

# Mobile Forensic of Facebook Messenger on Cyber Fraud Case using National Institute of Standard Technology Method

Regina Fitria

Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

Imam Riadi

Department of Information System  
Universitas Ahmad Dahlan  
Yogyakarta of Indonesia

## ABSTRACT

In Indonesia, Facebook messenger users are growing rapidly, especially on mobile devices, this development brings positive and negative impacts. The most common impact at this time is crimes committed in cyberspace, one of which is online buying and selling fraud. Facebook messenger is one of the instant messaging applications with the largest number of users, so there are opportunities for cybercrime. To obtain digital evidence, this research uses the National Institute of Standards and Technology (NIST) stages. The research was conducted using a mobile-based Facebook messenger application with a conversation scenario created by the author. The study was conducted to restore deleted conversations, the steps used in this study were collection, examination, analysis and reporting. This study also uses two smartphones in the condition that one smartphone is rooted and the second smartphone is not rooted, both smartphones are used as evidence. The acquisition process uses several forensic software including MOBILedit Forensic Express, Systool SQLite and AccessData FTK imager. Digital evidence obtained using the MOBILedit Forensic Express tools is 75%, then Systool SQLite tools are 67% and AccessData FTK imager tools are 67%. The results obtained from this research are conversations that have been deleted and user accounts on smartphones that are rooted while in unrooted smartphones don't get digital proof.

## Keywords

Mobile forensics, Facebook Messenger, Cybercrime, Online buying and selling fraud, NIST, Smartphone

## 1. INTRODUCTION

The development of internet technology has given birth to new citizens called networked communities who perform virtual social interactions, one of the most popular social media applications is Facebook Messenger. In 2025 the number of Facebook users in Indonesia is estimated to reach more than 256 million, an increase of around 185 million in 2019 [1]. Facebook Messenger is an instant messaging application, which distinguishes it from other instant messaging applications, Facebook Messenger is a third-party application. With the largest number of users, of course, it is also an opportunity to be used as a communication medium for negative purposes. The Facebook Messenger application, which is very familiar to Indonesian people, allows users to send messages in the form of text, images, videos, and voice messages [2]. Online fraud is one of the most reported crimes. From January to September 2020, online fraud took the top two positions. Around 28.7% of cybercrimes come from this category. From 2016 to 2020 In September, the total reported cases of online fraud totaled 7,047. On average, there are

1,409 cases of online fraud every year, crimes committed using computers or computer networks as tools, targets and places for crime, including child pornography, fraud online, bullying, identity fraud, and others [3]. The research was conducted using a Facebook messenger-based mobile application with a conversation scenario created by the author. The study was conducted to restore deleted conversations, the steps used in this study were collection, examination, analysis and reporting. This study also uses two smartphones in the condition that one smartphone is rooted and the second smartphone is not rooted, both smartphones are used as evidence [4].

## 1.1 Research Literature

### 1.1.1 Previous Study

Yudhana, Riadi & Anshori (2017) conducted a study entitled Forensic Analysis of Instant Messenger Applications on Android-Based Smartphones. To obtain information from digital evidence, namely the NIST (National Institute of Standards Technology) stage. The NIST stage has work guidelines, both policies and standards to ensure each examiner follows the same workflow so that work is documented and the results are repeatable and defensible [5].

Prasongko, Yudhana & Fadir (2018) conducted a study entitled Cocotalk Forensic Analysis Investigation using the National Institute Standard Technology method. The android application used to help gain root access is King Root which will be analyzed, carry out the process of removing digital evidence from the KakaoTalk application using the MobilEdit Forensic Tool software. The process to obtain digital evidence is carried out using the NIST method [6].

Bintang, Umar & Yudhana (2020) in his research entitled Facebook Lite social media analysis with forensic tools using the NIST method. This study uses MobilEdit Forensic tools which are useful for extracting data from a Smartphone to be analyzed. The results that have been obtained in using forensic tools are ID accounts, images, audio, and audio [7].

Umar & Sahiruddin (2019) in a study entitled NIST Method for forensic analysis of digital evidence on android devices. This study aims to recover deleted data in the form of contact data, call logs and messages on smartphone devices that are evidence. The tools used are dead forensics and live forensics, Retrieval of digital evidence using the National Institute of Standards and Technology (NIST) method [8].

