

Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method

Devi Anzali Putri
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta Indonesia

ABSTRACT

Information technology is growing rapidly every year, one of which is social media. The most popular and used social media in the category of communication (Chat) is WhatsApp. WhatsApp provides many features and conveniences, the more convenience WhatsApp gets, the more crimes that occur, one of which is threatening crimes. This research was conducted by creating conversation scenarios containing threats carried out through the WhatsApp application mobile. The research aims to restore evidence of conversations containing threats that have been deleted by applying the forensic stages of the National Institute of Standards and Technology (NIST) by carrying out four stages, namely collection, examination, analysis and reporting. This study uses two smartphones that have installed the WhatsApp application with rooted and not rooted conditions to compare the findings of the evidence that has been obtained. The process of searching for digital evidence uses three tools forensic, namely MOBILedit Forensic Express, SysTools SQLite Viewer and WhatsApp Viewer. The findings of digital evidence in this study are by the desired scenario and objectives. On a Smartphone rooted, they managed to get 100% conversation data, 67% of the time messages were sent or received, 33% of user information and contact findings Smartphone 67% of. Whereas on a smartphone that is not rooted, it does not manage to get any digital evidence.

Keywords

Forensics, WhatsApp, Smartphones, Threats, NIST.

1. INTRODUCTION

The rapid development of social media has both positive and negative impacts. The positive impact of using social media has a better impact on social change in society, but the negative impact tends to bring about social change in society so that it eliminates the values or norms of Indonesian society. Examples of the negative impacts of social media include the increasing number of crimes committed through social media such as fraud, cyberbullying, pornography, provocative content, and so on [1]. WhatsApp is one of the social media that is widely used today to socialize as well as to convey messages, both by individuals and groups. However, the question is to what extent WhatsApp is used as a communication medium [2]. WhatsApp messenger has the feature of being able to chat online in the form of exchanging text, sharing mp3 files, mp4 files, exchanging photos, videos, voice notes, location maps and various kinds of document files. With this feature, it makes it easier for users to communicate with each other user to user with WhatsApp messenger. So that there are opportunities for people who

intend to commit crimes by utilizing WhatsApp messenger in the form of information that can be in the form of text or files [3]. Information that is disseminated or received through the WhatsApp application leaves a trail in the form of digital evidence on the cellphone [4]. Involving and investigating cases Cyber Crime that occur, the method can be used NIST (National Institute of Standards and Technology) [5].

1.1 Study Literature

1.1.1 Previous Study

(Yudhana et al., 2018) has conducted a study entitled "Analysis of Digital Evidence for Facebook Messenger Using NIST Stages". This study discusses the removal of digital crime evidence as much as possible from facebook messenger on Android smartphones using the Oxygen forensic tool. The conclusion of the study is that digital forensics can be carried out on smartphones used by criminals, the results obtained are in the form of conversational texts, images and audio [6].

(Syahib et al., 2018) have conducted a study entitled "Digital Forensic Analysis of Beetalk Applications for Handling Cybercrime Using NIST Stages" discussing digital forensic analysis on the Beetalk application for handling Cybercrime Forensic evidence found in this study were account names, location data, telephone number, date of birth, photo profiles, cover photo, posting text, posting an image, private messages in text and private messages in the form of pictures [7].

(Fitriana et al., 2020) study conducted entitled "Implementation method National Institute of Standards and Technology (NIST) in Digital Forensic Analysis for Handling Cybercrime". The results of this study are conversations that have been deleted have been successfully retrieved, in addition to the conversation session, WhatsApp contact number, date / month / year of the conversation and a description of the time of the conversation and all contacts can be found stored on the smartphone regardless of whether the contact is connected to WhatsApp or not [5].

(Mualfah & Ramadhan, 2020) entitled "Digital Forensic Analysis of CCTV Camera Recordings Using the NIST (National Institute of Standards Technology) Method" Judging from the results of CCTV metadata testing and analysis, digital evidence of information related to metadata obtained from CCTV camera recordings has been successfully maintained and ensuring the integrity of the digital evidence, as well as the procedures for recording evidence in chronological order that can be used as valid digital evidence in court [8].

(Hariyadi & Pasa, 2018) has conducted a study entitled "Identification of Conversation Evidence for Dual Apps

WhatsApp Applications on Xiaomi Phones Using NIST Mobile Forensics". The conclusion of this research is that the extraction results using Andriller and Laron cannot find digital evidence of WhatsApp conversations as a whole, both the original version and Dual Apps, so extraction must be carried out using a manual method through ADB to obtain more valid evidence or data [9].

