

Mobile Forensic for Cyber Fraud Case on WhatsApp Services using National Institute of Standard Technology Method

Syofia Nur Aniza
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The development of information technology is very rapid, one of which is social media such as WhatsApp. WhatsApp is a communication medium that has many features and conveniences it. The ease with which WhatsApp is used has led to an increase in crimes such as buying and selling fraud online. This research was conducted with a conversation scenario about buying and selling fraud through-based WhatsApp mobile services. This research aims to restore evidence of conversations that have been deleted by applying the NIST forensic stages (National Institute of Standards and Technology), namely collection, examination, analysis, and reporting. Based on the test results from conversations (evidence) that have been deleted, it can be obtained using two tools, forensic namely MOBILedit Forensic Express and AccessData FTK Imager. Evidence obtained from a smartphone in the rooted form of user information, profile photo, phone number, picture, voice recording, date and time the message was sent/received. The evidence of conversation findings that have been found is 100%, user information is 50%, contacts smartphone are 100%, and the time when messages are sent/received is 50%. Smartphones are already at the root of secured evidence in accordance with the stages of digital forensics.

Keywords

Forensics, WhatsApp, Smartphone, Fraud, NIST

1. INTRODUCTION

The development of technology modern in Indonesia is growing rapidly in human life. Technology offers easy access to information and is now in great demand by the wider community. The rapid advancement of technology had a positive impact on the development of communication media such as WhatsApp, Facebook, and Instagram as a means of communication. Information and communication are very influential on society so that increasingly advanced technology creates large opportunities for crime and the vulnerability of existing information security, such as the number of crimes related to internet applications [1]. The internet is a communication system that is an important need for people in everyday life. The internet is not only used for entertainment but is also used as a marketing medium in the business world, especially for mothers who are business people [2]. This concept is related to the social structure between social media actors, most people are connected through social media to communicate with business colleagues or exchange information [3]. Quoted from cyberthreat.id that the number of internet users increased by 25 million from last year. Connected smartphones increased

to 15 million, and social media users increased by 12 million [4]. Dissemination of information through social media is very fast because social media has text messaging services, photos, and video postings. The ease of using social media such as the WhatsApp application makes fraud more and more online. WhatsApp is a social media application that can exchange messages without credit and has features that can make it easier for users to send text messages, photos, videos, audio, documents, and so on. To use the application, it is enough to register using a telephone number. The development of the WhatsApp application in Indonesia is growing rapidly, so many people use it as a medium for sales promotion or business online. Business Online can change the mindset of the customers in the shop because of the ease in the process of purchase of the product [5]. WhatsApp has the potential as a means of crime such as buying and selling fraud online. Article 28 paragraph (1) of the ITE Law stipulates that a person who intentionally spreads false news and causes consumer losses in Electronic Transactions will be sentenced to a maximum imprisonment of six years and/or a maximum fine of one billion rupiahs [6]. Fraud is one of the negative impacts of crime that is currently approaching many people. Fraud that occurs on the internet or other social media also has the potential to harm others. In social media, fraudulent crimes often occur in the name of buying and selling businesses and offering products that are sold at low prices. Scams usually use a way to sell goods that are attractive to buyers because the price is lower than the original price, which is why the buyer is finally attracted and sends money to sign up for the goods. The number of problems in buying and selling transactions online such as products or goods that do not match the picture until the promised goods are not received by the buyer [7]. This fraudulent act only deceives certain people or the public in attracting profits for their own company [8].

1.1 Study Literature

1.1.1 Previous Study

This study uses references from 5 previous studies that are relevant to the problem to be studied regarding data search cases of buying and selling fraud on WhatsApp-based mobile services. The first research is entitled "Facebook Lite Social Media Analysis with Forensic Tool NIST Method". This research raises the evidence of digital crime in the Facebook Lite application. In this study, the tools that will be used are Mobile edit Forensic Pro forensic tools with the help of the National Institute of Standards Technology (NIST) method. NIST has a good workflow. The results of the study will be obtained in the form of the account used, Audio, Conversation, and Image [9].

The second study is entitled "Analysis of Forensic Investigations Cyberbullying on Whatsapp Messenger Using the National Institute Of Standards and Technology (NIST) Method". The results of the research are digital forensic evidence found in the WhatsApp application in the form of text and help identify actions that lead to cyberbullying, and to identify cyberbullying using the method Cosine Similarity [10].

