HASIL CEK_60020397_Point-C12-IRD-850GB-FRAMEWORK ANALYSIS OF IDFIF V2 IN WHATSAPP INVESTIGATIONPROCESS ON ANDROID SMARTPHONES

by Imam Riadi 60020397

Submission date: 11-Dec-2020 09:43AM (UTC+0700)

Submission ID: 1471634764

File name: F_V2_IN_WHATSAPP_INVESTIGATIONPROCESS_ON_ANDROID_SMARTPHONES.pdf (504.72K)

Word count: 5461

Character count: 29470

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(3): 213-222
The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-0011

Framework Analysis of IDFIF V2 in WhatsApp Investigation Process on Android Smartphones

Rahadhian Dinnur Rahman[1], Imam Riadi[2]
[1]Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
(rahadhian1400018136@webmail.uad.ac.id, imam.riadi@is.uad.ac.id)

ABSTRACT

The development of technology that is increasing rapidly, may cause problems for users of the technology itself. One of the problems of abuse of technology like WhatsApp is used as a communication medium for committing crimes. Examples of these problems are the increasingly widespread fraud through WhatsApp, make deals and selling illegal drugs and others. Smartphones that are used to commit crimes can be confiscated by law enforcement officials as one of the evidences. The method of proving to obtain valid evidence is to conduct an investigation using a digital evidence handling approach known as digital forensics. Integrated Digital Forensics Investigation Framework version 2 (IDFIF v2) is one way of investigating smartphones. IDFIF v2 framework is the latest framework that has been developed so that it can be used for smartphone investigations. In this study there are several common stages, namely preparation, incident response, laboratory process and presentation. The final result of this study is to find an existing database on a smartphone and report on the results of analysis of smartphone evidence.

KEYWORDS

Forensic, WhatsApp, Evidence, IDFIF V2, Smartphone.

1 INTRODUCTION

Rapid technological development can cause problems for users of the technology itself, the more advanced people's lives, the more advanced crime will also be. Crime also becomes part of the culture itself, which means that the higher the level of culture and the more modern a nation, the more modern the crime is in its form, nature and manner of implementation, it can be seen from the applications on the smartphone.[1]

According to the official WhatsApp website more than 1 billion people in more than 180 countries use WhatsApp to stay connected with friends and family, anytime and anywhere. WhatsApp is free and offers the ability to send messages and make simple, safe and reliable calls, which are available for calls worldwide.

Given the high popularity and level of use of WhatsApp, the potential for abuse has also increased as has happened in SMS services. Message archives stored on the WhatsApp application installed on cell phones can be used as digital evidence to uncover crimes that use this application as a communication medium. One example of a real case of crime using WhatsApp is in the case of pornographic chat between Rizieq Shihab and Firza Husein. In this case it was explained that there were misuse of features such as conversations, voice recordings and photos of naked women who were included in pornographic content. Therefore, WhatsApp is used as evidence.[2]

The research that applies the new Integrated Digital Forensic Investigation Framework (IDFIF) V2 is applied to the SMS (Short Message Service) service. There is no research that applies IDFIF V2 to the WhatsApp application. Therefore, IDFIF V2 needs to be applied also to the WhatsApp investigation. IDFIF is the latest Framework that has been developed so that it is expected to be a standard method of investigation by investigators because IDFIF V2 has the flexibility to handle various types of digital evidence.[3]

Thus, seeing from the problems that occur such as the rise of digital crime cases that use WhatsApp application media as a communication tool, the researchers conducted research using the IDFIF Framework because the investigation process will be more structured and scheduled. It is expected to provide solutions to problems in crime cases that use WhatsApp as the communication media.

2 BASIC THEORY

2.1 WhatsApp

WhatsApp is free and offers the ability to send messages and make simple, safe and reliable calls, which are available for calls worldwide. WhatsApp Messenger is a communication medium that allows exchanging messages without SMS costs because WhatsApp Messenger uses the same internet network for email, web search, and more. The WhatsApp Messenger app uses a 3G or Wi-Fi connection for data communications.[4]

2.2 Digital Forensic

Digital Forensic Investigation is a rapidly growing field involved in the Information Technology era emergent. It indicates the numerous techniques how the crime in a computer system is handled which occupied from the very lowest part end user to the highest level. [5]

Forensics entails the use of science to determine matters of fact where such facts are required to settle disputes (for example, in courts of law) or to determine the root cause of an event of interest. Forensics employs the notion that scientific knowledge is true and hence a good basis to settle such disputes and/or determine causes. Digital forensics is that branch of forensics that studies evidence that exists in digital form.