1.1.2 Digital Forensics

Digital forensics can be interpreted as an activity to investigate and determine facts related to crimes and legal issues [10]. Digital forensics is very important for the prosecution of digital criminals involving digital devices [11]. Digital forensics can also be interpreted as the collection and analysis of data from various computer resources that include computer systems, computer networks, communication lines, and various storage media that are suitable for submission in court proceedings [12].

1.1.3 Mobile Forensics

Mobile forensics is the science that uses the methods by the conditions forensics to make the process of recovery of digital evidence from mobile devices [13]. The use of mobile devices such as smartphones with various types and operating systems for criminal activity is increasing, but their methods of Mobile Forensic then can help solve criminal cases related to mobile devices, especially Smartphones [14]. Mobile forensics itself is not only aimed at meeting the needs of digital evidence in court (litigation process) but can also be used for non-litigation processes [15].

1.1.4 Smartphone

Smartphone is a device that allows communication, which also has a PDA (Personal Digital Assistant) function and can function similar to a computer [16]. Smartphones can be used to become personal assistants because Smartphones can now store important business data as well as being a reminder of what activities the user must do [17]. Smartphone image can be seen in Figure 1



Figure 1. Smartphone pictures

Figure 6 is a display of smartphone development from year to year which is increasingly sophisticated and modern.

1.1.5 Cybercrime

Cybercrime is a crime committed by making a computer or computer network a tool, target, and place of crime [5]. Another definition states that cybercrime can be declared as an illegal act carried out by using a computer network as a tool or using a computer as an object [18].

1.1.6 Threats Electronic Media

The criminal act of threatening through short message services must meet the requirements specified in Article 27 paragraph (4) of the ITE Law, namely intentionally, without permission, distributing, transmitting, providing, and/or making access to electronic information and/or Electronic documents containing extortion and/or threats and the main elements of Article 29 of the ITE Law are intentionally and without rights sending electronic information and/or electronic documents containing threats of violence or intimidation aimed at individuals [19].

1.1.7 Digital Evidence

Evidence is the evidence value of information stored or transmitted in digital form. Meanwhile, according to Eoghan Casey, digital evidence is data stored or transmitted using a computer that supports or refutes the theory of illegal processes, or contains illegal elements such as intentions or alibis [9]. Digital evidence is divided into 15 types, namely logical files, deleted files, encrypted audio files, video files, image files, email, user id/password, etc [20].

1.1.8 WhatsApp

WhatsApp messenger is a cross-messaging application platform that allows users to exchange information via conversational messages without SMS fees because to use WhatsApp, users must use an internet data package [3]. The use of WhatsApp smartphones as a medium of information plays a very important role in providing and disseminating information to others [21].

1.1.9 National Institute of Standard Technology

National Institute of Standard and Technology (NIST) is widely applied to forensic analysis mobile [22]. NIST is a method that has four stages, namely Collection, Examination, Analysis, and Reporting [23]. NIST is the body responsible for developing standards, guidelines, and minimum requirements to provide adequate information security for all assets and parties who have competence in the field of digital forensics [24]. The stages of NIST can be seen in Figure 2

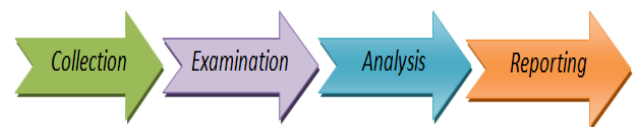


Figure 2. Display of NIST Stages

Figure 2 represents 4 stages of NIST that can be used for forensic processes, the descriptions are as follows:

1. Collection
This stage is the process of identifying, marking, recording, and retrieving data from data sources related to procedures maintenance of data integrity.
2. Examination
Examination is a process to maintain or protect digital evidence from damage and alterations made by other parties who are not responsible.
3. Analysis
The analysis phase is carried out to analyze the data that has been extracted with the correct methods and techniques based on applicable regulations.
4. Reporting
The final stage aims to report or present the results of the analysis.

2. METHODOLOGY

2.1 Research Scenario

This scenario is designed to illustrate how to carry out various stages of the forensics process mobile. The research was carried out by simulating criminal cases of on the WhatsApp service to obtain digital evidence. Examination of evidence Smartphone using the tools forensic MOBILedit Forensic Express, SysTools SQLite Viewer and WhatsApp Viewer.