The third study used the NIST SP 800-86 method and the Support Vector Machine in a study entitled "Digital Forensic Investigation and Analysis on WhatsApp Group Conversations Using NIST SP 800-86 and Support Vector Machine". The results of this study use the algorithm Support Vector Machine (SVM) to classify the quality of conversation in a group. This study succeeded in classifying digital evidence in the form of a group conversation with a percentage of approximately 96.21% negative content. This percentage value can be used as an initial indicator in detecting the quality of negative conversations [11].

The fourth study entitled "Identification of Skype Digital Evidence on Android Smartphones with the National Institute Of Justice (NIJ) Method" obtained digital evidence of online fraud cases on Skype using the National Institute of Justice (NIJ) method. The results of the study are used as supporting evidence by investigators in handling criminal cases [12].

The fifth study entitled "Analysis and Comparison of Forensic Evidence for Facebook and Twitter Social Media Applications on Smartphones Android" suggest that the simulation method is used in the study by running 11 scenarios. The results of this study indicate that all forensic evidence on the Facebook social media application was found. Meanwhile, the Twitter social media application was only found in the form of account names, location data, profile photos, cover photos, posts in the form of text, and posts in the form of images [13].

1.1.2 Digital Forensics

Digital forensics is a forensic science that is used to investigate data related to crimes. Forensics can be found on digital devices such as computers, smartphones, tablets, PDAs, net-working devices, storage, and the like [14]. Digital forensics aims to help analyze and secure digital evidence that can be used as evidence in court [15]. The investigation uses data analysis techniques on a computer with the stages of identification, preparation, extraction, documentation of data on a computer to obtain digital evidence.

1.1.3 Mobile Forensics

Forensics Mobile is a science that analyzes and performs recoverable digital evidence from devices mobile with a method commonly used by digital forensic science [16]. There is digital evidence that can be extracted from a device mobile. Types of evidence from mobile can be in the form of contact numbers, text messages, call logs, audio files, photos, emails, and internet history [17]. Application mobile is a program created specifically for Smartphones that can add to the functionality of the device itself and can be downloaded on Google Play [18].

1.1.4 Digital evidence

Evidence is any information that can prove a violation or crime in digital form. Digital evidence uses computers to present the information obtained [19]. Digital evidence is very

useful for criminal investigations such as fraud, theft of personal data, child abuse, trafficking in illicit goods, and murder. Digital evidence that can be used as evidence in court includes account information, phone numbers, audio, photos, videos, and text conversations from an application [20]. Fraud perpetrators who use applications such as WhatsApp will delete digital evidence in the form of text conversations, photos (proof of transfer), and audio that can be evidence of a crime [21]. Technology-based crimes continue to increase with various modes, the refore it is necessary to analyze existing digital evidence, both stored and transmitted through other digital devices. Digital evidence can be found in the forensic stage. Computerized records can assist investigators in knowing the suspect's intention to commit a crime [22].

1.1.5 Smartphone

The Smartphone is a small computer that has the capability of a telephone [23]. Smartphones offer users to download additional applications from the centralized store it offers, synchronization, mobile payment services, and virtual assistants. The advanced smartphones of sophisticated makes it easier to carry out various activities such as reading business documents, playing music, surfing the internet, viewing videos, and so on. Smartphones are also widely used for tutoring online from children to adults [24].

1.1.6 WhatsApp

WhatsApp is a messaging application using an internet data connection (without credit) that allows users to send and receive messages from smartphones. The WhatsApp application can also make video calls, make calls, and create stories. This application is also very easy to use by registering a phone number so that it can be easily understood by users of the application. So don't be surprised if the WhatsApp application can develop very rapidly.

1.1.7 Fraud

Fraud is a crime committed intentionally to gain an advantage and harm others by lying. Fraud often occurs in the name of buying and selling businesses and offering products at low prices. Business Online is an opportunity for those who are not responsible for the crimes that can cause harm to others. Buying and selling online manyfrauds occur using transaction systems via accounts [25]. Fraud is carried out using social media, such as fake bills, fake documents, false advertising, fake identities, fake product offers, and so on. Shopping Online has a lot of risk of theft of personal data information that can be used by people inappropriately [26].

1.1.8 National Institute of Standard Technology

National Institute of Standards and Technology (NIST) is a method used to obtain digital evidence and has forensic stages collection, examination, analysis, and reporting. The explanation of the NIST stages is as follows.