Digital forensics is a part of forensic science that covers the discovery and investigation of material (data) found in digital devices (computers, cellphones, tablets, PDAs, net-working devices, storage, and the like) Digital forensics can be further divided into related forensics with computers (hosts, servers), networks (networks), applications (including databases), and devices (digital devices). Each has its own deepening. Digital forensics is a part of forensic science that covers the discovery and investigation of material (data) found in digital devices (computers, cellphones, tablets, PDAs, net-working devices, storage, and the like) Digital forensics can be further divided into related forensics with computers (hosts, servers), networks (networks), applications (including databases), and devices (digital devices). Each has its own deepening. [6]

2.3 Mobile Forensic

Digital forensic has many branches, one of which is mobile forensics. Mobile forensics is a branch of digital forensics that deals with the recovery of digital evidence or data from a smartphone device database. Mobile devices usually refer to smartphones, but can also relate to digital devices that have internal memory and communication capabilities.[7]

In forensics activities have a purpose, one of which is to help restoring, analyzing, and presenting digital material / entities or electronics in such a way that they can be used as valid evidence in court.[8]

Mobile Forensic is needed because mobile-based services are increasing and getting more users, with the growing popularity of mobile computing and mobile commerce, the need of mobile transactions are also getting higher. The quality and speed of the mobile service provider must be comparable to the number of mobile transactions that occur.[9]

Mobile phones become thus omnipresent and play such an oversized social group role, there's a high chance that these same devices are going to be a part of those investigations.[10]

2.4 Oxygen Forensic Suite

Oxygen Forensic Suite provided general information about the smartphone and the network that the device was connected to. The tool recovered all contacts, SMS and MMS messages, and user's files. Likewise, all non-removed memos, anniversaries, and meetings defined in the calendar and also to-do entries were extracted. It acquired all email messages that were stored on the mobile phone. Additionally, Oxygen Forensic Suite gathered event logs up to 30 days. Based on the event logs and their corresponding date and time, Timeline feature organizes and sorts all SMS and MMS messages, emails and Internet connections. [11]

2.5 MOBILedit Forensic Express

MOBILedit is a forensic tool that allows investigators to logically obtain. This tool uses several connectivity mechanisms, especially wireless connectivity rather than similar tools. This software is good enough to be used to obtain phone system information and other information such as contacts and text messages.[12]

Mobiledit Lite is an open source tool for mobile forensics using which address book, SMS, Media files, Notes and Files can be analysed. Backup of the phone can be created so that further analysis is not carried out on the evidence itself. The software is able to identify the IMEI (International Mobile Equipment Identity) number of the mobile phone. It has been blacked out in the image for security purposes. These are the features provided by the free version.[13]

2.6 Andriller

Andriller is one of the software that can be used for forensic analysis purposes on smartphones. This application is a cross platform application that operates on Microsoft Windows and Ubuntu Linux. Andriller has the ability to perform non-destructive analysis on Android devices, such as : extracting and decoding data automatically, unlocking the lockscreen pattern, lifting the SMS and MMS data, and application databases.Andriller can also generate reports in HTML and Excel formats. Andriller is a paid smartphone forensic software to acquire data that can run on Windows and Linux operating systems. Andriller has features such as Lockscreen Decoding, Gesture Pattern Decoding, Code-Cracking PIN Lock screen, Lock Screen Password Cracking, Bruteforce Lockscreen Password, Decrypt Encrypted Database, and Decrypt and Merge Multiple Database. Andriller is a utility with a group of forensic tools for smartphones. Part of these bundled tools are specialized in android forensic. It performs read-only, forensically sound, non-destructive acquisition from Android devices. [14]

2.7 IDFIF V2

IDFIF is the latest Framework that has been developed so that it is expected to be a standard method of investigation by investigators because IDFIF V2 has the flexibility to handle various types of digital evidence.[3]

IDFIF (Integrated Digital Forensic Investigation Framework) Version 2 which is a model for the process of investigating the digital evidence and claimed to have complete stages and can accommodate all stages of the cybercrime investigation process. After analyzing the investigation process, IDFIF V2 has several stages that have been modified so that it has been in accordance with the investigation procedure and the process of confiscation of evidence found at the crime scene. [15]

3 METHODOLOGY

In this study researchers used a case study simulation to apply IDFIF V2 to analyze WhatsApp on smartphones. This simulation was carried out with the aim to test IDFIF V2 on the WhatsApp application that is on the smartphone to look for proof of the message to commit a crime and make the contents of the message into evidence.