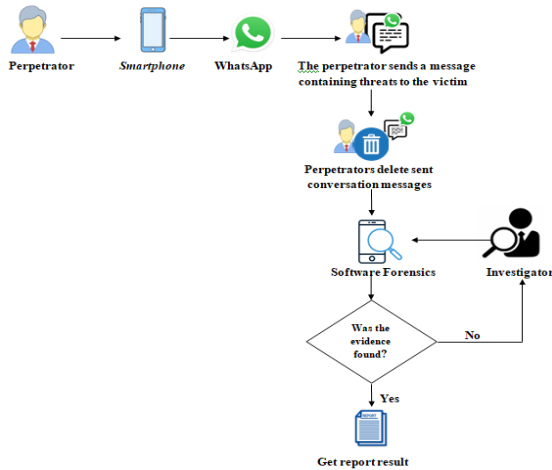


Figure 3. Research case scenario

In Figure 3, the case scenario is how the perpetrator sends a message to the victim containing threats via WhatsApp on the perpetrator's smartphone to scare the victim. Then the perpetrator deletes the conversation sent to the victim after the victim threatens to report it to the authorities. Then the victim reports the perpetrator's actions to the authorities, then the police will investigate to obtain evidence to be submitted to the investigator. The smartphone belonging to the perpetrator who had been confiscated and the conversation on WhatsApp that had been deleted by the perpetrator became evidence for imaging files using tools forensic by investigators. After the forensic process is complete, the results of the report will be issued.

2.2 Research Stages

At this implementation stage, investigators carry out a series of activities to obtain information according to the procedure [25]. The reference stages used in this research are the stages of the National Institute of Standards and Technology (NIST), which consist of four stages carried out in the settlement and investigation of cases, namely collection, examination, analysis and reporting.

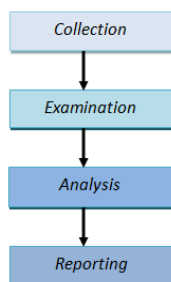


Figure 4. Research Stages

This research refers to the NIST stage consisting of 4 stages carried out to carry out the investigation process [26].

2.2.1 Collection

Collection of digital evidence using the help of several tools and software forensics to obtain the desired data on the Smartphone belonging to the perpetrator and the victim. Several pieces of evidence were successfully confiscated by the police during the investigation process, which can be seen in Table 1

Table 1. Evidence seized by the police


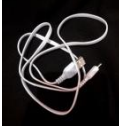


No	Name of evidence	Picture	Description
1.	Smartphone 1		The Samsung Galaxy Grand Prime is on, connected to the network and rooted
2.	Data Cable 1		Data Cable to connect Smartphone 1 with laptop
3.	Smartphone 2		Samsung Galaxy A7 2018, with conditions not rooted
4.	Data Cable 2		Data Cable to connect Smartphone 2 with laptop

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

2.2.1.1 Collection Smartphone Rooted

Collection begins by connecting the Smartphone to a laptop using a data cable. On a Smartphone, it rooted managed to obtain a data imaging file using the tool MOBILedit Forensic Express, as shown in Figure 5

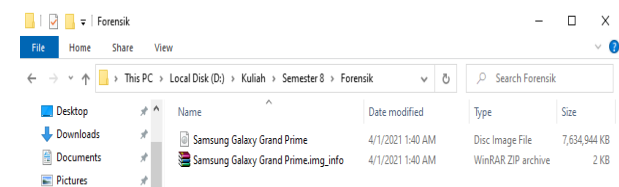


Figure 5. The results of imaging files.

Figure 5 is a display of the results of imaging files from the Smartphone in the root and stored in the selected directory.

2.2.1.2 Collection Smartphone Not Rooted

The process of collection is collecting a smartphone, not with a non-condition is rooted different from a smartphone with a condition rooted... Because on the display of the tools MOBILedit Forensic Express menu Physical Create Image is not available, then the processing imaging files can not be

done without rooting on the Smartphone.

2.2.2 Examination

This stage is the process of proving data integrity. Examination is a stage of the process to protect evidence carried out by investigators from damage and interference in the process of collecting evidence in the form of electronic evidence and electronic data analysis by irresponsible parties, one of which is by hashing electronic data that has been successful. The backup on the process. collection way it works is to match the results of the initial hash with the results of the final hash, to find out whether the file is original or not.

2.2.2.1 Examination Smartphone Rooted

Process Hashing This research was conducted on the results of files imaging on Smartphones in the root that were successfully obtained during the process collection using the Hash Tool application.