1. Collection
The collection stage is to identify, label, record, and retrieve data from relevant sources in accordance with data integrity procedures.
2. Examination
The examination stage is to process data and collect it forensically with a combination of various scenarios according to needs and maintain data integrity.
3. Analysis
The analysis stage is to the analyze the results of the

examination using the forensic stage so as to obtain information that can answer questions in data collection.

4. Reporting

The reporting stage is reporting the results of the analysis and explaining the tools and procedures selected through the forensic process [27].

2. METHODOLOGY

2.1 Research Scenario

The research scenario is made to explain how the stages of the fraud investigation process will be made. This scenario uses a smartphone that the perpetrator uses to deceive the victim. This stage will explain the process of identifying evidence. An investigator collects evidence from the smartphone perpetrator's which can be seen in Figure 1.

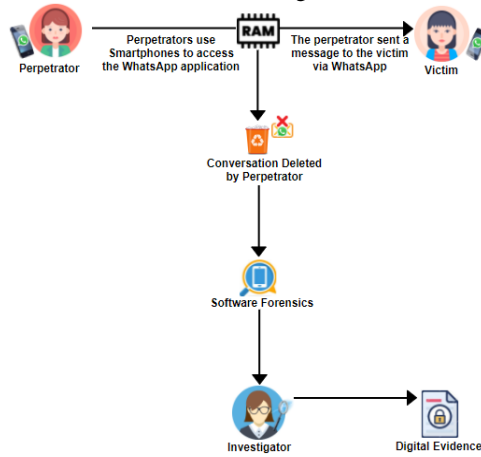


Figure 1. Research Case Scenario

Figure 1 is a research case scenario. The smartphone used by the perpetrator and the victim is turned on and the WhatsApp application has been installed, as in the picture above which depicts the perpetrator sending a message to offer a product, namely masks and body temperature measuring devices, to convince the perpetrators to send sample images at low prices. The perpetrator stated that the goods were there and ready to be sent if the victim had sent the money as a sign that they had ordered the goods.

2.2 Research Stages

The stages in this study refer to the method National Institute of Standards and Technology (NIST) namely Collection, Examination, Analysis, and reporting. The following is the process for obtaining evidence which can be seen in Figure 2.

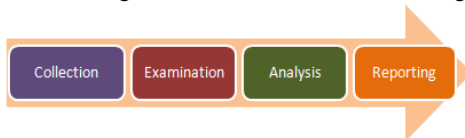


Figure 2. Implementation Stages

Figure 2 is the implementation stage where investigators carry out the forensic stages issued by NIST to find digital evidence of the crime of buying and selling fraud on the WhatsApp service. The explanation of the above implementation stages is as follows.

2.2.1 Collection

The collection stage is the initial stage carried out by investigators to search for, and collect evidence obtained. The collection of digital evidence is obtained through searching

data from the tool MOBILedit Forensic Express. The evidence can be seen in Table 1.

Table 1. Digital Evidence

No	Name of Evidence	Picture	Information
1	Perpetrator Smartphone		The Samsung Galaxy J1 ace (MPT) brand is rooted, turned on, and connected to the internet
2	Perpetrator Smartphone Data Cable		The data cable is connected to the perpetrator Smartphone

Table 1 is the evidence obtained from the fraud perpetrator which will then be processed through a forensic process to find digital evidence on the smartphone. The next stage is to install the software Odinto install SuperSU and get full access rights to the smartphone used by the perpetrator. Then the data obtained from the smartphone will be acquired and analyzed to obtain digital evidence related to fraud cases.

2.2.2 Examination

The Examination is a stage to prove data integrity, protect digital evidence, and ensure that evidence is not damaged or altered by irresponsible parties. To protect the evidence, you can hash the electronic data that has been backed up. The process is hashing used to determine the authenticity of the data so that it does not experience changes or damage by matching the initial results and the final results of hashing [28]. The process hashing uses the application Hash Tool. The first step that can be done is to copy the original folder from the data that has been backed up. After copying the original data folder from the MOBILedit software. Click **Select File** and select the database "msgstore" there in the original folder of the data results MOBILedit software. Next, open the backup copy file and select the database "msgstore" so that it will look like Figure 3.

