Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method

Muhammad Iqbal Ramadhan
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
WhatsApp Messenger is a popular Instant Messaging (IM) application that is widely used in the 2017-2019 range. A large number of WhatsApp Messenger users will certainly have a positive and negative impact, the negative effects that are usually found are cases of crimes such as fraud into cybercrime crimes. The way to prove the perpetrators of the crime is to find evidence through digital forensics. This case will be revealed by one branch of digital forensics, namely mobile forensics because the evidence obtained is a smartphone which is a mobile device. This research uses the method of the National Institute of Standard Technology (NIST). NIST is a method that conforms to standards in the forensic field and has 4 forensic stages namely Collection, Examination, Analysis, Reporting. The results of this study are a comparison of evidence between a smartphone in a smartphone and a smartphone without a smartphone. The rooted smartphone managed to get an 11 encrypted and 1 decrypted conversation database, 152 images received and 60 sent, 8 conversation times, 8 video notes, 3 folder voice notes, 1 document sent and 5 received. Smartphones not rooted only managed to get evidence in the form of text conversations and the time of sending messages.

Keywords
Forensic, Mobile, WhatsApp, Android, NIST, Cybercrime.

1. INTRODUCTION
The development of the digital world also impacts on the development of communication technology, many Instant Messaging (IM) applications are used by users to communicate every day. Lots of instant messaging applications such as Blackberry Messenger (BBM), Line, WhatsApp Messenger, Imo, Telegram, etc. One of the applications that are growing rapidly and has many WhatsApp Messenger users. The WhatsApp application is a messaging application for smartphones and is a cross-platform message that allows users to exchange messages without the cost of SMS because WhatsApp uses internet packages to carry out these interactions [1]. WhatsApp not only functions as a sender or recipient of text, but also functions as a sender of media such as audio, video, documents, and can also make voice or video calls with contacts that are owned, but it also has features of view contact, copy-paste, status messages, broadcast, block [2]. WhatsApp users registered in 2017 around 1 billion users, this number has increased every year as in Figure 1.

Figure 1. 2017 WhatsApp Users

Security is also a challenge in the rapid development of technology today. A large amount of user data must save the potential for cybercrime crime. Cybercrime itself is a crime committed in cyberspace by utilizing computer technology or internet networks [3]. Cybercrime has many types, including cyber espionage, cyber sabotage, and extortion, an offense against intellectual property, cracking, cyberbullying, carding [4]. Data of all application activities are generally stored in a database that has a certain encryption format, to be able to see all the information in the database the data decryption process must be done first. According to a report from Hackmageddon in February 2017 stated that the amount of cybercrime crime was 64.5%. Cybercrime cases require special handling because evidence must be obtained and prove the crime.

This research will be informing cybercrime crime by using the WhatsApp application that runs on the Android platform using the National Institute of Standard Technology (NIST) method to handle and solve cybercrime crime problems. NIST is a standardized method that can be used to solve and analyze digital evidence to get information from the evidence [5].

1.1 Literature Review
1.1.1 Previous Studies
This activity is carried out to find out if there is any research that has been done, as well as studying the research to find out what information can be obtained and how to resolve the problem. The following are some of the previous studies that were found and relevant to this research. Nuril Anwar and Imam Riadi (2017) with the title "WhatsApp Messenger Smartphone Forensic Investigation Analysis Against WhatsApp Web-Based" Managed to obtain information and evidence coming from the WhatsApp web and WhatsApp from Smartphone [6].

Guntur Maulana Zamroni, Rusydi Umar, Imam Riadi (2016) with the title "Forensic Analysis of Android-Based Instant Messaging Applications" managed to get evidence from unrooted smartphones [7]. Syukur Ikhsani and Bekti Cahyo Hidayanto (2016) with the title "WhatsApp Forensic Analysis and Line Messenger on Android Smartphones as a Reference in Providing Strong and Valid Evidence in Indonesia" managed to get the database structure from the conversation

[8]. Muhammad Kukuh Tri Haryanto (2018) with the title "Forensic Analysis of SQLite Database on Android-Based IMO Applications" managed to find the database structure on the IMO application [9]. Yesi Novaria Kunang Anggie Khristian (2017) with the title "Implementation of Forensic Procedures for WhatsApp Applications on Android Phones" managed to get evidence of artifacts from smartphones that serve as evidence [10].