In summary, the methods and stages of the research carried out can be described as in Figure 1

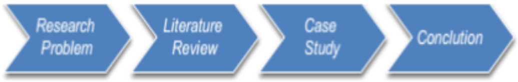


Figure 1. Methods and Stages of Research

Figure 1 is the method there are several stages of research are:

1. The research problem is the first step taken to obtain and determine research topics to be studied further. At this stage, it begins by looking at various phenomena, events, and information obtained in various ways.
2. The literature review is expected to explore all the information related to the issues to be studied and the object of the research objectives and provide the basis for the direction of research that will be conducted and become the beginning of thinking for each researcher so that research can be used as the reference again in the future.

3. Case Study is the process of applying IDFIF Version 2 to Web-based WhastaApp Messenger investigation process. as shown in Figure 2.

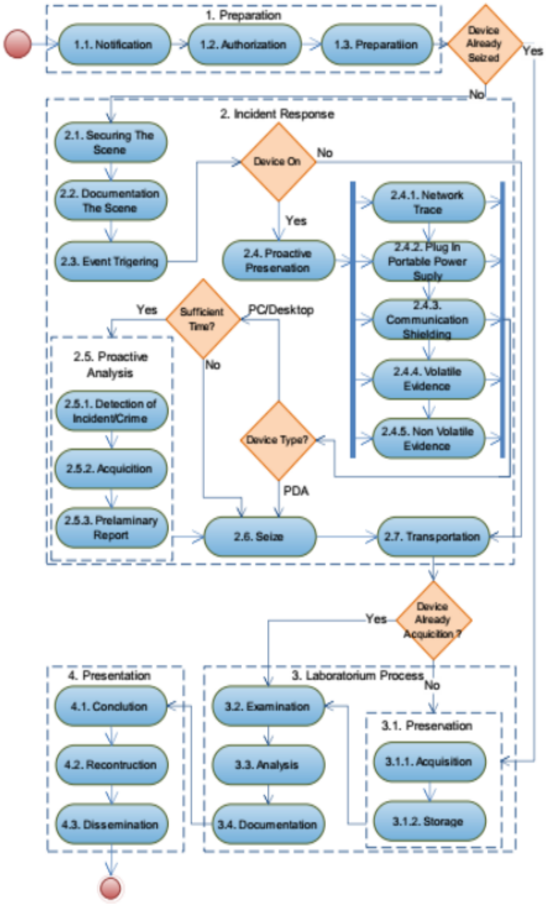


Figure 2. IDFIF V2 [3]

Figure 2 , is the result of research that has several stages in handling digital evidence, that is:

a. Preparation

It is a preparation that must be done to conduct the investigation process in handling digital evidence starting from the event of the case to the making of the final report.

1) Notification: Notification of investigation or report of a crime to law enforcers.
2) Authorization: Stages to gain access to evidence and legal status of the inquiry process.
3) Preparation: Preparation that includes the availability of tools, personnel and various needs of the investigation.

b. Incident Response

It is an activity carried out at the scene of the case with the aim of securing the existing digital evidence so as not to be contaminated by other matters.

1) Securing The Scene: Conduct a mechanism to secure crime scenes and protect the integrity of evidence.
2) Documentation The Scene: The main objective of this stage is to process the crime scene, search for trigger sources of events, search for communication or network connections and document the scene by taking pictures of every detail of the scene.
3) Event Triggering: Perform a preliminary analysis of an event process that occurred.
4) Proactive Preservation: Has 5 substages of network trace perform trace search through the network used by digital evidence.
    a) Plug in a portable power supply is a process of securing digital evidence with the condition "on" so that the power contained in digital evidence can be maintained during the trip up to the forensic laboratory.
    b) Communication shielding is a phase of data communication deactivation in digital evidence so as to prevent changes in data from outside.
    c) Volatile and Non-Volatile Evidence is a process of securing digital evidence. At the end of the proactive Preservation stage, there is a decision process. This stage is not called directly into stages, but the output of this decision is also important for the continuity of the investigation process. From this stage, it was decided that digital evidence should be immediately confiscated and further examination in the forensic laboratory or conducted on-site inspection to obtain an initial report of the incident.
5) Proactive Analysis: the live analysis stage of the inventory and build the initial hypothesis of an event. Detection of Incident / Crime, at this stage, is the stage, to ensure that there has been a violation of the law. The acquisition is the process of data acquisition of

inventory items so as to lighten the workload of digital forensic analysis in the laboratory. Preliminary Report is a preliminary report on the proactive investigation that has been done.