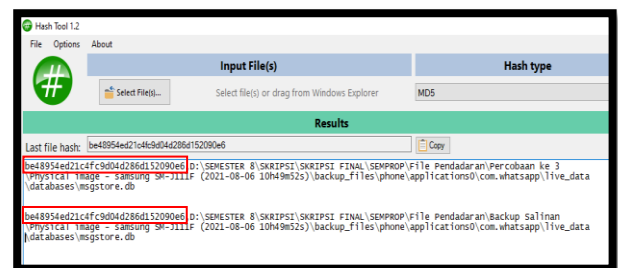


Figure 3. Results of HashingBackup Files Data Smartphone

Figure 3 shows results of the database file MOBILedit hashing. The original and file the file copy show the result of hashing by generating a hash (Code from database). The code generated from the two folders with different storage places is **be48954ed21c4fc9d04d286d152090e6** which means the data is still original or there is no change to the digital evidence.

2.2.3 Analysis

The analysis stage is looking for and finding digital evidence to examine the data from the physical image process collection on the smartphone perpetrator's a condition root. This stage analyzes and examines the data according to the forensic tools used [29]. Analysis of digital evidence search results using tools forensic, such as MOBILedit Forensic Express, and AccessData FTK Imager.

2.2.3.1 MOBILedit Forensic Express

This stage is used by investigators to find and process data on smartphones by connecting the smartphone perpetrators to a laptop and selecting one of the options USB connection, Wi-Fi connection, or Bluetooth connection. The list of applications on the smartphone perpetrators can be seen in Figure 4.

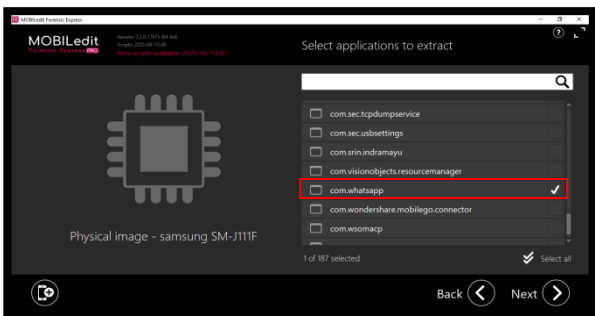


Figure 4. List of Applications you want to Extract

Figure 4 is a list of applications installed on a smartphone. Next, the investigator will choose the application to be extracted, the WhatsApp application by selecting the data in com.whatsapp. The results of data extraction will be saved automatically in the form of a report (reporting). The extraction process is not successful or an error will be marked in red and the extraction process is successful if there are no errors. The data extraction process should not experience errors as shown in Figure 5.

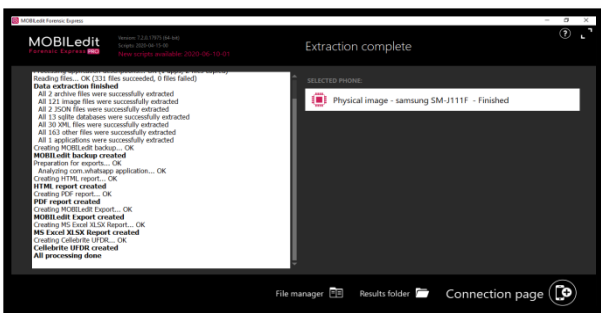


Figure 5. Display of the Data Extraction Process

Figure 5 is a display of the data extraction process on the WhatsApp application that is already installed on the smartphone perpetrators. The results of data extraction will be stored automatically in the form of a report (reporting).

2.2.3.2 AccessData FTK Imager

AccessData FTK Imager is used in the analysis process database stored in the folder backup data to obtain digital evidence from the smartphone perpetrator. To see image files the captured can be seen in Figure 6.

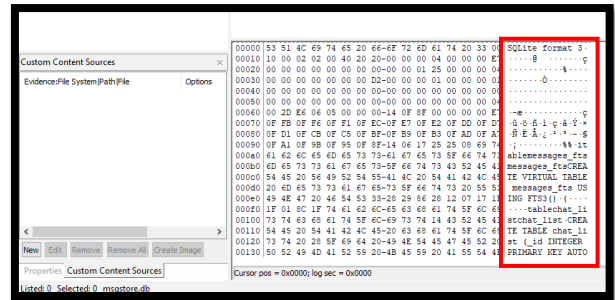


Figure 6. Display of Captured data

Figure 6 is an image file display that shows the data in the image file that has been successfully added. search data or digital evidence can be searched by using keywords. The data search display can be seen in Figure 7.