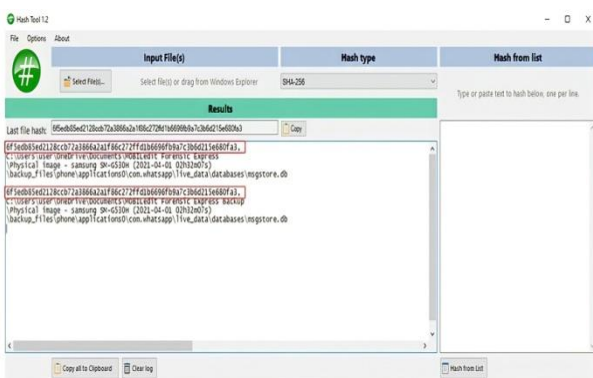


Figure 6. The result of hashing the file backup data

Figure 6 shows the hashed result of the data backup MOBILEdit Forensic Express. The red color indicates the encryption code for the file. Judging from the wording of the file encryption code that is displayed remains unchanged, it shows that there is no change in the data.

2.2.2.2 Examination Smartphone Not Rooted

On Smartphone does not at the root does not generate files backup data in the previous process, so the process cannot be done Hashing using the software Hash Tool.

2.2.3 Analysis

The analysis stage is the stage carried out by investigators to find traces and process data from identification, collection, and examination of data in the process physical image at the stage collection on a Smartphone with conditions root using the MOBILEdit Forensic Express, SysTools SQLite Viewer and WhatsApp Viewer tools. Because at the stage of searching for evidence on a Smartphone with a condition that is not rooted, it cannot find any evidence in the form of conversation history, conversation time, telephone contact, or others so that it cannot be analyzed

2.2.3.1 Analysis of evidence on a rooted smartphone.

At the stage of searching for evidence on a rooted smartphone, you can find evidence in the form of conversation history, time information and others so that analysis can be carried out.

2.2.3.1.1 MOBILEdit Forensik Express

The analysis process will begin by opening the tool

MOBILEdit Forensic Express, then the investigator selects Application analysis to extract application data on the Smartphone, the application to be extracted is the WhatsApp application, by executing a checklist of data stored in the folder **com.whatsapp**, as shown in Figure 7

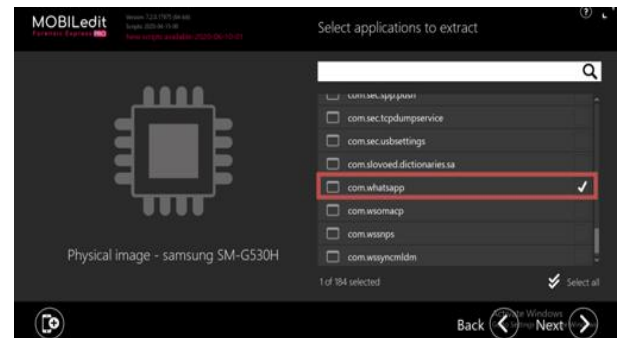


Figure 7. Application options to be extracted

In Figure 7 after selecting what application to extract the data, the extraction process will appear, as shown in Figure 8

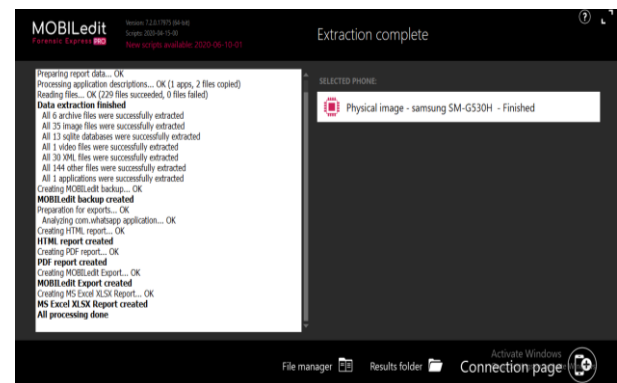


Figure 8. MOBILEdit Forensic Express extraction process

Figure 8 shows the extraction process, after the data extraction process is completely completed, the extracted file will be in the form of a report that is saved automatically in the directory selected by the investigator.