Fitriana, Khairan & Marsya (2020) has conducted research with the title Application of the National Institute of Standards and Technology (NIST) method in digital forensic analysis for handling cybercrime. This research was

conducted to investigate the WhatsApp application to obtain evidence that had previously been deleted in the form of conversations, contact lists, profile photos of victims and others. The study was conducted by reading the database files that have been backed up through the WhatsApp application which is encrypted to save deleted conversations. This research uses the method (National Institute of Standards and Technology (NIST). Digital evidence can be obtained using one of the forensic tools, namely WhatsApp Viewer [9].

### 1.1.2 Forensic Digital

Forensics is the use of analytical and investigative techniques to identify, collect, examine and store evidence/information that is magnetically stored/encoded on a computer [10]. Digital Forensics can be said to be the use of science to recover digital evidence on a device, be it a computer or smartphone with certain stages, aiming to collect data that is accepted by the court as one of the evidences [11]. Digital forensics itself has sub-disciplines that are divided into several: computer forensics, mobile forensics, memory forensics, network forensics, malware forensics, operating system forensics, image forensics, cloud computing forensics, and audio forensics [12]. 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 [13]

### 1.1.3 Forensic Mobile

Forensics mobile is digit response forensics to the development of information technology has been evolving the traditional computer device into a tablet computer and communication world have been applying computer very well so that it becomes a smartphone [14]. Forensics on mobile devices can retrieve data from mobile phones and by itself can be used as digital evidence, mobile forensics is a branch of digital forensics that deals with the return of digital evidence or data from mobile devices, but can also relate to digital devices that have internal memory and communication skills [15].

### 1.1.4 Digital Evidence

Evidence is very important for proving computer crime cases involving storage media devices. Digital Evidence in question can be in the form of: E-mail, word processor files, spreadsheets, source code of software, images, web browsers, bookmarks, cookies, calendar, If there is an error in the handling of the evidence, it may not be recognized in court. By accepting relative evidence in a crime, half the truth has been revealed. The next step is to follow up on the existing evidence in accordance with the objectives to be achieved [16].

### 1.1.5 Social Media

Social media is a tool or container to convey information where the process of delivering th at information can be done more easily, quickly, and personally [17]. The development of information and communication technology continues to increase throughout the world including Indonesia, the increasing use of social media can be a huge opportunity for business people to do business through various types of social.

### 1.1.6 General Review Facebook Messenger Application

Facebook is a website that has a social networking service where users can interact with many people likely to come from all over the world [18]. Some of the features of facebook

messenger include: New message, voice call, video call, attach photo or video, GIF is a feature used to select a GIF to be sent to chat friends, sticker selection, emoji selection is, voice clip is a message feature that can be sent to chat friends, file attachments choose the type of file to be sent in the form of an image file, video file, or document file column to search for contacts, chat rooms, or find a word in a conversation.

### 1.1.7 Smartphone

The development of technology smartphone is also accompanied by many social media users that can make it easier to interact between users. The number of active social media users worldwide reaches 2.31 trillion, which is equivalent to 31% of the world's total population. In January 2016 social media users who accessed smartphones were 1.97 trillion or equivalent to 27% of the world's population [19].

### 1.1.8 Cybercrime

Cybercrime is one of the negative impacts of technological developments that cause extensive losses for all modern life today [20]. Instant messaging App Mobile opens up opportunities for cybercrime to increase. Cybercrime is a crime that can be committed by individuals or groups of people by using computers or the internet, cybercrime can be interpreted as an unlawful act committed by using a computer network as a means/tool or a computer as an object, both for profit or not [21]. There are two categories of cybercrime, the first category of violence/potential violence is a computer device that causes a physical impact on another person [22].

### 1.1.9 Fraud Online

Currently, crimes that occur cannot be categorized as physical crimes, but crimes are currently also experiencing development along with the modernization of life. fraud Online scams, in principle, the same as the conventional to be a difference only in the deeds means using Electronic Systems (computers, internet, telecommunication devices) [23].