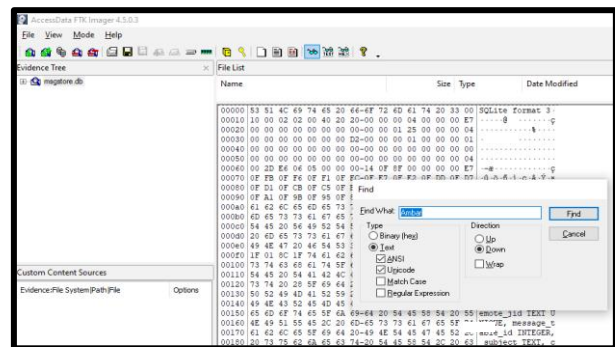


Figure 7. Searching Data by Keyword

Figure 7 is a search view based on keywords that can be done by pressing the CTRL+F key, then entering the keywords (parameters) you want to search as evidence in the form of conversations. a perpetrator with the victim. Proof of conversation can be seen in Figure 8.

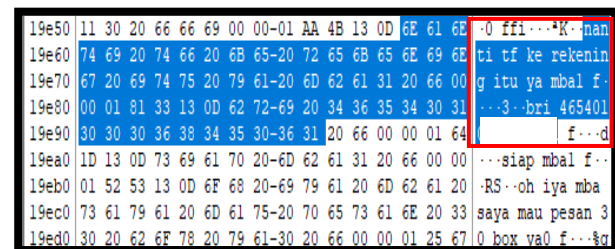


Figure 8. Conversation Evidence from the Perpetrator

Figure 8 is a conversation from a perpetrator who offers a product at a low price so that the victim feels interested and wants to order the product through the perpetrator. The perpetrator sends an account number to the victim if he wants to transfer money so he orders goods.

2.2.4 Reporting

Reports are the final stage carried out by investigators to present the results of data analysis that have been found. At this stage, the investigator will report the results of data analysis found in accordance with the NIST stage [30]. The report on the results of digital evidence from this research consists of the tools MOBILedit Forensic Express and AccessData FTK Imager.

2.2.4.1 MOBILedit Forensic

Results reporting obtained after using the MOBILedit Forensic Express Tool are in the form of data extraction results that are saved automatically in PDF form. The PDF file displays conversation proofs, usernames, phone numbers, photos, voice recordings, sent/received messages, product images and receipts transfer. The following is useful information which can be seen in Figure 9.



Figure 9. Evidence of finding the victim's smartphone contact

Figure 9 is evidence of findings related to user information in the form of the victim's name, photo, and WhatsApp number. While the replies to WhatsApp messages that have been deleted by fraudsters can be seen in Figure 10.



Figure 10. Display of Replies to WhatsApp Messages that have been deleted

Figure 10 is a display of messages sent (sent) and received (received) that have been deleted by the perpetrators of buying and selling fraud and there is evidence in the form of conversations, the date and time of sending the message, as well as a description of the message that has been read by the victim. In addition to the text conversation, further pictures of the products offered can be seen in Figure 11.

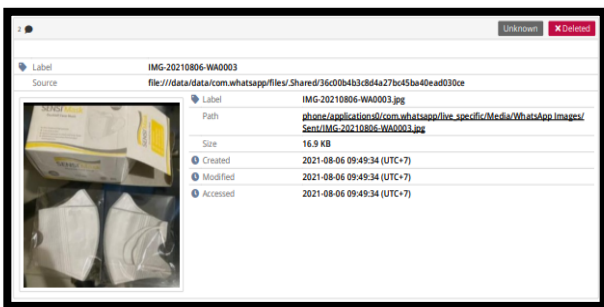


Figure 11. Proof of Mask Products Offered by Perpetrators

Figure 11 is the findings of mask products offered by fraud perpetrators at low prices. Furthermore, the examination of the conversations used as evidence of the crime of fraud can be seen in Figure 12.