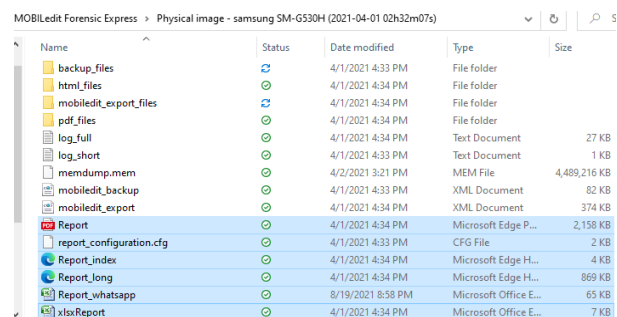


Figure 9. The extracted data file.

Figure 9 is a report on the results of WhatsApp data extraction using Forensic MOBILEdit in the form of .pdf, .excel, .txt and .html. Open the pdf file to find out what the results of the report were.

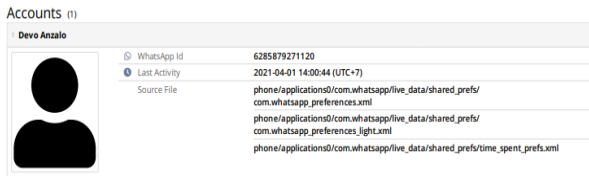


Figure 10. Display of the perpetrator's account

Figure 10 shows the account information suspected of carrying out the threat which contains the username Devo Anzalo with WhatsApp id numbered 6285879271120, Last Activity on April 1, 2021 at 14:00 and Source files. And there are also other evidence findings regarding information regarding user numbers, usernames, source files, conversation times, and others.

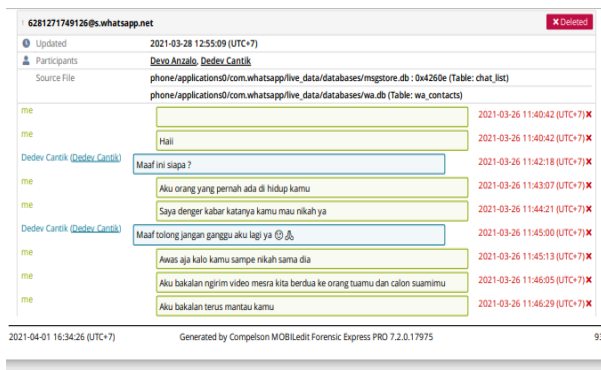


Figure 11. Display of conversation messages obtained

Figure 11 is a display of conversation messages obtained. The next evidence finding is in the form of contacts found on Smartphones

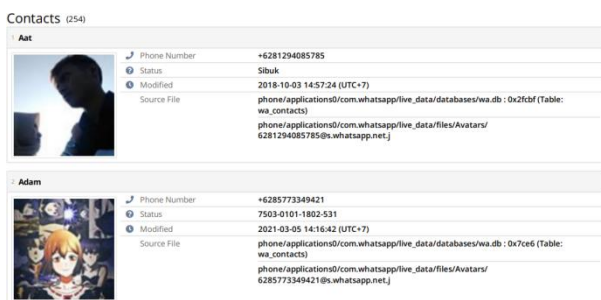


Figure 12. Findings of contacts on Smartphones

In Figure 12 it can be seen that there are 254 contacts on Smartphones, there are also photos of users, user numbers, status and Source File stored contacts.

2.2.3.1.2 WhatsApp Viewer

Stages of the analysis process begin by opening the tool WhatsApp Viewer. After getting all the data related to the WhatsApp application in the previous process, the next step is to unlock the database encryption by describing the encrypted crypt12 database on WhatsApp by adding a key, like a Figure 13

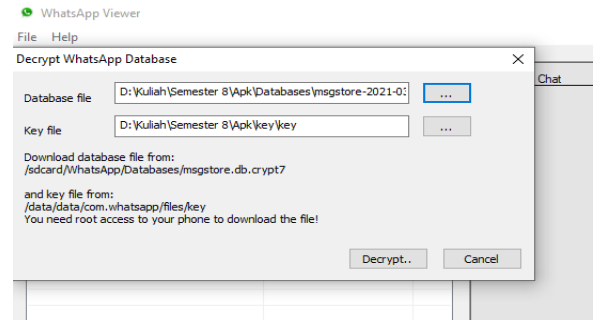


Figure 13. The process of exporting an encrypted

In figure 13, after decrypting the encrypted backup database file, the next step is to open the encrypted database using the WhatsApp Viewer tool to find out which conversations have been deleted.