### 1.1.10 Buying and Selling Online

In Indonesia, e-commerce has been known since 1996, although it is not very popular. In 1999 to 2006 transactions e-commerce attracted attention even though it was only limited to a minority of Indonesian people who were familiar with technology. E-commerce brings advantages, but on the other hand it also has weaknesses in terms of security because it uses a public network and transactions are indirect (Faceless nature) [24].

### 1.1.11 National Institute of Standard Technology (NIST)

National Institute of Standards and Technology (NIST) is a forensic stage that has a policy of work guidelines and standards to ensure each examiner follows the same workflow so that work is documented and the results can be repeated and can be maintained [25].



Figure 1. Stages of the National Institute of Standard Technology method

Figure 1 shows the national institute of standard technology (NIST) stage has four stages to carry out the mobile forensics investigation process to obtain digital evidence. The four stages are Collection, Examination, Analysis, and Reporting.

### 1.1.12 Rooting

Rooting is a process that allows a smartphone to have full access (super user), by rooting a smartphone can access and modify system files which are usually limited by the OS. The main disadvantage of rooting is that it is a security and privacy risk and the device has no warranty if rooting the device will void the warranty and the only way to get it back is to unroot the device [26].

### 1.1.13 MOBILedit Forensic Express

MobilEdit is software that is used to extract, analyze data, and generate reports on the results of data extraction on smartphones. This tool uses several connectivity mechanisms, especially wireless connectivity compared to similar tools. This software is good enough to use for get telephone system information and other information such as contact lists and messages [27].

## 2. METHODOLOGY

### 2.1 Research Scenario

Case scenarios in the form of online buying and selling transactions on social media, the following picture illustrates the steps of how digital evidence is obtained in online buying and selling cases and the evidence can be used as accurate evidence in court.

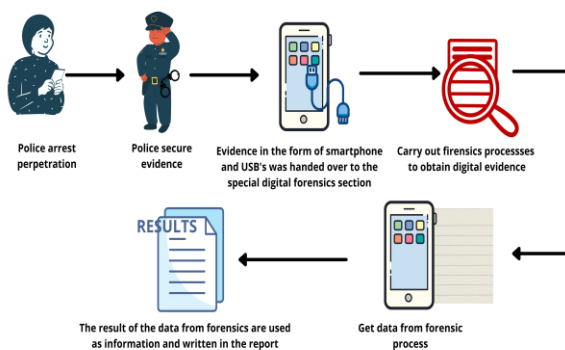


Figure 2. Digital evidence search and collection flow

Figure 2 The police arrested the perpetrator and the police secured evidence from the seller (suspect) who had made a transaction with the buyer (victim) through social media Facebook messenger using a smartphone. During the arrest the police got a smartphone after that the police secured the smartphone as evidence and stored it in an available place. The evidence is brought to the forensics department to carry out further investigations to obtain evidence and can be used as evidence in court. In the Facebook application messenger on a smartphone, a message was found that had been deleted by the seller (the suspect), to retrieve the deleted message in order to obtain evidence, the forensics carried out an examination using several procedures using software forensic.

## 2.2 Research Stages

Search for evidence on a-based Facebook application was mobile carried out using the stages National Institute of Standard Technology (NIST) to find evidence that led to buying and selling fraud online.

### 2.2.1 Collection

The stage collection is a process in which to collect digital evidence data that can be used as evidence during the trial.

Table 1. Evidence Found at the Crime Scene





No	Name of Evidence	Figure	Description
1	Smartphone of the suspect		Smartphone brand Samsung galaxy V2 J1 mini prime
2	USB cable of suspect		Micro USB used by suspect
3	Smartphone of victim		Smartphone brand of Samsung Galaxy A30s
4	USB cable of victim's		USB type-C belonging to victim

Table 1 Evidence found by the police and submitted to investigators for analysis.

#### 2.2.1.1 Smartphone rooted condition

The data acquisition process uses the MOBILedit Forensic Express tool, a smartphone that has been rooted is connected to a laptop using a data cable for the process transfer data on the smartphone.