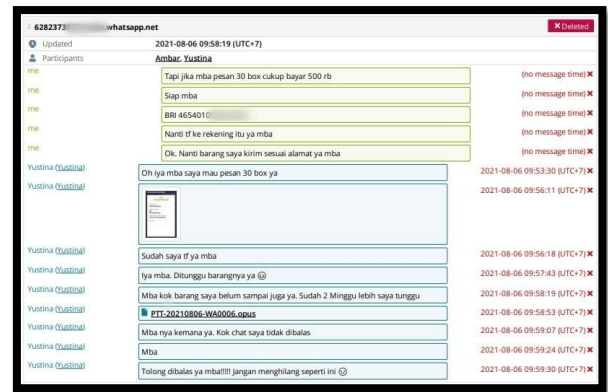


Figure 12. Deleted Conversation Evidence Fraudsters

Figure 12 is a conversation display deleted by perpetrators. The evidence of the conversation that was obtained and used as evidence of the crime of buying and selling fraud in the form of user information, the content of the conversation, when the message was sent and received, and the description of the conversation had been deleted by the perpetrator.

2.2.4.2 AccessData FTK Imager

The process of obtaining evidence on AccessData FTK Imager by analyzing the smartphone database perpetrators. The results of the search for evidence in the form of contacts smartphones can be seen in Figure 13.

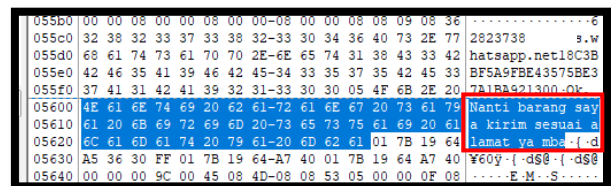


Figure 13. Evidence of Deleted Text Messages by Perpetrators

Figure 13 shows the findings of digital evidence in the form of text messages, and smartphone contacts that have been deleted by fraud perpetrators. Evidence of the victim having paid for the finished product ordering the goods can be seen in Figure 14.

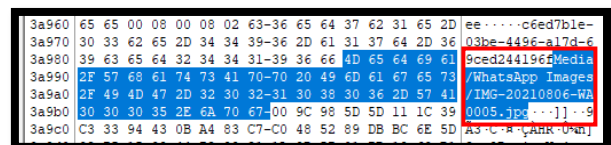


Figure 14. Proof of the victim having paid for the product

Figure 14 shows a picture message that proves the victim has paid for the product by matching the image code, namely **IMG-20210806-WA0005** the same as the image code obtained from MOBILedit.

2.2.5 Results

The results of the analysis using several tools, forensic namely MOBILedit Forensic Express and FTK Imager, resulted in data findings in the form of conversations that had been deleted by the perpetrators of fraud with the smartphone perpetrators that had been rooted. The digital evidence that has been obtained will be matched with the evidence of the conversation from the victim, which can be seen in table 2.

Table 2. Conversation Evidence from Victims and Digital Evidence Findings


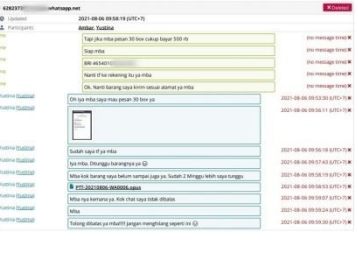
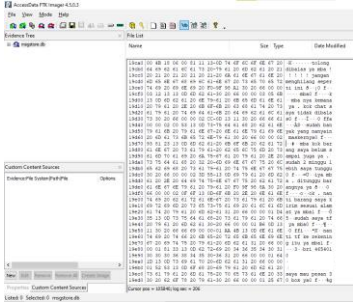
Conversation Evidence from the Victim	Findings of Digital Evidence (Conversation)
	<p>MOBILedit Forensic Express</p>  <p>AccessData FTK Imager</p> 

Table 2 shows the results of the search for evidence that found similarities between digital evidence reported by victims to report to investigators and digital evidence obtained using the MOBILedit and FTK Imager tools.

Table 3. Comparison of digital evidence findings from forensic tools

Smartphone Condition	Digital Evidence Results	Tools	
		MOBILedit Forensic Express	Access Data FTK Imager
Root	Conversation	✓	✓
	User Information	✓	-
	Smartphone Contact	✓	✓
	Time Message Sent/Received	✓	-

Table 3 shows results the findings were carried out using 2 tools, forensic namely MOBILedit Forensic Express and AccessData FTK Imager. The tool MOBILedit managed to get evidence, namely conversations, user information, contacts smartphone, and when the message was sent/received. Tools FTK Imager managed to find findings in the form of conversations, and contacts smartphones. Digital evidence analysis was carried out using several tools forensic, the results of the WhatsApp service analysis found digital evidence as shown in table 4.

