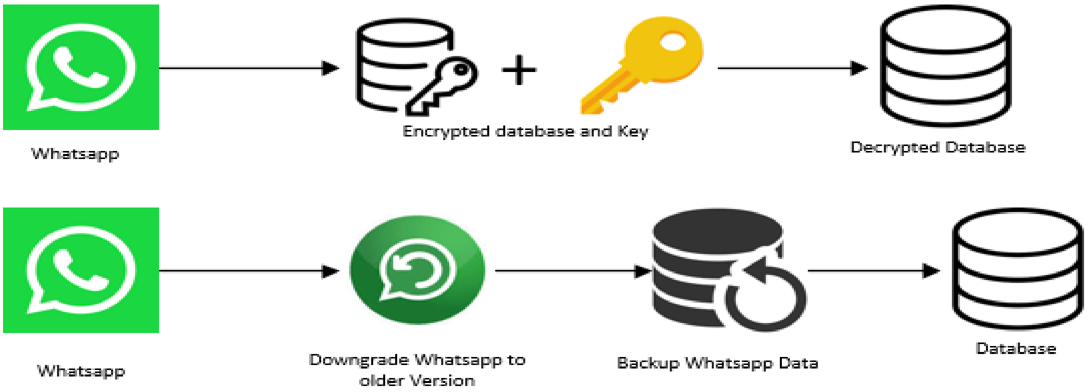


Figure 3. Process to get Decrypted Database

d. Report the Result
Last step is to report the result of the research. After analyze those data. In this step, the researchers make report on the steps that have been taken. The report contain data we get from identification, collect data and analyze data.

3. Result and Discussion

The research succeeded in producing the desired evidence, where the evidence was obtained from the *WhatsApp* data extraction or database (*msgstore.db).* The database contain conversations between the perpetrator and victim on *WhatsApp Application.* Table 1 below contain tools and material that will be used in the research.

Table 1. Tools and Materials

No.	Tools and Materials	Information
1	Laptop	Asus type A456UR
2	Smartphone	Samsung J5 Pro
3	*WhatsApp*	*WhatsApp* is a chatting application which is an object for this research
4	*MOBILedit* Express version 7.1.0.17644	Tool for acquisition data from the digital evidence
5	*Smartphone Forensic System*(SPF)	Tool for mobile forensic and one of the feature can decrypt *WhatsApp* databases
6	*WhatsApp Viewer*	View *WhatsApp* messages from databases

3.1. Identification

In this step the researcher find and gather information from perpetrator smartphone such as specification of the smartphone and the condition of the smartphone.

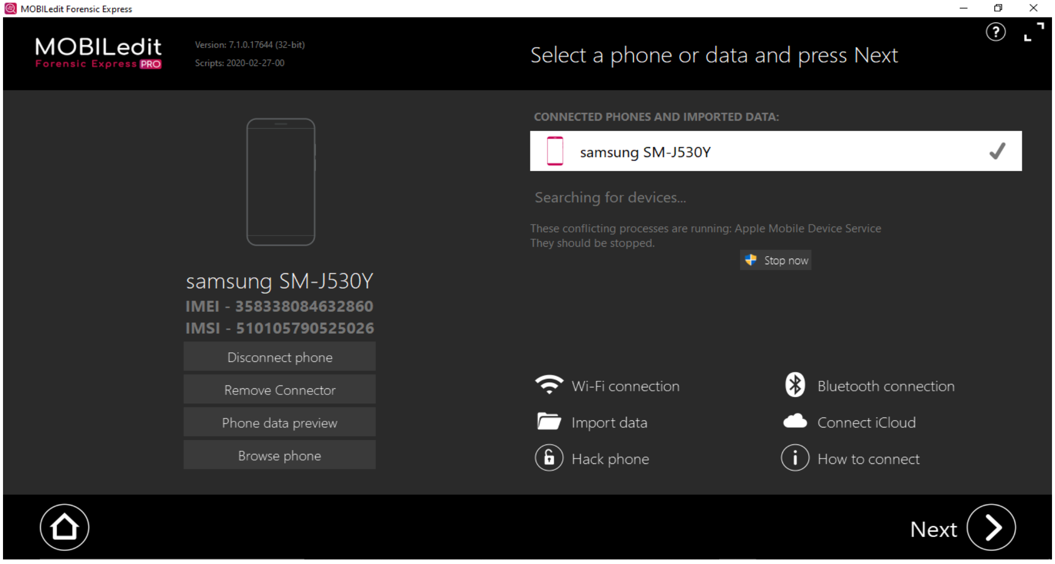
Table 2. Perpetrator Smartphone Spesification