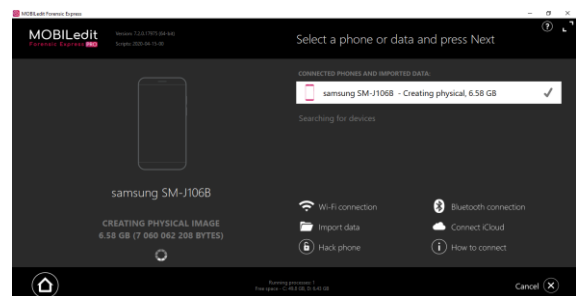


Figure 3. Imaging process on a rooted smartphone

Figure 3 display of imaging file process on a running smartphone using the MOBILedit tool. When the process is complete, the imaging results will be stored in the pre-arranged directory.

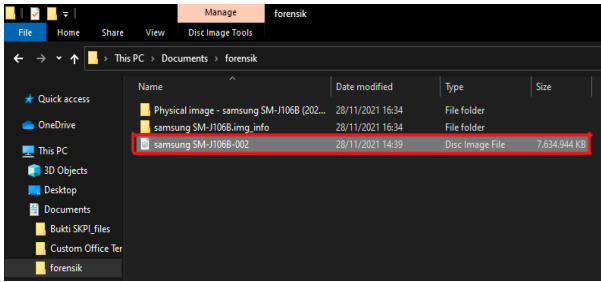


Figure 4. Results of imaging data on a smartphone

Figure 4 imaging results on a rooted smartphone on file imaging is used to search for messages that have been deleted using forensic tools

### 2.2.1.2 Smartphone is not rooted

Process collection on a smartphone that is not at the root of the imaging process cannot be done because the initial appearance MOBILedit there is no menu Create Physical image that serves to imaging data on the smartphone corresponding original data.

### 2.2.2 Examination

The Examination stage is the stage for examining and acquiring data from the imaging results file that has been carried out previously, the acquisition process is carried out using the MOBILedit tool this process is carried out to obtain the desired digital evidence. Furthermore, the data acquisition process in the imaging results file after the acquisition process is complete is continued by extracting data on the Facebook messenger application, the extraction process produces output formats such as HTML report, PDF report, MS Excel report and output data exports in the form of MOBILedit backup, MOBILedit export and UFDR

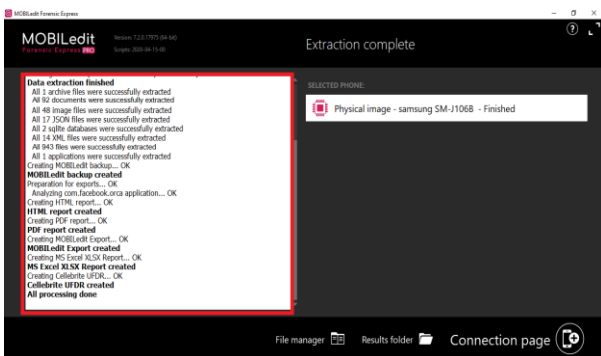


Figure 5. Extraction process on facebook messenger application

Figure 5 Extraction process on facebook messenger app and shows successful extraction on rooted smartphone.

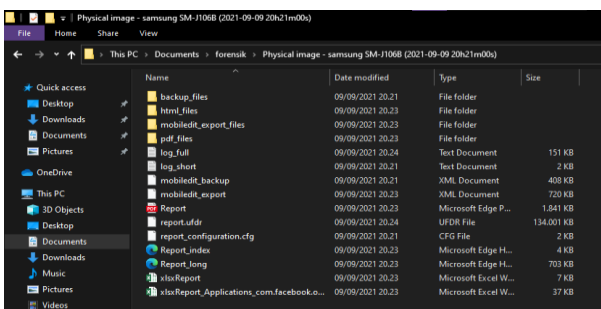


Figure 6. Extraction results on the application

The result of data extraction on smartphones found complete profile data along with conversations that had been previously deleted by the suspect.

### 2.2.2.1 Hashing

This stage is the stage to protect evidence from damage and data integrity, hashing is done to find out whether the data that has been successfully backed up is still original and has not been modified or has been modified. Hashing is done using Hash tool 1.2.