1.1.2 Digital Forensic

Digital forensics is a way that includes the recovery and investigation of material found in digital devices. Digital forensics is used as an investigation of devices that can store digital data [11]. The opinion of another expert said that digital forensics is computer science and technology to examine and analyze every electronic evidence and digital evidence in order to see the relationship between digital evidence with other digital evidence so that the crime becomes clear and the perpetrators can be arrested to be responsible answer the crime [12]. Forensic stages have many versions, one of which is identification, maintenance, analysis, presentation [13].

1.1.3 Mobile Forensic

Mobile forensics is one of the fields of science originating from branches of the field of digital forensics, which deals in the recovery of digital evidence or data from mobile devices with accountable methods [14]. Another understanding expressed is that mobile forensics is the science or expertise in the process and managing digital evidence originating from mobile devices with the method is in accordance with the standard and can be justified [15].

1.1.4 Digital Forensic Mobile Evidence

Digital evidence is information obtained in digital format and cannot be directly used as evidence in the judicial process because according to its nature which is inconsistent and easily changed [16]. Mobile forensics has the main goal of finding and finding information proving a case that is stored and transmitted in digital form and can be used in court as evidence that has been processed and analyzed previously [17]. The rapid development of mobile devices technology and the increasing number of users causes the great potential for digital crime, a new fact states that mobile forensics is one of the important elements in digital forensics today [18].

2. RESEARCH METHODOLOGY

2.1 Research Steps

The initial stage in this research is data collection that is derived from literature studies and observations. A Literature study is a method of collecting data by reading documents related to sources and references such as journals, thesis, books. The second method is observation, namely by making direct observations using case scenario engineering then the process of identifying and analyzing the evidence obtained is carried out. Figure 2 is a research step carried out from the beginning to the discovery of evidence

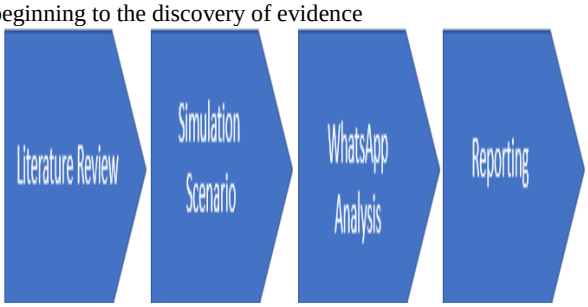

Figure 2. Research Steps

The process of finding this object in this research is based on research sources that have been done before, the second step is to simulate a case and create a scenario design to carry out the digital forensic investigation stage. Then, the WhatsApp evidence analysis phase, the activity to be carried out is to search for digital evidence. The final step is to make a digital forensic report analysis.

2.2 Research Scenario

The research scenario aims to explain the mobile forensic stages that are being handled in this study, Figure 3 scenarios are made to illustrate what cases are being handled. This research uses a case of fraud by informing suspects and victims who interact through WhatsApp on their respective smartphones.

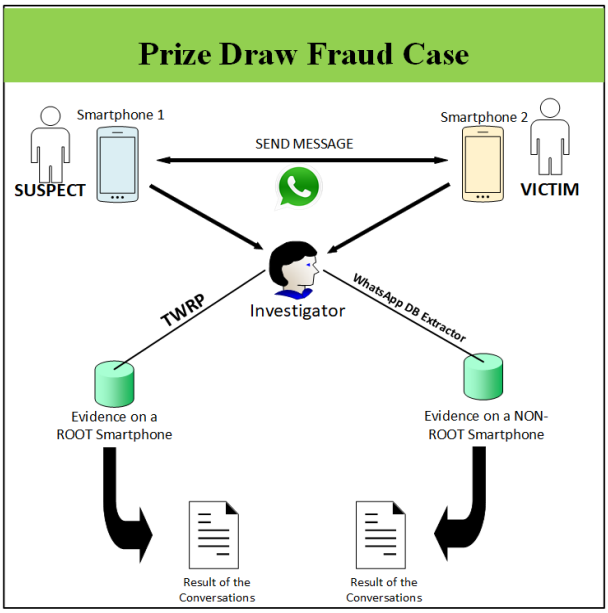

Figure 3. Research Scenario

The scenario depicts a suspect who deceives the victim by sending a gift message that must be redeemed by the victim. The investigator will take the evidence using the forensic process and do the imaging to secure the evidence so that it stays awake and does not change. Evidence of data that has been obtained will be extracted to see the results of conversations that have been carried out by the perpetrators and victims in each WhatsApp evidence. The state of both smartphones in a living condition and can turn on. The perpetrator's smartphone is rooting to get full access rights to the system, while the victim's smartphone remains in the initial condition ie not rooted.