Model	Information
Samsung J5 Pro (SM-J530Y/DS)	OS Version: Android 9 RAM : 3 GB Internal Memory : 32 GB Condition: The Smartphone Works Well , nothing broken

The information above is specification of perpetrator smartphone. The evidence is secure and no data has changed. If the smartphone is not secured, then someone who is not responsible may change the data from the smartphone.

3.2. Collect Data

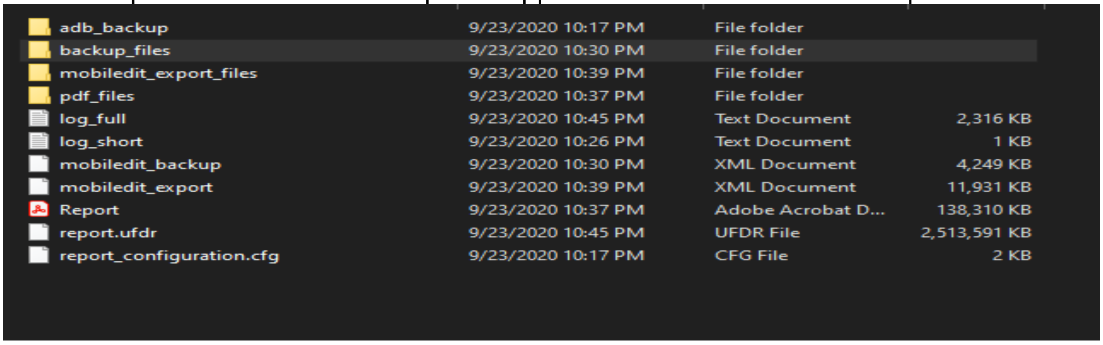
In this step the researcher begin to acquisition data from the smartphone. The Software that we should use is *MOBILedit*. This software will extract all data from the smartphone, after that we will find the all extracted data in specific folder.



These conflicting processes are running: Apple Mobile Device Service
They should be stopped.

Figure 4. *MOBILedit*

Figure 4 is the appearance of *MOBILedit* Forensic Software, this software extract all data from smartphone included all backup from applications that installed in smartphone.



adb_backup	9/23/2020 10:17 PM	File folder	
backup_files	9/23/2020 10:30 PM	File folder	
mobiledit_export_files	9/23/2020 10:39 PM	File folder	
pdf_files	9/23/2020 10:37 PM	File folder	
log_full	9/23/2020 10:45 PM	Text Document	2,316 KB
log_short	9/23/2020 10:26 PM	Text Document	1 KB
mobiledit_backup	9/23/2020 10:30 PM	XML Document	4,249 KB
mobiledit_export	9/23/2020 10:39 PM	XML Document	11,931 KB
Report	9/23/2020 10:37 PM	Adobe Acrobat D...	138,310 KB
report.ufdr	9/23/2020 10:45 PM	UFDR File	2,513,591 KB
report_configuration.cfg	9/23/2020 10:17 PM	CFG File	2 KB

Figure 5. Extracted Data

Figure 5 shows All the extrated data in specific folder. The *WhatsApp* folder application must be in *backup_files* folder, where the databases is stored.

3.3. Analyze Data

WhatsApp application store all the message in database named *msgstore.db.crypt12* we know that the file is encrypted, because recent or latest version of *WhatsApp* use encryption on their databases. There is two ways to decrypt the database, first we need to find the key encryption.

Actually after *WhatsApp* encrypt the database it also generate the key encryption and store it in the smartphone, but it is not easy to find because we need to *ROOT* the smartphone to gain access to the folder where the key stored. The second way is to downgrade the *WhatsApp* application and backup all the data, because the older version of *WhatsApp* not using encryption to the databases. Because the recent smartphone is too hard to *ROOT,* the second way is the method chosen by the researchers. There is a tool used for this method, the tools is *Smartphone Forensic System*. The tool has feature to decrypt the database from *WhatsApp*.