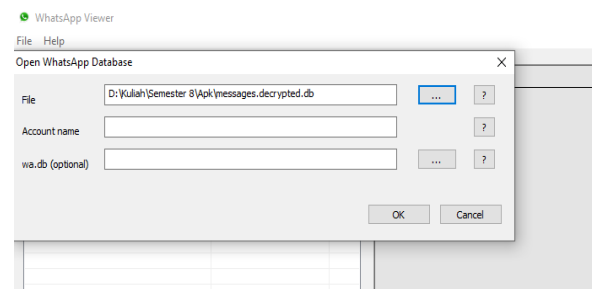


Figure 14. The display of opening the WhatsApp database that has been described

In figure 14, after successfully opening the WhatsApp database that has been described, the scripted conversation, WhatsApp contact number, description of the date/month/year and time of the conversation have been retrieved. And reports can be saved in the form of .txt .html or .json.

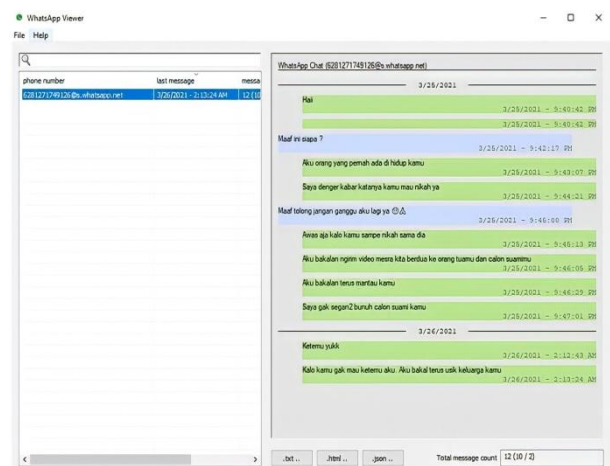


Figure 15. Display of conversations that have been successfully

Figure 15 is a display of messages that have been successfully obtained, there is also a description of the time of the conversation.

2.2.3.1.3 SysTools SQLite Viewer

The analysis process begins by opening the tool SysTools SQLite Viewer, then opening the database file "messages.decrypted.db", the next step is to select the table "message" to display the conversations between the

perpetrator and the victim, the successful conversation is shown in Figure 16

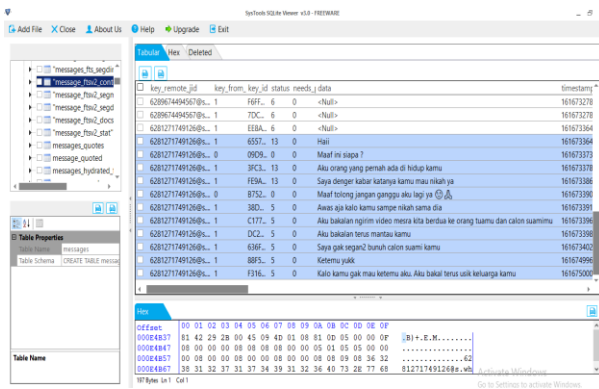


Figure 16. Finding evidence of the conversation

Figure 16 is a display of conversation evidence findings. Other digital evidence found in the form of contacts contained on Smartphones, such as Figure 17

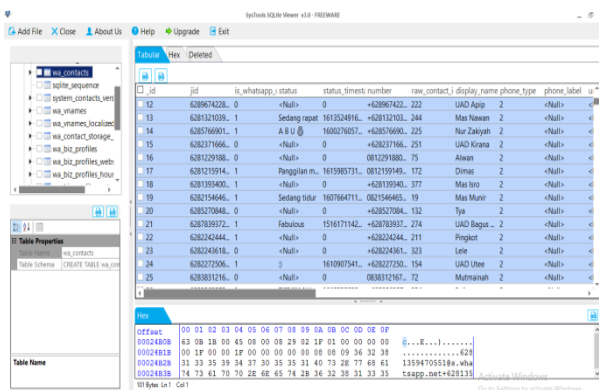


Figure 17. Finding evidence of contacts on Smartphone

Figure 17 shows the findings of data contacts that were successfully obtained from the forensic process that was carried out using SysTools SQLite Viewer.

The results of the analysis on a rooted smartphone managed to get evidence of conversations related to threats that have been deleted and also supported by other evidence findings such as user account information, smartphone contacts, and information when sent/received.

2.2.3.2 Analysis of evidence on a Smartphone that is not rooted

At the stage of searching for evidence on a Smartphone with a condition that is not rooted, it cannot find any evidence in the form of conversation history, conversation time, telephone contact, or others so that it cannot be analyzed.