2.3 Research Stages

The stages of the research aim to carry out simulations on how to use methods that are in accordance with the standards. One method often used to expose crime is the National Institute of Technology (NIST) method, Figure 4 below show the steps of NIST.

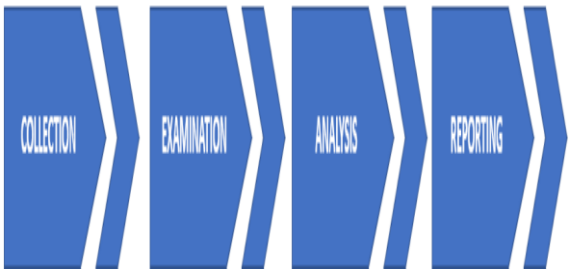

Figure 4. NIST Method

All steps are taken from the beginning to successfully obtain valid evidence and a report can be presented to the court to decide on a case.

2.3.1 *Collection*

The process of identifying, recording, collecting and taking evidence related to crime. This stage is looking for physical evidence that is a smartphone that is used to transact between the perpetrator and the victim. The evidence is secured so that it is not misused and the stored data is still maintained its integrity.

2.3.2 *Examination*

Data processing or checking stage of the collected evidence is then carried out backup data on both smartphones using forensic tools. This research uses forensic tools namely FTK Imager and ProDiscover Basic to perform data imaging processes. Figure 5 below shows the steps of the examination process of this research.

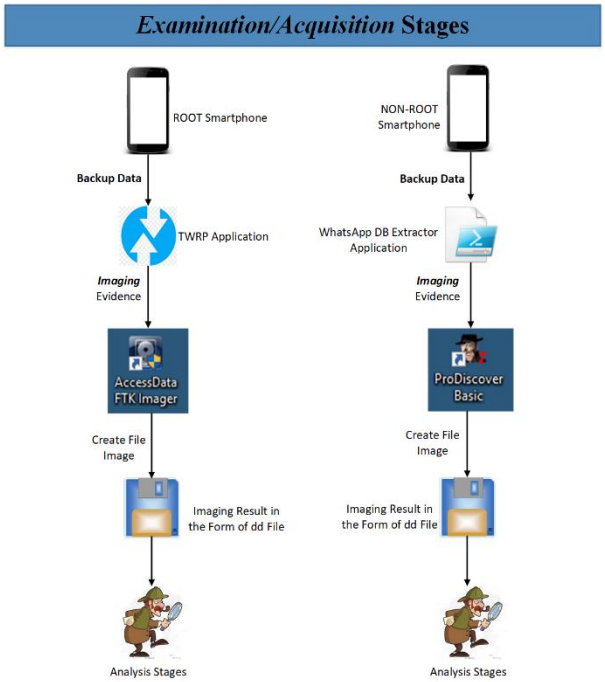

Figure 5. Acquisition Process

The data backup process on the rooted smartphone uses the TWRP application by backing up data from the android and internal smartphone partition system, after which the data is entered into other storage media for imaging processes using the FTK Imager tool. The process of data backup on a smartphone is not rooted almost the same as a smartphone that uses the WhatsApp DB Extractor tool then the evidence data is saved to the storage media and performed imaging with ProDiscover Basic tools.

2.3.3 *Analysis*

The process of an investigator analyzing evidence from imaging results in the previous stages to obtain further evidence related to this crime. Figure 6 is checks are done by reading the conversation evidence stored on a WhatsApp storage database.

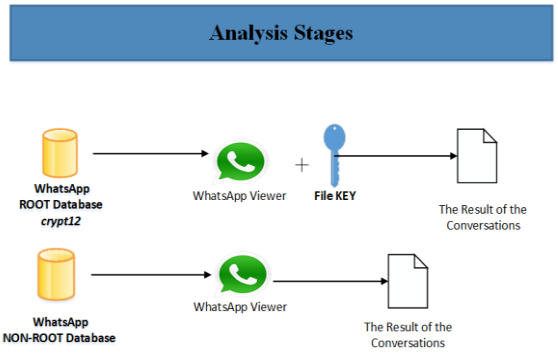

Figure 6. Analysis of Conversation Database

The results of the database that have been read then do the similarities between the conversations that are on the victim's smartphone and the perpetrator's smartphone. Evidence of the conversation is at the core of the case.