Table 4. Findings of data that were successfully obtained


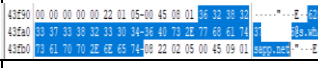
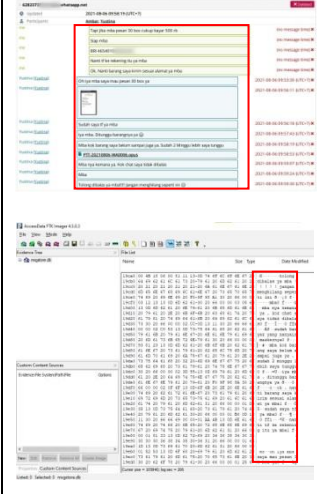

Information	Digital Evidence	Description
Account		found
Smartphone Contact		found
Conversation		found
Time of message sent/received		found

Table 4 shows the similarities between the digital evidence reported by the victim to the police with digital evidence obtained using the tools MOBILedit and FTK Imager, so it can be concluded that all information related to the fraud case that was successfully obtained is suitable and can be used as evidence digital in court.

3. CONCLUSION

The forensic process carried out to obtain digital evidence of criminal acts of fraud on the mobile-based WhatsApp service managed to find digital evidence in the form of conversations, user information, smartphone contacts, and when messages were sent/received. The evidence of conversations generated from the forensic process on smartphones with root conditions is in accordance with the purpose of the study. This study uses 2 forensic tools to analyze digital evidence, namely MOBILedit Forensic Express, and AccessData FTK Imager by applying the National Institute of Standard and Technology method. Evidence of findings from a rooted Smartphone managed to get 100% conversation data, 50% user information, 100% smartphone contacts, and 50% of the time messages were sent or received. The results of the smartphone that have been rooted managed to get evidence according to the digital forensic stage. This research uses the stages of the National Institute of Standards and Technology (NIST), for further research try with different stages. This study uses cases of buying and selling fraud on WhatsApp services, for further research it is recommended to use different cases, social media, and forensic tools.