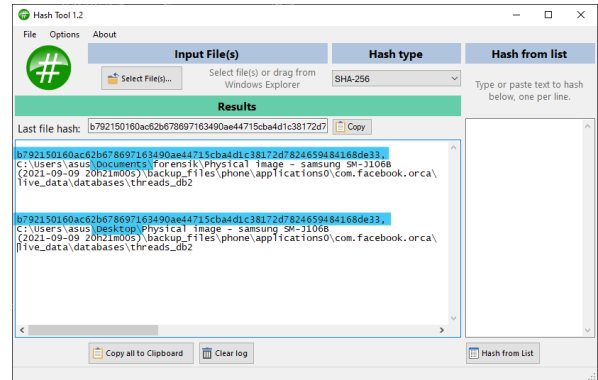


Figure 7. Hashing database of data acquisition results

Figure 7 shows hashing results from both files that there is the same encryption code, which means no data changes.

### 2.2.3 Analysis

Analysis is the stage to get digital evidence from evidence in the form of a smartphone that has been rooted by the perpetrator. The evidence to be sought is in the form of a chat that has been deleted by the suspect. In this process, several forensic tools are used, including MOBILedit Forensic Express, AccessData FTK Imager and SysTools SQLite Viewer.

### 2.2.3.1 MOBILedit Forensic Express

The stages of analysis of evidence are found on a smartphone in a rooted state by analyzing files that have been extracted previously.

Table of Contents	
Applications	1
com.facebook.orca	1
Accounts	2
Conversation Users	3
Conversations	4
Messages	6
Other Media Files	13
Images	13
Video	42
Documents	43

Figure 8. Table of contents extracted data from facebook messenger

Figure 8 information about the application used, the perpetrator's account, contacts (friends list), messages, chats and other media files such as images, emoticons, audio, video and documents.

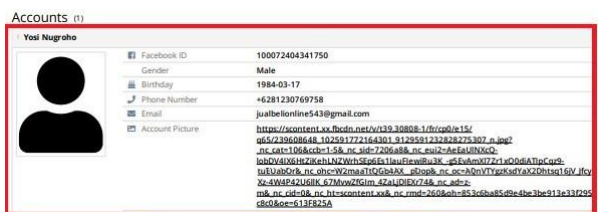


Figure 9. Suspect account details



Figure 9 shows the account details used by the suspect to commit online buying and selling fraud.

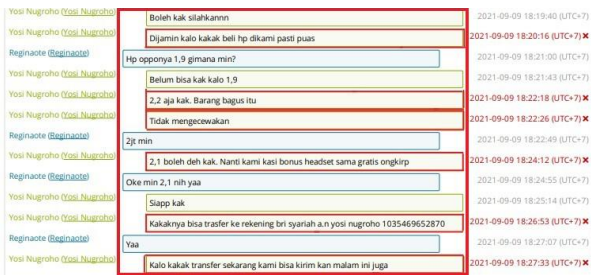


Figure 10. Conversations that were successfully recovered

Figure 10 Show chats that were successfully restored, there were 2 participants in the conversation, namely the suspect and the victim. The conversations that have been deleted by the suspect are 6 conversations.

### 2.2.3.2 SysTools SQLite viewer

Stages of analysis to get evidence in the database the smartphone suspect's. The database file can be retrieved in the previously extracted data folder.

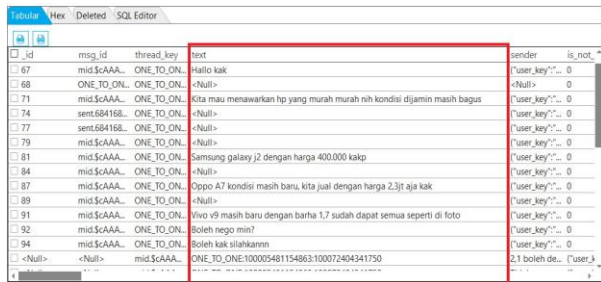


Figure 11. Conversation details on database

Figure 11 database on the messenger, the conversation between the suspect and the victim can be seen in the Text column. The evidence obtained is only in the form of chat conversations while chat in the form of images cannot be obtained.