2.3.4 *Reporting*

This stage is the stage to write the results of the investigation process and the data obtained from all investigations. The report contains the results of the identification of the extracted image file from the evidence of smartphones being rooted and smartphones not rooted. This reporting process will also be brought to the trial process and must include all evidence found in the physical form and obtained from the forensic process.

3. RESULT AND DISCUSSION

The results of research that have been carried out succeeded in getting evidence on Android smartphones belonging to perpetrators and victims. The following is Table 1 which contains information about hardware and software needed in this study.

Table 1. Tools, Materials dan Specification

No.	Name	Specifications	Information
1.	Laptop	Lenovo G40-80, Windows 10	Hardware
2.	WhatsApp Messenger	Android Application v2.19.188	Software
3.	FTK Imager	Forensic Tools v3.4.3.3	Software
4.	TWRP	Backup Tools V3.1.1.0-Mido Redmi Note 4X	Software
5.	ProDiscover Basic	Forensic Tools	Software
6.	WhatsApp DB Extractor	Backup Tools V4.7 (official)	Software
7.	WhatsApp Viewer	Forensic Tools v1.9	Software

Applications that are in Table 2, are used to retrieve data on evidence. The evidence will later be carried out the imaging process using forensic tools and get the MD5 and SHA1 values to find out whether the evidence is identical and can be used for the analysis process or not.

3.1 Collection

The collection stage is the stage used for searching, collecting data, and documenting evidence. The evidence used in this study is a smartphone that is scanned as evidence of a crime. WhatsApp is currently using its database encryption, crypt12, WhatsApp will automatically backup according to the smartphone's settings. Figure 7 is a smartphone as evidence, the left smartphone is rooted, while the right smartphone is not rooted.

Figure 7. Smartphone Evidence

Table 2. Smartphone Evidence Specification

No	Name	Model Number	Imei & RAM	OS Version
1.	Xiaomi Note 4X (C31da8fd0504)	Redmi Note 4	-Slot 1: 867307039155941 -Slot 2: 867307039155958 -RAM: 3GB -Internal: 32GB	7.0 NRD90M
2.	Xiaomi Note 3 Pro (7aa3fa8d)	Redmi Note 3	861980036873488 -RAM: 2GB -Internal: 16GB	5.1.1 LMY47V

Table 2 is a specification table of the smartphone evidence found in this case. all evidence is secured so that the data contained therein is not contaminated and changed. This safeguard is also carried out for the purpose of maintaining the integrity of evidence data. digital evidence is very susceptible to change and if data security is not immediately carried out then it is possible that it could be used by someone who is not responsible

3.2 Examination

This stage is the stage for data acquisition in evidence on smartphones. The process carried out to obtain evidence on the smartphone is rooted using TWRP tools to back up the data first because the smartphone cannot be detected directly to the FTK Imager on the laptop being used. Figure 8 is the TWRP application that has been installed on the rooted smartphone.

Figure 8. TWRP in Root Smartphone

Data on the rooted smartphone will be backed up and stored into another storage media, namely the flash, after that the process of making the image is done through the flash. The acquisition results must be the same as the original file that is on the smartphone, to find out the same results or not checking through the MD5 and SHA1 values. Figure 9 is the MD5 and SHA1 hash values in the image file.