6) Seize: Perform the confiscation of digital evidence that has been found for further analysis.
7) Transportation: Is the process of moving digital evidence from the scene to the forensic digital laboratory.

c. Laboratorium Process

After the handling of digital evidence at the scene of the case, then at this stage is to process the data analysis of evidence that has been obtained previously so that can be found the type of crime that has occurred.

1) Preservation: Maintains the integrity of the findings by using a chain of custody and hashing functions.
2) Examination: Processing evidence to find its relevance to events.
3) Analysis: Is a technical study and assembles the linkages between the findings.
4) Documentation: Documentation of all activities that have been done from the beginning of the investigation process to the end of the analysis process in the forensic laboratory.

d. Presentation

This is the final stage in the process of digital investigation. At this stage is the process of making reports related to the results of the analysis performed in the previous stage and ensure that each process is done in accordance with applicable law rules.

1) Conclusion: Summing up the results of the investigation that has been done.
2) Reconstruction: The process of analysis and an overall evaluation of the results of the investigation.
3) Dissemination: The recording of the investigation process and the records may be disseminated to other investigators who are conducting similar cases.

4. The conclusion is the process of all the stages that have been done in the process of this research from the process of handling physical evidence and get digital but goods in the form of variables related to the conversation time, the content of the message conversation, the profile of the perpetrator and the victim on WhatsApp messenger, and the data can be analyzed whether in accordance with the reporting of victims and there is a crime, to the final stage of making a final report to be presented in court to strengthen evidence in a crime.

4 RESULTS AND DISCUSSION

The step of this research starts from the report that goes to the police, obtains evidence, identifies evidence, acquires evidence, looks for data that is in evidence until it analyzes the data obtained from the evidence and concludes it. The identification phase is done to obtain digital evidence obtained from the smartphone, in the form of a database of message conversations in the WhatsApp application. After the identification phase, the next step is to analyze the database that has been obtained by implementing the Integrated Digital Forensic Investigation Framework Version 2 (IDFIF V2). The Integrated Digital Forensic Investigation Framework Version 2 (IDFIF V2) can be seen in Figure 3.

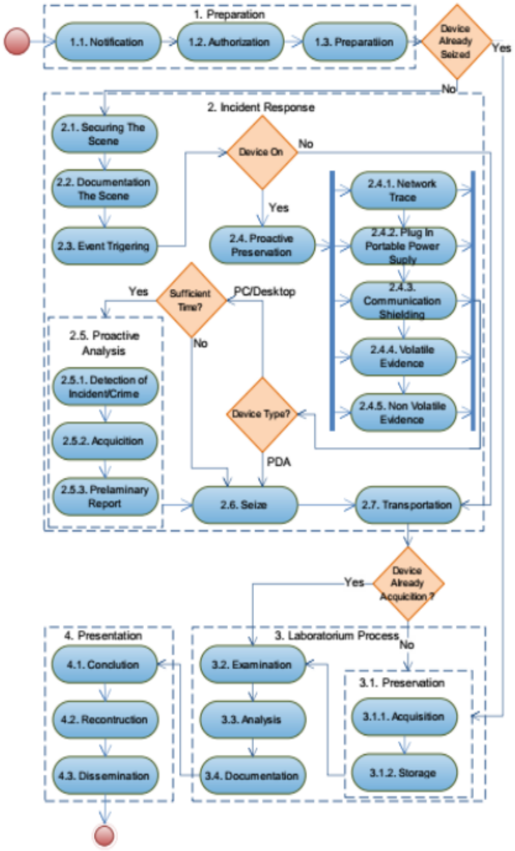


Figure 3. IDFIF V2[3]

Figure 3.[3] step Integrated Digital Forensic Investigation Framework Version 2 (IDFIF V2) on the investigation, The main stages of IDFIF Version 2 consist of 4 stages, namely preparation, incident response, laboratory process, and presentation which will be implemented in this study.

4.1 Preparation: is the initial stage of the investigation of evidence. At this stage, the preparation of the investigation is to prepare equipment and various documents needed. This stage is divided into 3 sub-stages, namely:

a. Notification: People report concerns about the circulation or sale and purchase of drugs through WhatsApp. After reports, the responsible authorities or police can be determined based on the geographical criteria for the location of the crime scene or the nature of the crime committed. This reporting is important because the information collected at this stage can determine the next step in the investigation.

b. Authorization: The authorities, namely the police, have collaborated with related parties to conduct investigations.

c. Preparation: The authorities, namely the police, prepares all needs and needs in the investigation process starting from personnel to carry out searches in order to obtain evidence of the perpetrator, investigation equipment to support investigations, hardware and software.