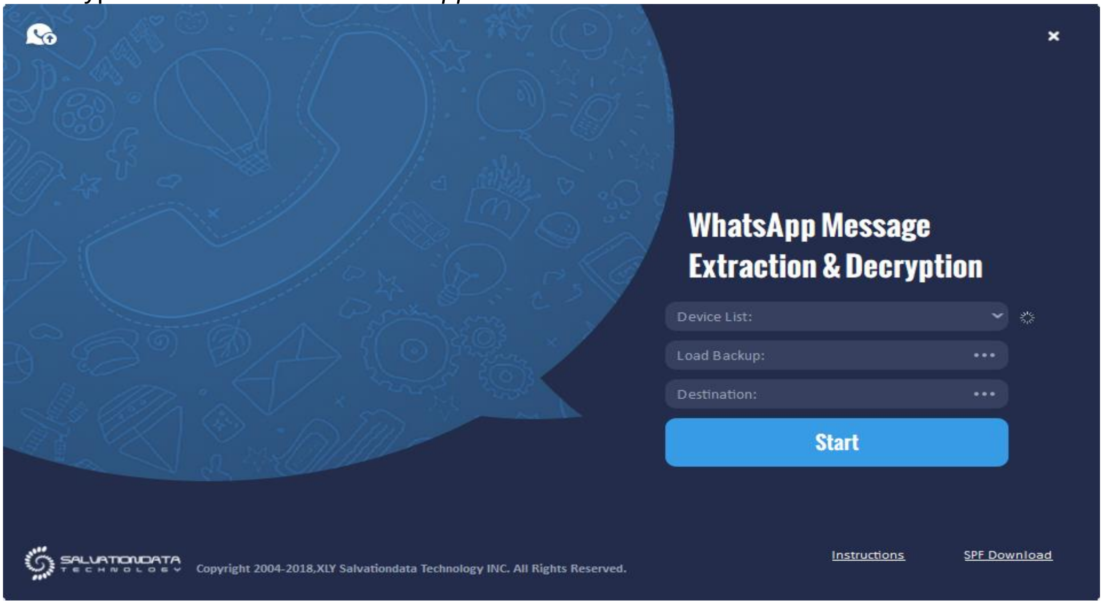
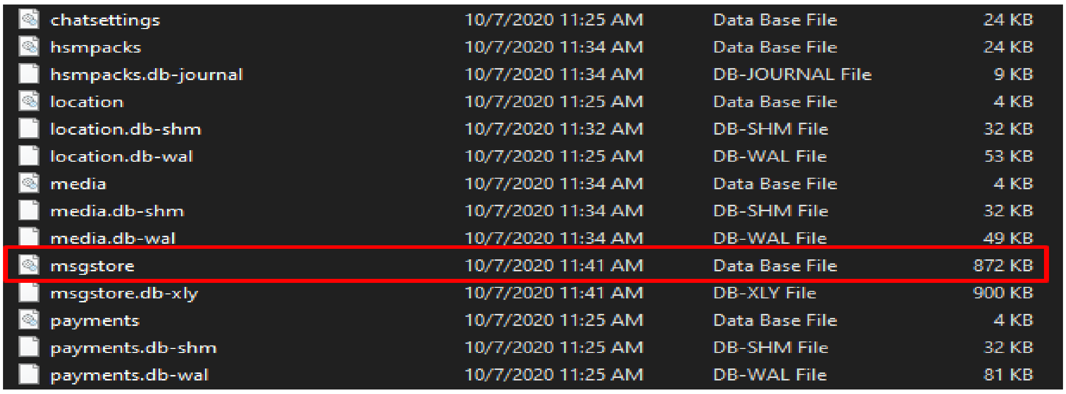

WhatsApp Message Extraction & Decryption
Device List:
Load Backup:
Destination:
Start
SALVATIONDATA TECHNOLOGY
Copyright 2004-2018,XLY Salvationdata Technology INC. All Rights Reserved.
Instructions
SPF Download

Figure 6. *WhatsApp* Message Extraction and Decryption

This Software can be used to decrypt the database, to use it we must connect the smartphone by USB and wait until the software detect the device, after that select the folder destination and start.