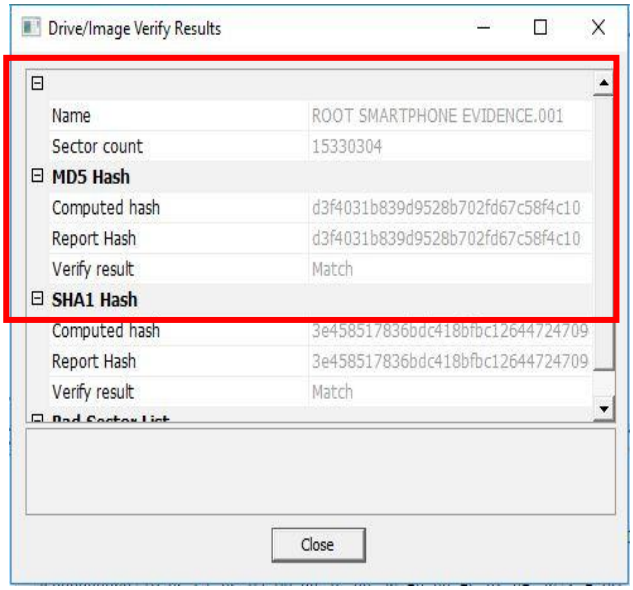

Figure 9. MD5 and SHA1 Hash Value

Data that on the smartphone is not rooted, it is backed up through the WhatsApp DB Extractor application. This is done because the smartphone is not rooted also can not be detected directly into ProDiscover Basic that is on the laptop used. Figure 10 is a WhatsApp DB Extractor application.

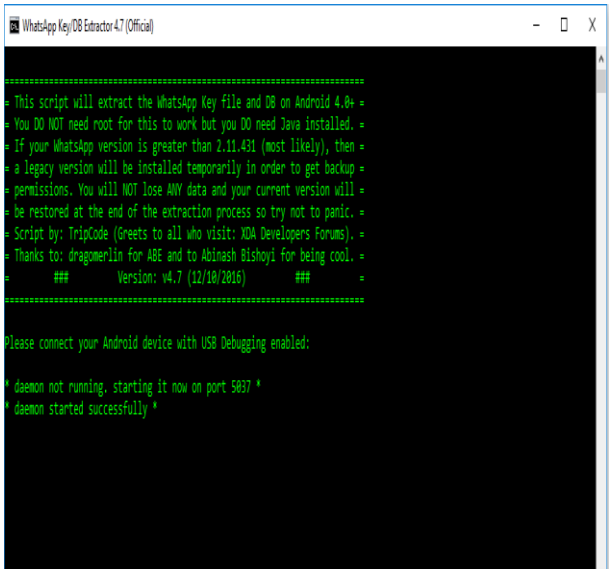

Figure 10. WhatsApp DB Extractor Application

Data backups originating from smartphones that are not rooted are also stored on flash disk storage media for imaging processes. The imaging process uses the ProDiscover Basic application. Figure 11 is a ProDiscover Basic application and MD5 value of imaging results.

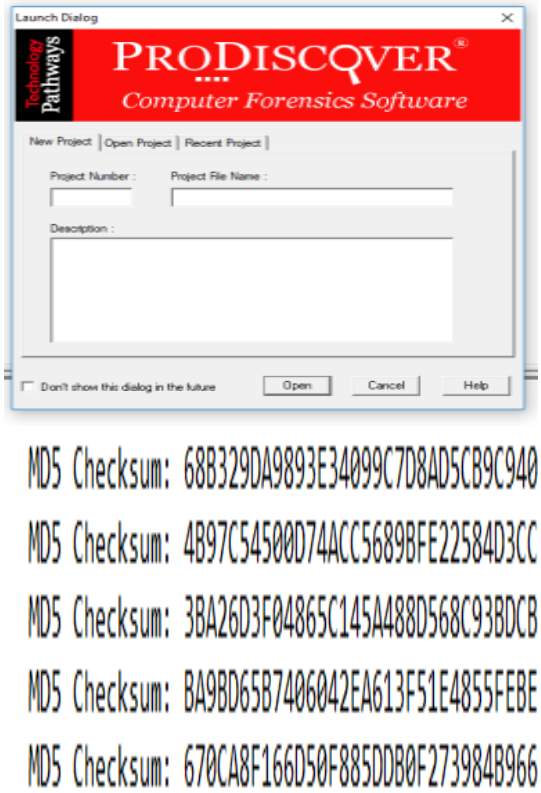

Figure 11. ProDiscover Basic Application and MD5 Hash Value

The data that has been obtained and the validity of the same level is based on the same MD5 and SHA1 value of the evidence, then extracted and enter the next stage, namely the analysis phase.