4.2 Incident Response: is the initial stage in the investigation process. Because the existence of the perpetrator has been known, the investigator goes to the place where the perpetrator has been known to be in the process and then carries out the arrest procedure for the perpetrator. The incident response stages are as follows:

a. Securing The Scene: The investigator and the authorities carry out the process of guarding and securing the crime scene so that in actual circumstances such as when seen and found officers who carry out the first action at the crime scene so that the evidence is not lost, damaged and unchanged such as a reduction or addition and the location of evidence has not changed so as not to influence the investigation process and change the results of the investigation so that others cannot deny it.

b. Documentation The Scene: The investigator performs documentation at the crime scene by photographing the crime scene and photographing evidence found at the crime scene. Evidence found successfully as in the Table 1.

Table 1. Evidence

No	Evidence	Picture	Explanation
1.	Smartphone		Evercoss A28A smartphone In a live state, connected to the network, and in the Root state.

c. Event Triggering: if the Securing The Scene stage is that the investigator secures the crime scene has been carried out, after that the investigator carries out the initial analysis of the case and looks for the cause of the crime at the scene so that the investigator can conclude that the type of crime committed is not in accordance with the report It is mandatory to further process it in a digital forensic laboratory.

d. Proactive Preservation: The investigator secures the Smartphone evidence found at the scene so that the evidence can maintain the integrity of the data contained therein until analysis in the digital forensic laboratory.

1) Plug in portable power supply: The investigator secures the digital evidence on the smartphone by charging the smartphone evidence using a portable power supply because the smartphone battery is not fully charged, the battery charging process is required to use a portable power supply to maintain the condition of smartphone evidence in "on" condition to the digital forensic laboratory for further investigation to obtain information about evidence of drug transactions through the WhatsApp application.

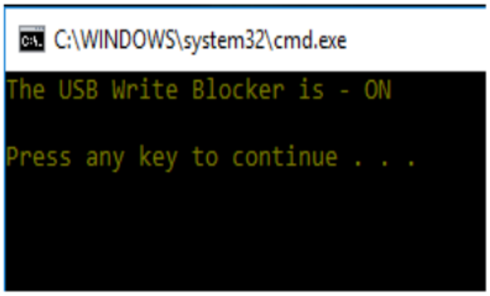
2) Communication shielding: At this stage, the Investigator secures the smartphone evidence found at the crime scene by disconnecting the smartphone from the network so that it does not experience changes in the data on the evidence, and the evidence found is not connected to any network.

e. Seize: the investigator takes action to confiscate evidence found at the crime scene.

f. Transportation: The investigator performs the procedure for transferring evidence, namely the smartphone device from the crime scene to the digital forensic laboratory for further investigation. In this process, the smartphone must be maintained and stored safely to the digital forensic laboratory so that the smartphone evidence remains in good condition and maintained.

4.3 Laboratory Process: Process Laboratory is the core stage of the smartphone investigation process. At this stage, the smartphone that has been obtained in the previous process is analyzed to obtain evidence related to the crime. This stage is divided into several stages, namely:

a. Preservation: The investigator carries out the process of securing smartphone evidence. The condition of the smartphone when the acquisition process must be disconnected from the existing network data communication. Before the investigator acquires data, the investigator activates the USB write blocker on the laptop that is used to make acquisitions as can be seen in Figure 4



```
The USB Write Blocker is - ON

Press any key to continue . . .
```

Figure 4. USB Writeblocker

In Figure 4 above it can be seen that the USB write blocker on the laptop used for the acquisition of evidence has been on or has been active. The USB write blocker serves as protection during the data acquisition process to evidence. Write blockers are needed because of the nature of the computer operating system that automatically changes 39 metadata files on storage media, and in addition to preventing the writing process of data acquisition from malicious applications such as viruses and spyware.

1) Acquisition: The investigator takes digital data evidence from a Smartphone device found at the scene.
Acquisition Smartphone imaging internal memory is carried out for the acquisition process using the Oxygen forensic suite application which is imaging data in internal memory to find WhatsApp conversations to find out the perpetrator identity profile, message information and conversation time.