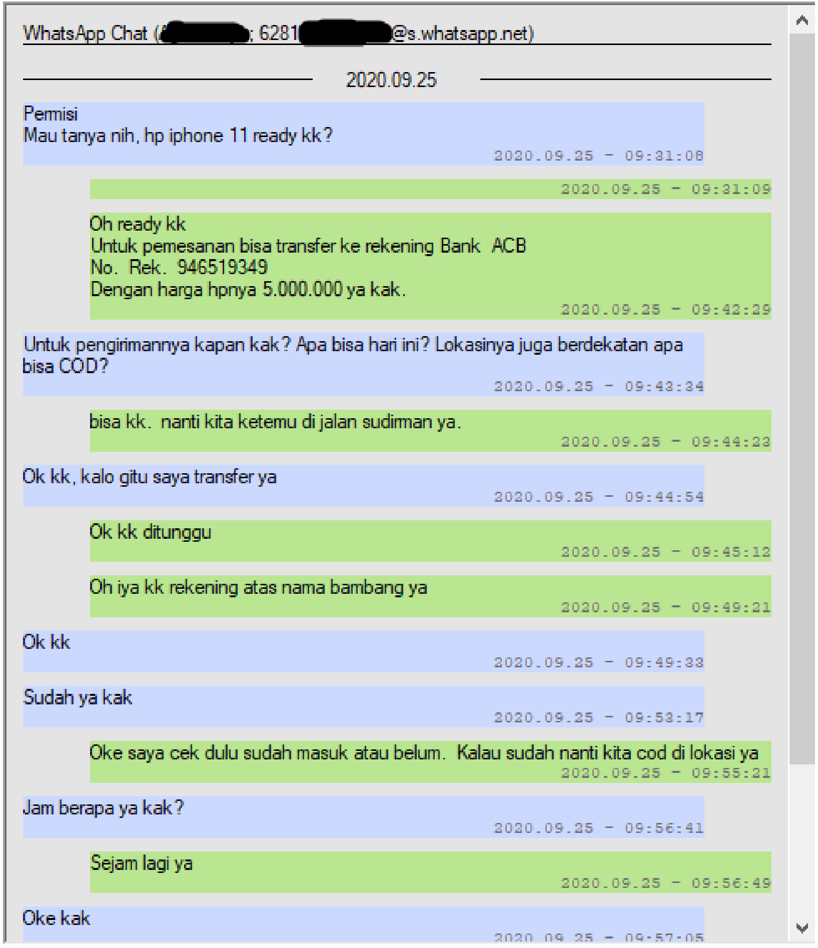


chatsettings	10/7/2020 11:25 AM	Data Base File	24 KB
hsmpacks	10/7/2020 11:34 AM	Data Base File	24 KB
hsmpacks.db-journal	10/7/2020 11:34 AM	DB-JOURNAL File	9 KB
location	10/7/2020 11:25 AM	Data Base File	4 KB
location.db-shm	10/7/2020 11:32 AM	DB-SHM File	32 KB
location.db-wal	10/7/2020 11:25 AM	DB-WAL File	53 KB
media	10/7/2020 11:34 AM	Data Base File	4 KB
media.db-shm	10/7/2020 11:34 AM	DB-SHM File	32 KB
media.db-wal	10/7/2020 11:34 AM	DB-WAL File	49 KB
msgstore	10/7/2020 11:41 AM	Data Base File	872 KB
msgstore.db-xly	10/7/2020 11:41 AM	DB-XLY File	900 KB
payments	10/7/2020 11:25 AM	Data Base File	4 KB
payments.db-shm	10/7/2020 11:25 AM	DB-SHM File	32 KB
payments.db-wal	10/7/2020 11:25 AM	DB-WAL File	81 KB

Figure 7. Decrypted Database File

Figure 7 shows the result of decryption *WhatsApp* database. The database change from *msgstore.crypt12* to *msgstore* database file.After the database decrypted the next step is to view what inside the database. To view message inside the database we need to use

WhatsApp Viewer tool.This tool unable to view the message with user interface and looks like *WhatsApp* Application.