3.3 Analysis

The analysis process succeeded in finding evidence and extracted a conversation database to see the similarities between evidence on a rooted smartphone and a smartphone not rooted. Evidence on the smartphone being rooted managed to find two types of conversation databases originating from smartphone internal storage and android partitions, the different for two types of databases is their condition. The condition of the database on the android system is already in the decrypted condition and database decryption process is needed, while the database on the internal smartphone is still in an encrypted state so the decryption process needs to be done first. The process of encrypting the database that is still encrypted crypt12 is done by entering the key file that is on the Android partition. Figure 12 is the different types of databases obtained from Android partitions and those obtained from internal smartphones.

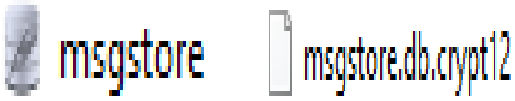

Figure 12. Android Partition Database Condition (left), Internal Smartphone (right)

Figure 13 is the result of a conversation that can be displayed using the Whatsapp Viewer application so it looks neater and is like reading directly on a smartphone. Conversation displayed on smartphones rooted and not rooted have the same content. The result of the conversation displayed on the WhatsApp Viewer application can also be exported in the form of text, HTML, and JSON. All of the export have their own appearance.

Figure13. Result of the Conversation

The conversation results obtained have in common with each other, besides that the evidence on the smartphone being robbed managed to get additional evidence such as image files, videos, documents, voice notes in the "media" directory. A Smartphone is not rooted only managed to get proof of conversation text as shown in Figure 13.

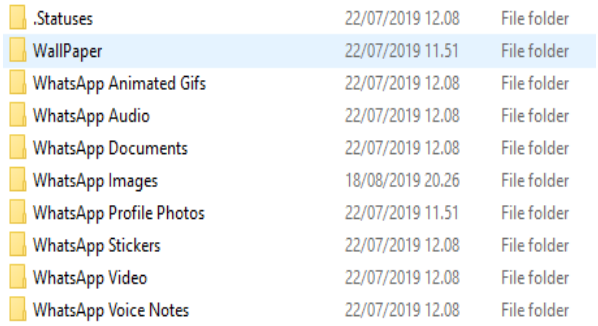

Figure 14. Media Directory

Figure 14 is the WhatsApp data successfully obtained from the smartphone's internal imaging process. The evidence that was found has exactly the same similarity as that of the smartphone of the perpetrator and the victim, this proves that the MD5 and SHA1 values from the imaging results are correct and there is no doubt the similarity.

3.4 Reporting

The reporting stage is the stage of reporting the results of the analysis relating to the case being handled, namely the analysis relating to the WhatsApp Messenger application which is used as a crime that has been scanned in this study. The following is Table 3 of the findings from the forensic process with the TWRP + FTK Imager tools (smartphone rooted) and WhatsApp DB Extractor + ProDiscover Basic (smartphones not rooted). Table 3 contains what data has been found and the number of details. the data found is exactly the same as the data in the smartphone which is used as evidence

Table 3. Evidence Findings

INFORMATION	SMARTPHONE 1 (ROOT)	SMARTPHONE 2 (NON- ROOT)
MOBILE PHONE NUMBER	08228157****	08222030****
APPLICATION VERSION	V2.19.188	V2.19.188
USERNAME	Gojek	Target
CONTACT	403	800
ENCRYPTED DATABASES	Yes (11)	No
AVATAR	Yes (308)	No
STICKER	Yes (37)	No
PROFIL PICTURES	Yes (1)	No
WHATSAPP AUDIOS	No	No
WHATSAPP CALLS	No	No
WHATSAPP DOCUMENTS	Yes - 1 (receive) - 5 (sent)	No
WHATSAPP IMAGES	Yes - 152 (receive) - 60 (sent)	No
WHATSAPP PROFILE	No	No
WHATSAPP VIDEO	Yes -8 (receive)	No
WHATSAPP VOICE NOTES	Yes 3 folder	No

The results above are the results obtained when the data is still in the smartphone and managed to find text messages, delivery times, contacts, pictures, documents, videos, voice notes, etc. When data is deleted from the smartphone it cannot find any evidence and fails to recover the lost data. That is because the smartphone cannot be detected directly by the forensic tools used, so the data that is on the smartphone must be backed up to other storage media first and cannot be directly imaging the smartphone.