2.2.4 Reporting

Reporting or reports is the final stage and aims to display the analysis of data that has been found in the process of collection, examination and analysis. The results of the evidence report consist of several tools used, namely MOBILedit Forensic Express, SysTools SQLite Viewer and WhatsApp Viewer. The three tools used produce different digital evidence findings. Digital evidence that has been found will be matched with evidence from the victim. table of digital evidence findings with evidence from victims can be seen in Table 2

Table 2. Table of evidence from victims and findings of evidence

Evidence From The Victim	Digital Evidence Finding
	1. Tool MOBILedit Forensik Express
	2. Tool SysTool SQLite Viewer
	3. Tool WhatsApp Viewer

From the table of digital evidence findings, the conversations that have been successfully obtained from the forensic process carried out by the investigators have a match with the evidence of conversations from the victim, which later the findings of the digital evidence will be used as support in court by adding other digital evidence findings such as information findings. User, contacts Smartphone and conversation time.

3.1.1 Results

After testing with various forensic tools on smartphones that are rooted and not rooted, the tools used produce different evidence findings. so that a comparison table is made, the comparison of the results of the evidence is shown in Table 3

Table 3. Comparison of the findings of digital evidence

Smartphone condition	Tool	Results Of Digital Evidence			
		Message conversation	Time of message sent/received	User information	Smartphone Contact
Rooted	MOBILedit Forensik	✓	✓	✓	✓
	SysTools SQLite	✓	-	-	✓
	WhatsApp Viewer	✓	✓	-	-
	WhatsApp Viewer	✓	✓	-	-
Not Rooted	MOBILedit Forensik	-	-	-	-
	SysTools SQLite	-	-	-	-
	WhatsApp Viewer	-	-	-	-
	WhatsApp Viewer	-	-	-	-

Can be seen in Table 3, based on the results of research conducted on a rooted smartphone using the MOBILedit Forensic Express tool, managed to get evidence of deleted conversations, information on when sent/received, user information, and smartphone contacts. on SysTools SQLite Viewer tool managed to get deleted conversations and smartphone contacts. And the last tool, WhatsApp Viewer managed to get the deleted conversation and the time it was sent/received. While the results of research conducted on smartphones were not rooted, failed to obtain any evidence from the three tools used.

4. CONCLUSION

Based on the results of the study, the findings of digital evidence were carried out using 3 forensic tools, namely MOBILedit Forensic Express, WhatsApp Viewer, and SysTools SQLite Viewer, and different digital evidence results were obtained. Finding digital evidence on a rooted Smartphone managed to get 100% of conversation data, 67% of the time messages were sent or received, 33% of user information, and 67% of contact findings on Smartphone numbers. While on a smartphone that is not rooted, it does not manage to get any digital evidence. This research is expected to be used as a reference by further researchers in carrying out the forensic process. This research can still be developed, suggestions for further researchers can use operating systems, forensic tools, and different forensic stages.

5. REFERENCES

- [1] A. S. Cahyono, "Pengaruh media sosial terhadap perubahan sosial masyarakat di Indonesia," *J. ilmu Sos. ilmu Polit. diterbitkan oleh Fak. Ilmu Sos. Polit. Univ. Tulungagung*, vol. 9, no. 1, pp. 140–157, 2016, [Online]. Available: <http://www.jurnal-unita.org/index.php/publiciana/article/download/79/73>.
- [2] - Trisnani, "Pemanfaatan Whatsapp Sebagai Media Komunikasi Dan Kepuasan Dalam Penyampaian Pesan Dikalangan Tokoh Masyarakat," *J. Komunika J. Komunikasi, Media dan Inform.*, vol. 6, no. 3, 2017, doi: 10.31504/komunika.v6i3.1227.
- [3] N. Anggraini *et al.*, "Analisa Forensik Whatsapp Messenger Pada Smartphone Android," vol. XII, no. 1, pp. 83–100, 2020.
- [4] D. Hariyadi and I. Y. Pasa, "Dual Apps Whatsapp Pada Ponsel Xiaomi," *J. INTEK*, vol. 1, pp. 1–7, 2018.
- [5] M. Fitriana, K. A. AR, and J. M. Marsya, "Penerapana Metode National Institute of Standars and Technology (Nist) Dalam Analisis Forensik Digital Untuk Penanganan Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, pp. 29–39, 2020, doi: 10.22373/cj.v4i1.7241.