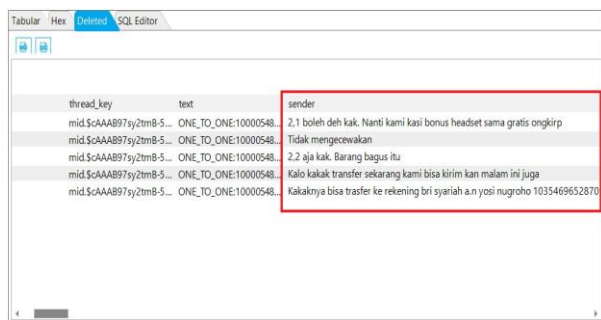


Figure 12. The conversation has been deleted

Figure 12 table view of conversations that have been deleted by the suspect

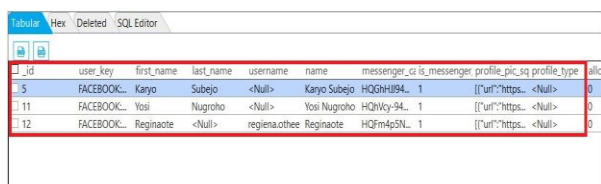


Figure 13. list of users who are in the conversation

Figure 13 table User there are three users in the table including the user selecting the suspect and the user belonging to the victim.

### 2.2.3.3 AccessData FTK Imager

Analysis to get evidence also uses tools AccessData FTK Imager. The analysis process also uses results imaging that have been done previously, digital evidence obtained in the form of conversations by entering keywords to find the conversation you are looking for, in addition to conversations other digital evidence found is the suspect's email and username.

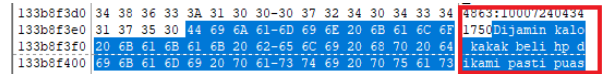


Figure 14. The 1st conversation that was deleted

Figure 14 by entering the keyword "Guaranteed if you are a brother".

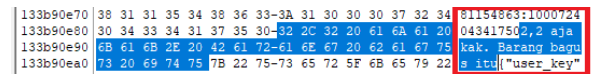


Figure 15. The 2nd conversation deleted

Figure 15 by entering the keyword "2.2 only".

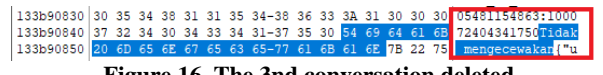


Figure 16. The 3rd conversation deleted

Figure 16 by entering the keyword "Not disappointing".

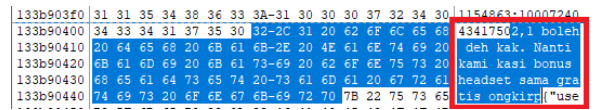


Figure 17. The 4th conversation that was deleted

Figure 17 by entering the keyword "2.1 okay".

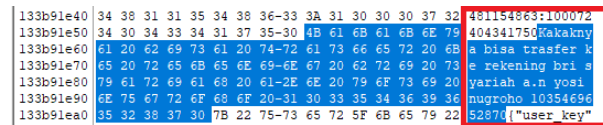


Figure 18. The 5th conversation that was deleted

Figure 18 by entering the keyword "account".

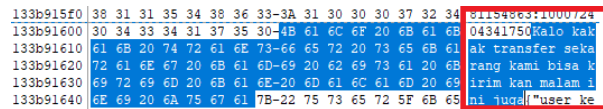


Figure 19. The 6th conversation that was deleted

Figure 19 by entering the keyword "Kalo brother".

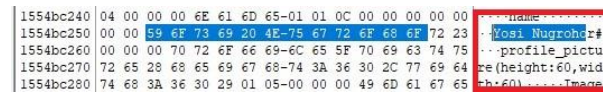
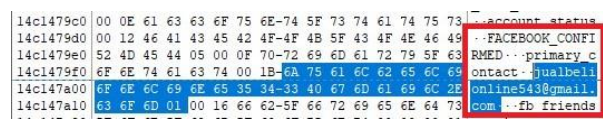





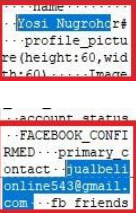
Figure 20. The suspect's email and username

Figure 20 by entering the keywords “online buying and selling” and “yosi nugroho”.

### 2.2.4 Reporting

The reporting stage is the stage of reporting the results of the evidence found by investigators. The application used is the Facebook messenger application and uses a rooted Samsung Galaxy J1 mini prime smartphone and also uses case simulation for research, to obtain assistance items by using several forensic tools including Forensic MOBILedit, SysTools SQLite and FTK Imager to acquire and extract data. that is on the smartphone. The results on the rooted smartphone belonging to the perpetrator were then adjusted to the evidence provided by the victim.