2) Storage: The investigator prepares the storage in the designated laptop investigator directory to store backups of digital evidence data coming from smartphones that have been backed up. In this study, the investigator has prepared a special directory to store digital evidence of disk evidence E: \ backup digital evidence \ on a Laptop investigator. The contents and form of digital evidence will be stored in a safe and sterile place, to ensure that digital evidence cannot be changed because if the digital evidence undergoes a slight change it will change the results of the investigation.

b. Examination: The investigator checks to find evidence related to the case being handled on the perpetrator's smartphone device. For checking digital evidence on smartphones by exploring digital evidence in order to find evidence that is the conversation about drug buying and selling on the WhatsApp database on the smartphone device of the perpetrator. For the next stage, exploration of devices, namely:

1) Digital evidence exploration
At the stage of digital evidence exploration, namely finding the WhatsApp database on a smartphone, to find the WhatsApp database on a smartphone device can be seen in Figure 5

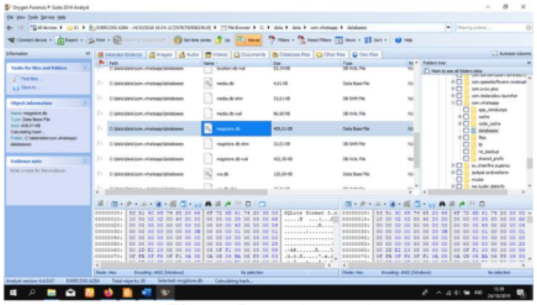


Figure 5. Database WhatsApp

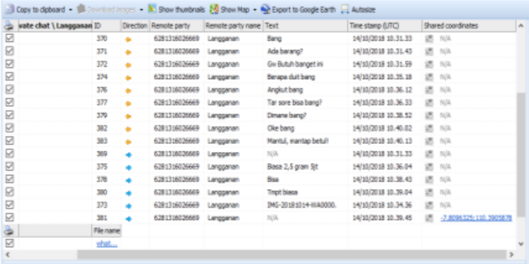
In Figure 5 the Oxygen application successfully finds the WhatsApp application database. The WhatsApp application database storage location can be seen in Table 2.

Table 2. WhatsApp Database File Storage Location

File Type	Storage location	File Name
Database WhatsApp	C:\data\data\com.whatsapp\databases	Mgstore.db.

In table 2, the WhatsApp database is explained in the laptop investigator in the directory:
c: \ data \ data \ com.whatsapp \ databases

c. Analysis: at this stage, the investigator conducts studies related to fraud cases and digital evidence in the can, then the next investigator to extract the database contained in the laptop and smartphone devices to be able to detail information on the evidence in the can, the first stage of the process of extraction against the WhatsApp database on smartphone devices. After carrying out the inspection process of the smartphone, the investigator conducts a technical review and arranges the linkages between the findings that exist between the actor and the smartphone that is obtained. In some cases, sometimes it requires the collection of physical and logical evidence in the form of data extraction, but in this case, the necessary evidence is the conversation between the perpetrator (drug dealer) and the buyer, the time of conversation, and the identity of the perpetrator's profile located on the smartphone's internal storage. The buyer asks the actor whether there is an item (drug), then the perpetrator and the buyer plan a meeting somewhere to conduct drug buying and selling transactions. The message sent by the buyer to the perpetrator can be seen in Figure 6.



	vate chat \ Langganan	ID	Direction	Remote party	Remote party name	Text	Time stamp (UTC)	Shared coordinates
☑		370	→	6281316026669	Langganan	Bang	14/10/2018 10.31.33	N/A
☑		371	→	6281316026669	Langganan	Ada barang?	14/10/2018 10.31.43	N/A
☑		372	→	6281316026669	Langganan	Gw Butuh banget ini	14/10/2018 10.31.59	N/A
☑		374	→	6281316026669	Langganan	Berapa duit bang	14/10/2018 10.35.18	N/A
☑		376	→	6281316026669	Langganan	Angkut bang	14/10/2018 10.36.12	N/A
☑		377	→	6281316026669	Langganan	Tar sore bisa bang?	14/10/2018 10.36.33	N/A
☑		379	→	6281316026669	Langganan	Dimane bang?	14/10/2018 10.38.52	N/A
☑		382	→	6281316026669	Langganan	Oke bang	14/10/2018 10.40.02	N/A
☑		383	→	6281316026669	Langganan	Mantul, mantap betul!	14/10/2018 10.40.13	N/A
☑		369	←	6281316026669	Langganan	N/A	14/10/2018 10.31.33	N/A
☑		375	←	6281316026669	Langganan	Biasa 2,5 gram 5jt	14/10/2018 10.36.04	N/A
☑		378	←	6281316026669	Langganan	Bisa	14/10/2018 10.38.43	N/A
☑		380	←	6281316026669	Langganan	Tmpt biasa	14/10/2018 10.39.04	N/A
☑		373	←	6281316026669	Langganan	IMG-20181014-WA0000.	14/10/2018 10.34.36	N/A
☑		381	←	6281316026669	Langganan	N/A	14/10/2018 10.39.45	-7.8096329;110.3905878
		File name						
☑		what...						