4. CONCLUSION AND FUTURE WORK

Based on the results of this study have successfully raised evidence and still maintain the authenticity of data originating from smartphones Xiaomi Note 4X (root) and Xiaomi Note 3 Pro (non-root) viewed from the results of MD5 and SHA1 which have similarities. Evidence was obtained by backing up evidence from both smartphones and stored it in other storage media for imaging processes with forensic tools, the imaging results were then extracted and analyzed the level of conversation similarities from smartphones being rooted and not rooted and also searching for evidence other than conversation. The results obtained on the smartphone were key files, 11 (encrypted) and 1 (decrypted) conversation databases from different locations, 8 videos received, 152 images received and 60 sent, 1 document received and 5 sent, voice notes as many as 3 folders from different senders, while the smartphone is not rooted only managed to get the text conversation only. This research has not been able to find evidence that has been deleted and returned all the evidence, so it is hoped that further research can recover data that has been deleted by the suspect using different forensic tools, to obtain varied results.

5. REFERENCES

[1] Suryani, R. 2017. The function of Whatsapp Grup Shalehah in Bandar Lampung Branch as the Development of Da'wah Media in the Form of Ahlakul Kharimah. Lampung: Gadjah Pustaka.

[2] Rusni, A., & Lubis, E. 2017. Use of WhatsApp Online Media in One Day One Juz Community Activities (ODOJ) in Increasing ODOJER Tilawah Interests in Pekanbaru City. JOM FISIP.

[3] Wahid, A., & Labib, M. 2005. Mayantara Crimes

(Cybercrime). Jakarta: PT. Refika Aditama.

[4] Basariyadi, A. 2017. Cybercrime: Definition, Types, and examples [Online]. Available: https://www.google.com/url?sa=t&source=web&rct=j&url=http://koko.staff.gunadarma.ac.id/Downloads/files/63127/20171124-ForensikDigital.pdf

[5] Kent, K., & Chevalier, S. 2006. Guide to Integrating Forensic Techniques into Incident Response. Special Publication 800-86.

[6] Anwar, N., & Imam, R. 2017. WhatsApp Messenger Smartphone Forensic Investigation Analysis of WhatsApp Web-Based. Scientific Journal of Electrical Computer Engineering and Information Technology, 2(1), 1-10.

[7] Guntur, M., etc. 2016. Forensic Analysis of Android-Based Instant Messaging Application. Annual Research Seminar, 2(1), 102-105.

[8] Ikhsani, S., & Bekti, C.2016. WhatsApp Forensic Analysis and Line Messenger on Android Smartphones as a Reference in Providing Strong and Valid Evidence in Indonesia. ITS Engineering Journal, 5(2), A728-A736.

[9] Kukuh, M., Riadi, I., Prayudi, Y. 2018. Forensic Acquisition and Analysis Method of IMO Messenger. International Journal of Computer Applications (0975-8887) Volume 179-No.47, June 2018.

[10] Novaria, Y., & Anggie, K. 2017. Implementation of Forensic Procedures for WhatsApp Applications on Android Phones. Annual Research Seminar, 2(1), 65-73.

[11] Marten, A. 2010. Digital Forensic Analysis Harddisk. Jakarta: Pelita Raya.

[12] Azhar, M. 2012. Digital Forensics Practical Guide to Computer Investigation. Jakarta: Salemba Infotek.

[13] Asrizal. 2012. Digital Forensic [Online]. Available:https://edokumen.kemenag.go.id/files/VQ2Hv7uT1339506324.pdf.

[14] Hidayat, Y. 2016. Digital Forensic Ontoloc on Small Scale Devices. Jurnal Forensik Digital, 1(1), 1-7.

[15] Ayers, R., Jansen, W., & Brothers. 2014. Guidelines on Mobile Device Forensics (NIST Special Publication 800-101 Revision 1). NIST Special Publication, 1(1), 85.

[16] Akbar, Z., etc. 2016. WhatsApp Forensic on Android Smartphone A Survey. Sinergi, 20(3), 207-212.

[17] Bachrudin, K. 2017. Digital Forensic Stages, Tools, and Analysis [Online]. Available: https://www.google.com/url?sa=t&source=web&rct=j&url=http://koko.staff.gunadarma.ac.id/Downloads/files/63127/20171124-ForensikDigital.pdf.

[18] Kukuh, M. 2018. Forensic Analysis of SQLite Database on Android-Based IMO Applications. Yogyakarta: Department of Informatics Islamic Indonesia University.