WhatsApp Chat ([redacted]; 6281[redacted]@s.whatsapp.net)

2020.09.25

Permisi
Mau tanya nih, hp iphone 11 ready kk?
2020.09.25 - 09:31:08

2020.09.25 - 09:31:09

Oh ready kk
Untuk pemesanan bisa transfer ke rekening Bank ACB
No. Rek. 946519349
Dengan harga hpnya 5.000.000 ya kak.
2020.09.25 - 09:42:29

Untuk pengirimannya kapan kak? Apa bisa hari ini? Lokasinya juga berdekatan apa bisa COD?
2020.09.25 - 09:43:34

bisa kk. nanti kita ketemu di jalan sudirman ya.
2020.09.25 - 09:44:23

Ok kk, kalo gitu saya transfer ya
2020.09.25 - 09:44:54

Ok kk ditunggu
2020.09.25 - 09:45:12

Oh iya kk rekening atas nama bambang ya
2020.09.25 - 09:49:21

Ok kk
2020.09.25 - 09:49:33

Sudah ya kak
2020.09.25 - 09:53:17

Oke saya cek dulu sudah masuk atau belum. Kalau sudah nanti kita cod di lokasi ya
2020.09.25 - 09:55:21

Jam berapa ya kak?
2020.09.25 - 09:56:41

Sejam lagi ya
2020.09.25 - 09:56:49

Oke kak
2020.09.25 - 09:57:05

Figure 8. *WhatsApp Viewer*

Figure 8 shows the conversation between the perpetrator and the victim. From the evidence that has obtained, it is seen that the victim made a transaction, then after the perpetrator got the money the perpetrator promised to meet the victim, but the perpetrator ran away. Because the researchers obtained the evidence, then the goal of the research was reached successfully.

3.4. Report

The last step is make report, the report contain all information from the previous steps. From identification the digital evidence that the researcher got is smartphone of the perpetrator. In collect data, begin the acquisition process using tool *MOBILedit* and backup all data in smartphone. The most important is data from *WhatsApp* application and it is the databases. The database that we used is message database, where the message or the conversation stored, the database file named *msgstore.db.crypt12*. The database was encrypted, so need to decrypt it using tool *Smartphone Forensic System* with built-in *WhatsApp* Message Extractor and Decryption. After decryption, begin analysis the database from the database that decrypted open it through *WhatsApp Viewer* and it will shows all messages stored in the database. From the conversation between the victim and the perpetrator that viewed by *WhatsApp Viewer*, The perpetrator talking about selling smartphone after the victim sure and send the money the perpetrator ran away and lost contact. This evidence is sufficient to prove that the perpetrator committed online scam and the evidence can be brought to court.

4. Conclusion

From the research that we have done, there so much we can explore in forensics especially in mobile forensics. There are many tools we can use depending on our needs. In this research we are using *MOBILedit* to acquisition the smartphone mobile data, *Smartphone Forensic System* to decrypt the databases and using *WhatsApp Viewer* to view all message that stored in the database. The latest version of *WhatsApp,* the database always encrypted so we must decrypt or extract it first before we can use *WhatsApp Viewer* to shows all the data from it. This research use forensic method from NIST where the steps are identify or identification, collect data, analyze data and report the result. The evidence that obtain from those steps. The steps can be applied to any forensic for mobile to obtaining data from *WhatsApp.*

References

[1] Patroli Siber, "Patroli Siber", 10 Januari 2020, Available: https://patrolisiber.id/news/tren-kejahatan-siber-2019-penipuan-menempati-posisi-teratas [accessed:9-Oct-20].

[2] Wirara,Ayubi. Hardiawan, Bangkit. Salman, Muhammad. "Identifikasi Bukti Digital Pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan *WhatsApp*". *Teknoin,* vol. 26, no. 1, p.66-67, 2020.

[3] Ghannam, Hussein Abed. "Forensic Analysis of Artifacts of Giant Instant Messaging "*WhatsApp*" in Android Smartphone". *Journal of Applied Information, Communication and Technology,* vol. 5, no. 2, 2020

[4] Syahib, Muhammad Irwan, Riadi Imam, Umar Rusydi. "Analisis Forensic Digital Aplikasi *BEETALK* untuk Pengamanan *Cybercrime* Menggunakan Metode NIST". *SemnasIF,* 2018.

[5] Ramadhan, Muhammad Iqbal, Riadi, Imam. "Forensic *WhatsApp* base Android using National Institute of Standard Technology (NIST) Method". *International Journal of Computer Applications.* Vol. 177, No. 8, 2019.

[6] Egho-Promise, Dr.Iyobor, Ola, Bamidele, Arhin,Aaron, Asuming, Richard. *International Research Journal of Computer Science(IRJCS).* Vol. 7. 2020