Figure 6. Proof of the Contents of WhatsApp Conversation

In Figure 6 can be seen evidence of conversations between perpetrators (drug dealers) and buyers. As shown above, the message is known as a private message type, it can also be seen that the message ID, direction message, remote party (buyer number), remote party name (buyer contact name), text (message content), UTC timestamp (conversation time)), shared coordinates (location coordinates). Conversations between actors (drug dealers) and buyers detected by the Oxygen application are types of private messages because they are only done by two people. Buyers' WhatsApp numbers detected can be seen in the remote party column. The contact name of the buyer has also been detected and can be seen in the remote party name column. All contents of conversations between actors (drug dealers) and buyers can be seen in the text column. In the time stamp (UTP) column it can be seen when the time of the conversation occurs. Whereas the shared coordinates column can be seen if the perpetrator shares the location message with the buyer. On message ID number 373 it appears that the perpetrator (drug dealer) sends a picture message detected by the Oxygen application with the name

IMG-20181014-WA0000. The contents of the picture message can be seen in Figure 7. below:

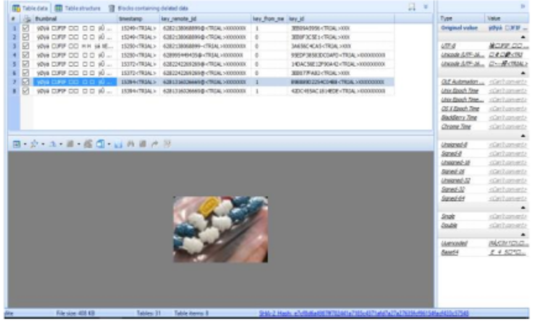


Figure 7. Picture Message

In Figure 7, it can be seen that there is a picture of a hand on the hand, there is one sheet of medicine that can be ascertained based on its form is illegal drugs. Fill in the picture message with ID 373 in the form of a picture message opened by the investigator using the same application, Oxygen Forensic SQLite Viewer. Messages with ID 381 in the share coordinates column can be seen in Figure 6 the perpetrator sent a location message. Coordinate message location can be seen using Google Maps which is integrated with the Oxygen application can be seen in Figure 8 below:

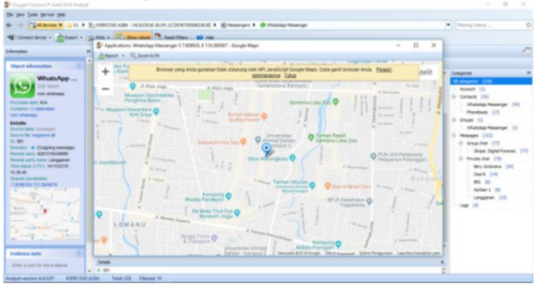


Figure 8. Location of Drug Transactions

Figure 8 describes the coordinates that can be seen on Google Maps where the location is located.

d. Documentation: After the analysis phase of the smartphone digital evidence found at the crime scene, the next stage the investigator assembles all the data and information found at the analysis stage to be processed into evidence in a criminal case that has sufficient information to be submitted to the party parties who have authority in the field of law. Data and information are presented in the form of information that can be understood and supported with evidence in accordance with the sufficient and acceptable crime. The data is made in the form of a .pdf file format with the name of the Report Report file and can be seen in the attachment sheet.

4.4 Presentation : A presentation is the final stage of the investigation process. At this stage, the handling of evidence that has been done before, securing evidence in a safe place and the review stage in the investigation of evidence of a crime that has been carried out for repairs in the next investigation process.

a. Conclusion: The evidence and information obtained in the investigation process by the investigator are sufficient for the investigation team to make demands on the conversation perpetrators of drug buying and selling transactions through WhatsApp media and can enter the perpetrator into custody with evidence that has been investigated.

b. Reconstruction: At this stage, the investigator reconstructs based on the findings of the investigative analysis carried out so that the perpetrator's activities can be known in the conversation of drug buying and selling through WhatsApp media.

c. Dissemination: Furthermore, in this final step is the recording process at the investigation stage so that if the researcher or investigator gets a similar case, this investigation process can be a reference in the process of analyzing WhatsApp forensic smartphone investigations.