**Figure 2. Findings of Evidence from the perpetrator's Smartphone**

Evidence from the victim	Evidence found on the perpetrator's smartphone
	<p><b>Text messages on messenger</b></p>  <p><b>Image Product and Payment</b></p>  <p><b>Username and Email</b></p> 

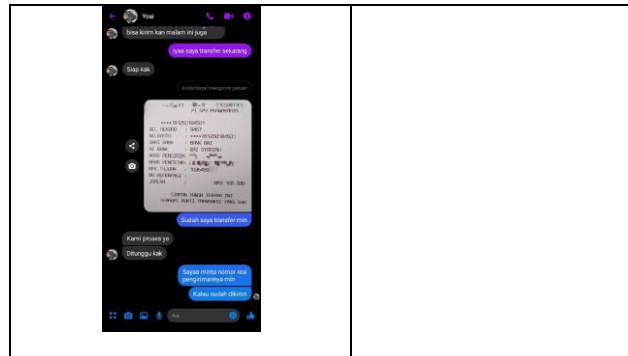


Table 2 It was concluded that from the table of digital evidence obtained with the evidence provided by the victim, it was the same person who had committed online buying and selling fraud, this was reinforced from the seller's account, text messages and pictures perfectly matched the evidence provided by the victim.

### 2.2.5 Results

The results were found with a smartphone that was rooted and used several forensic tools to help obtain digital evidence. This study focuses on rooted smartphones to look for evidence. The comparison of a smartphone that has been rooted with a smartphone that has not been rooted can be seen in table 3.

**Table 3. The comparison of the results of the second smartphone**

Smartphone condition	Tools	Result of evidence			
		Conversation	Picture	Account	Chat time
Rooted	MOBILedit Forensic	✓	✓	✓	✓
	SysTools SQLite	✓	X	✓	X
	FTK Imager	✓	X	✓	X
Not Rooted	MOBILedit Forensik	X	X	X	X

Table 3 In data extraction using the MOBILedit Forensic Express Tools on a rooted smartphone, a conversation between the suspect and including the conversation that was deleted along with the images sent and the accounts of the two users involved in the conversation and the time of the conversation took place was also investigated. using the SysTolls SQLite Viewer tool to generate conversations between the suspect and the victim including deleted conversations as well as the suspect and victim's accounts, the investigator also uses the AccessData FTK Imager tool, the results obtained are the same when the investigator uses the tools. Meanwhile, on a smartphone that is not rooted, it cannot be searched for evidence.

## 3. CONCLUSIONS

The conclusion is based on the results of the research entitled "Mobile Forensic of Facebook Messenger on Cyber Fraud Case using the National Institute of Standard Technology Method" using case studies on the Facebook Messenger application and searching for evidence using several forensic tools, including MOBILedit Forensic Express, SysTool

SQLite and AccessData FTK Imager. Digital evidence has been successfully obtained on a smartphone that has been rooted, while on a smartphone that has not been rooted the data cannot be retrieved. The digital evidence obtained are deleted conversations, pictures, perpetrator accounts and chat time between perpetrators and victims and the results of digital evidence obtained using the MOBILedit Forensic Express tool is 75%, the tool is Systool SQLite 67% and the tool is AccessData FTK imager 67%. The search for digital evidence that has been obtained uses the stages at the National Institute of Standards and Technology (NIST).