- [6] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.
- [7] M. I. Syahib, I. Riadi, and R. Umar, "Analisis Forensik Digital Aplikasi Beetalk untuk Penanganan Cybercrime Menggunakan Metode NIST," *Semin. Nas. Inform.*, vol. 2018, no. November, p. 134, 2018, [Online]. Available: <http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2629>.
- [8] D. Muallfah and R. A. Ramadhan, "Analisis Digital Forensik Rekaman Kamera CCTV Menggunakan Metode NIST (National Institute of Standards Technology)," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.
- [9] D. Hariyadi, "Komparasi Penanganan Barang Bukti Elektronik dan/atau Barang Bukti Digital sesuai SOP Pusat Laboratorium Forensik Polisi Republik Indonesia," pp. 1–5, 2019, doi: 10.31219/osf.io/37at6.
- [10] B. Raharjo, "Sekilas Mengenai Forensik Digital," *J. Sositelknologi*, vol. 12, no. 29, pp. 384–387, 2013, doi: 10.5614/sostek.itbj.2013.12.29.3.
- [11] M. Nur Faiz, W. Adi Prabowo, and M. Fajar Sidiq, "Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 1, pp. 63–70, 2018, doi: 10.20895/INISTA.VIII.
- [12] R. Meiyanti and I. Ismaniah, "Perkembangan Digital Forensik Saat Ini dan Mendatang," *J. Karya Ilm.*, vol. 15, no. 2, 2015.
- [13] I. Riadi and R. Umar, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017.
- [14] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," *Akuisisi Bukti Digit. Pada Instagram Messenger Berbas. Android Menggunakan Metod. Natl. Inst. Justice*, vol. 4, pp. 219–227, 2018.
- [15] A. N. Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *Int. J. Comput. Appl.*, vol. 174, no. 18, pp. 34–40, 2021, doi: 10.5120/ijca2021921076.
- [16] G. F. Mandias, "Analisis Pengaruh Pemanfaatan Smartphone Terhadap Prestasi Akademik Mahasiswa Fakultas Ilmu Komputer Universitas Klabat," *Cogito Smart J.*, vol. 3, no. 1, p. 83, 2017, doi: 10.31154/cogito.v3i1.47.83-90.
- [17] M. G. Sobry, "Peran Smartphone Terhadap Pertumbuhan Dan Perkembangan Anak," *M.gustian sobry*, vol. 2, no. 2, pp. 24–29, 2017, [Online]. Available: <http://jurnal.iicet.org/index.php/jpgi/article/view/222>.
- [18] Dista Amalia Arifah, "KASUS CYBERCRIME DI INDONESIA Indonesia's Cybercrime Case," *J. Bisnis dan Ekon.*, vol. 18, no. 2, pp. 185–195, 2011.
- [19] M. Safri, A. Sofyan, W. Sitorus, M. Ilmu, and H. Universitas, "No Title," vol. 5, no. 1, pp. 84–89, 2016.

- [20] T. Pandela and I. Riadi, "Browser Forensics on Web-based Tiktok Applications," *Int. J. Comput. Appl.*, vol. 175, no. 34, pp. 47–52, 2020, doi: 10.5120/ijca2020920897.
- [21] Sartika, "Kegunaan whatsapp sebagai media informasi dan media pembelajaran pada mahasiswa ilmu komunikasi STISIP persada bunda," *Medium*, vol. 6, no. 2, pp. 15–26, 2018.
- [22] R. Umar and Sahiruddin, "Metode Nist Untuk Analisis Forensik Bukti Digital Pada Perangkat Android," *Pros. SENDU_U_2019*, pp. 978–979, 2019.
- [23] M. I. Syahib, I. Riadi, and R. Umar, "Akuisisi Bukti Digital Aplikasi Viber Menggunakan Metode National Institute of Standards Technology (NIST)," *J-SAKTI (Jurnal Sains Komput. dan Inform.)*, vol. 4, no. 1, p. 170, 2020, doi: 10.30645/j-sakti.v4i1.196.
- [24] N. Nasirudin, S. Sunardi, and I. Riadi, "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.
- [25] R. Saputra and I. Riadi, "Forensic Browser of Twitter based on Web Services," *Int. J. Comput. Appl.*, vol. 175, no. 29, pp. 34–39, 2020, doi: 10.5120/ijca2020920832.
- [26] A. Nofiyana and M. Mushlihudin, "Analisis Forensik pada Web Phishing Menggunakan Metode National Institute Of Standards And Technology (NIST)," *JSTIE (Jurnal Sarj. Tek. Inform.)*, vol. 8, no. 2, p. 53, 2020, doi: 10.12928/jstie.v8i2.16697.