4. REFERENCES

- [1] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Designing Digital Forensics on Twitter Applications Using Live Forensics Methods," *Semin. Nas. information. 2008 (semnasIF 2008)*, vol. 2018, no. November, pp. 86–91, 2018.
- [2] Y. Yenni, I. Utnasari, and M. Rahmawati, "Socialization of The Utilization of Internet Information Technology Based on Social Media As Business And Transactions," vol. 4, no. 1, pp. 1–6, 2021.
- [3] B. Mahendra, "Adolescent Social Existence in Instagram (A Communication Perspective)," *J. Visi Komun.*, vol. 16, no. 1, pp. 151–160, 2017.
- [4] Julian Arisandi, "NEWS: Digital 2020: Indonesian Internet Users in Numbers," *Cyberthreat.Id.* pp. 1–1, 2020, [Online]. Available: <https://cyberthreat.id/read/5387/Digital-2020-User-Internet-Indonesia-dalam-Angka>.
- [5] A. Aqmarina, A. Mujahidin, and M. Zainudin, "Analysis of Social Media as a Promotional Media and Online Customer Review of Purchase Decisions at Beaqis Olshop," vol. 5, no. 1, pp. 1–8, 2021.
- [6] T. Arifiyandi, "How Investigators Track Fraud Perpetrators in Online Selling," no. Iclc, 2019.
- [7] A. Dermawan, Amalia, and Sudarmin, "The role of mothers in being aware of online shopping fraud on social media," *Communnity Dev. J.*, vol. 2, no. 2, pp. 214–218, 2021.
- [8] J. Solim, MS Rumapea, A. Wijaya, B. Monica, and W. Lionggodinata, "Online Buying and Selling Site Fraud in Indonesia," vol. 5, no. 1, pp. 96–109, 2019.
- [9] R. Ayatulloh, K. Noor, R. Umar, and A. Yudhana, "Facebook Lite Social Media Analysis with Forensic tools using the NIST Method," vol. 21, no. 2, pp. 125–131, 2020.
- [10] P. Widiandana and I. Riadi, "Forensic Investigation Analysis of Cyberbullying on Whatsapp Messenger Using the National Institute Of Standards and Technology (NIST) Method," pp. 488–493, 2019.
- [11] MW Indriyanto, D. Hariyadi, and M. Habibi, "Digital Forensic Investigation and Analysis on WhatsApp Group Conversations Using NIST SP 800-86 and Support Vector Machine," vol. 3, no. 2, pp. 34–38, 2020.
- [12] MR Setyawan, A. Yudhana, A. Fadlil, P. Studi, M. Teknik, and UA Dahlan, "Identification of Skype Digital Evidence on Android Smartphones with the National Institute Of Justice (NIJ) Method," pp. 565–570, 2019.
- [13] D. Ari Mukti, Vishnu; Ummi Masruroh, Siti; Khairani, "Analysis and Comparison of Forensic Evidence for Facebook and Twitter Social Media Applications on Android Smartphones," no. May, 2020, doi: 10.15408/jti.v10i1.6820.
- [14] B. Raharjo, "An Overview of Digital Forensics," *J. Sociotechnology*, vol. 12, no. 29, pp. 384–387, 2013, doi:10.5614/sostek.itbj.2013.12.29.3.
- [15] G. Hendita, A. Kusuma, and IN Prawiranegara, "Digital Forensic Analysis of CCTV Video Recordings Using Metadata and Hashes," *Pros. Semin. Nas. Sis. inf. and Technol.*, vol. 3, no. 1, pp. 223–227, 2019.
- [16] AP Heriyanto, *Mobile Phone Forensics: Theory: Mobile Phone Forensics and Security Series*, 1st ed. Yogyakarta: Cv Offset Andi, 2016.
- [17] S. Madiyanto, H. Mubarak, and N. Widiyasono, "Mobile Forensics Investigation Process of Mobile Forensics Investigation on IOS-Based Smartphones," *J. Rekayasa Sist. eng.*, vol. 4, no. 01, pp. 93–98, 2017, doi:10.25124/jrsi.v4i01.149.
- [18] VRG Leri and I. Riadi, "Data Search for Pornographic Content on Twitter Services using National Institute of Standard and Technology (NIST) Method," *Int. J. Comput. app.*, vol. 183, no. 24, pp. 25–31, 2021, doi:10.5120/ijca2021921610.
- [19] SM Dusu, "Mobile Forensic of Facebook Services using National Institute of Standard Technology (NIST) Method," vol. 183, no. 33, pp. 9–15, 2021.
- [20] MS Asyaky, "Analysis and Comparison of Digital Evidence of Instant Messenger Applications on Android," *J. Researcher. Tech. information.*, vol. Vol. 3 No., No. 1, pp. 220–231, 2019.
- [21] IW Putra, A. Suharso, and C. Rozikin, "Digital Evidence Acquisition and Image Authenticity Detection on Whatsapp Using NIST and ELA Methods," vol. 5, no. September, pp. 712–726, 2021.
- [22] DA Imtinan, "Digital Forensics of Android-Based Facebook Messenger Services, Digital Forensics of Android-Based Facebook Messenger Services," 2020.
- [23] Intan Trivena Maria Daeng, N. . Mewengkang, and ER Kalesaran, "91161-ID-usage-smartphone-dalam-menunjang-ak," *e-journal "Acta Diurna"*, vol. 1, no. 1, pp. 1–15, 2017.
- [24] A. Sah, I. Riadi, and Y. Prayudi, "Online Gambling Digital Evidence Detection Using Live Forensics on Android-Based Smartphones," *CyberSecurity and Digit Forensics.*, vol. 1, no. 1, pp. 14–19, 2018.
- [25] R. Kumalasari, DW Setiyanto, and AF Yogananti, "Preventing Online Sales and Purchase Fraud through Designing Public Service Advertisements," 2016.
- [26] AU Awaliah and HY Prabowo, "Analysis of the role of Polda D . I . Yogyakarta in disclosure," vol. 3, pp. 140–156, 2021, doi:10.20885/ncaf.vol3.art13.
- [27] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Analysis of Digital Evidence Recovery for Instagram Messengers Using the National Institute of Standards and Technology (Nist) Method," *Semin. Nas. Technol. inf. and Commune. - Semant.*, pp. 161–166, 2017.
- [28] DA Putri, "Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method," vol. 183, no. 30, pp. 1–8, 2021.
- [29] AP Utami, "Mobile Forensics Analysis of Line Messenger on Illegal Drug Transaction Case using National Institute of Standard Technology (NIST) Method," vol. 183, no. 32, pp. 23–33, 2021.
- [30] M. Jannah, "Forensic Browser on Line Messenger Services for Handling Cyberfraud using National Institute of Standard Technology Method," vol. 183, no. 30, pp. 9–16, 2021.