5. CONCLUSION

WhatsApp is a popular application for social networks where people can exchange personal information between users. This study uses Integrated Digital Forensic Investigation Framework Version 2 which functions to find digital evidence in the form of databases originating from smartphone evidence. The WhatsApp database that was found was then extracted using the oxygen forensic application that produces information related to the conversation time, user profile, and conversation content. The results of the evidence found were then made a case report, to be used as evidence in court. Case report can be seen in Table 3.

Table 3. Case Report

Common Information	
Evidence number	1
Inspector	Rahman
Case name	Drug transactions
Retail name	Evercoss A28A
IMEI	357673050823619
Serial number	SANZDWKB6RG7TTGSOV8
Software revision	4.4.4

In table 3, describes the report on the investigation of the evidence. The contents of WhatsApp messages that have been identified contain cybercrime, namely drug transactions. Can be seen in Figure 6.

REFERENCES

[1] A. Farjamfar, M. T. Abdullah, R. Mahmod, and N. I. Udzir, "A Review on Mobile Devices Digital Forensic Process Models," vol. 8, no. 3, pp. 358–366, 2014.

[2] A. R. Pratama, "Whatsapp Forensics: exploration of file systems and databases on Android and iOS applications," vol. 20, pp. 1–11, 2014.

[3] I. Riadi, Y. Prayudi, and Ruuhwan, "Application of Integrated Digital Forensic Investigation Framework v2 (IDFIF) in the Smartphone Investigation Process," vol. 2, 2016.

[4] S. Ikhsani and B. C. Hidayanto, "Forensic Analysis Whatsapp and LINE Messenger Provide Strong and Valid Evidence in Indonesia," vol. 5, no. 2, 2016.

[5] T. Authors, T. Url, P. Date, and A. This, "Digital forensics trends and future," 2014.

[6] B. Raharjo, "Overview of digital forensics," *sosioteknologi*, vol. 29, pp. 384–387, 2013.

[7] F. Karpisek, I. Baggili, and F. Breitinger, "WhatsApp network forensics : Decrypting and understanding the WhatsApp call signaling messages," *Digit. Investig.*, pp. 1–9, 2015.

[8] B. Nugraha *et al.*, "WhatsApp Forensics on Android Smartphone : A Survey," no. February 2017, 2016.

[9] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android ' s," vol. 15, no. 5, pp. 3–8, 2017.

[10] M. M. N. Umale, P. A. B. Deshmukh, and P. M. D. Tambhakhe, "Mobile Phone Forensics Challenges and Tools Classification : A Review," no. March, pp. 622–626, 2014.

[11] S. Mohtasebi and A. Dehghantanha, "Smartphone Forensics : A Case Study with Nokia E5-00 Mobile Phone," vol. 1, no. 3, pp. 651–655.

[12] A. Fadlil, "Evidence Gathering and Identification of LINE Messenger on Android Device," vol. 16, no. 5, pp. 201–205, 2018.

[13] R. Lohiya and P. John, "Survey on Mobile Forensics," vol. 118, no. 16, pp. 6–11, 2015.

[14] A. Abdallah, M. Alamin, A. Babiker, and A. N. Mustafa, "A Survey on Mobile Forensic for Android Smartphones," vol. 17, no. 2, pp. 15–19, 2015.

[15] B. Actoriano and I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," no. September, 2018.

HASIL CEK_60020397_Point-C12-IRD-850GB-FRAMEWORK ANALYSIS OF IDFIF V2 IN WHATSAPP INVESTIGATIONPROCESS ON ANDROID SMARTPHONES

ORIGINALITY REPORT

9%	5%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	journaldatabase.info Internet Source	3%
2	www.igi-global.com Internet Source	1%
3	Randi Rizal, Missi Hikmatyar. "Investigation Internet of Things (IoT) Device using Integrated Digital Forensics Investigation Framework (IDFIF)", Journal of Physics: Conference Series, 2019 Publication	1%
4	Submitted to West Salem High School Student Paper	1%
5	Submitted to John F. Kennedy Memorial High School Student Paper	1%
6	Submitted to Institute of Technology Blanchardstown Student Paper	1%

7	Submitted to Texas A&M University, Texarkana Student Paper	1%
8	www.ijritcc.org Internet Source	1%
9	Submitted to Indiana University Student Paper	1%
10	Ruuhwan Ruuhwan, Imam Riadi, Yudi Prayudi. "Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone", Jurnal Edukasi dan Penelitian Informatika (JEPIN), 2016 Publication	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		