#### 4. REFERENCES

- [1] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analysis of Digital Evidence for Facebook Messenger Applications on Android Smartphones Using the NIJ Method," *IT J. Res. Dev.*, vol. 5, no. 2, pp. 118–134, 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.
- [2] I. Ali, "Crime Against Information (Cybercrime) In the Context of Digital Libraries," *Visi Pustaka*, vol. 14, no. 1, pp. 32–38, 2012.
- [3] I. Alsmadi *et al.*, "Mobile Forensics," *Pract. Inf. Secur.*, pp. 297–308, 2018, doi: 10.1007/978-3-319-72119-4\_13.
- [4] 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.
- [5] I. Zuhriyanto *et al.*, "Forensic Digital Design In Applications," *Semin. Nas. Inform.*, vol. 2018, no. November, pp. 86–91, 2018.
- [6] J. P. Soepomo, "Forensic analysis of the KakaoTalk application using the National Institute Standard Technology method," vol. 2018, no. November, pp. 129–133, 2018.
- [7] M. I. Syahib *et al.*, "Beetalk Application Digital Forensic Analysis For Handling," vol. 2018, no. November, pp. 134–139, 2018.
- [8] 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.
- [9] P. T. Informasi and F. Tarbiyah, "Application Of The National Institute Of Standards And Technology (Nist) Method In Digital Forensic Analysis For Cyber Crime Handling," vol. 4, pp. 29–39, 2020.
- [10] S. R. Ardiningtias *et al.*, "Digital Investigation On Facebook Messenger," pp. 19–26, 2018.
- [11] G. Atiko, R. H. Sudrajat, K. Nasionalita, and U. Telkom, "Abstract The development of technology, information and communication that continues to increase makes the number of Internet users also higher throughout the world every year, Indonesia is no exception. Besides Facebook, Twitter, Youtube, Path, Line," Anal. strategy. Tourism Promotion Through Social Media. By The Ministry Of Tourism Of The Republic Of Indonesia (*studi deskriptif pada akun Instagram @indtravel*), vol. 3, no. 2, pp. 2349–2358, 2016.
- [12] R. A. K. N. Bintang, R. Umar, and U. Yudhana, "Live forensics comparison design on Instagram, Facebook and Twitter social media security on Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128, 2018.
- [13] D. A. Putri, "Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method," vol. 183, no. 30, pp. 1–8, 2021.
- [14] O. El, C. Natalia, S. I. Kom, and M. Si, "Youth, Social Media And Cyberbullying Background on the role of youth as a means to connect with social media. tool people to do," vol. 5, 2016.
- [15] R. Firmansyah, "News Clarification Web to Minimize the Spread of Hoax News," vol. 4, no. 2, pp. 230–235, 2017.
- [16] D. Hariyadi *et al.*, "Analysis Of Digital Evidence Applications On Paziim Phone Paziim Digital Evidence Analysis Application On Android," vol. 2, no. 2, pp. 52–56, 2019.
- [17] T. Jual *et al.*, "consumers to internet transactions, electronic means can also be under the Criminal Law Act. – Law on Information and there are two important things, namely," vol. 5, no. 7, pp. 1–13, 2016.
- [18] W. A. Luqyana, I. Cholissodin, and R. S. Perdana, "Cyberbullying Sentiment Analysis on Instagram Comments with the Support Vector Machine Classification Method," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 11, pp. 4704–4713, 2018.
- [19] Y. Prayudi and D. S. Afrianto, "Anticipation Of Cybercrime Using Computer Engineering," vol. 2007, no. Snati, 2007.
- [20] B. Raharjo, "Digital forensics at a glance," pp. 384–387.
- [21] J. P. Soepomo, "Forensic Analysis Of Digital Evidence On Frozen Solid State Drive Using The National Institute Of Standards And Technology (Nist) Method," Vol. 2, No. 2, Pp. 33–40, 2017.
- [22] D. A. Putri, "Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method," vol. 183, no. 30, pp. 1–8, 2021.
- [23] R. Sistem *et al.*, "Investigating Cyberbullying on WhatsApp Using Digital Forensics," vol. 1, no. 10, pp. 730–735, 2021.
- [24] P. Studi, T. Informatika, U. Ahmad, J. P. Soepomo, and S. H. J. Yogyakarta, "Forensic Analysis Instant Messenger Application," vol. 2, no. 2, pp. 25–32, 2017.
- [25] P. Widiandana and I. Riadi, "Cyberbullying Forensic Investigation Analysis On Whatsapp Messenger Using The National Institute Of Standards And Technology (Nist) Method," pp. 488–493, 2019.
- [26] P. A. K. D. J. Kharade, "Rooting & Custom Rom in Android," *Int. J. Sci. Res.*, vol. 6, no. 4, pp. 1945–1950, 2017, doi: 10.21275/ART20172750.
- [27] I. Z. Yadi and Y. N. Kunang, "National Conference on Computer Science (KONIK) 2014 Forensic Analysis on Android Platform," *Konf. Nas. Ilmu Komput.*, p. 142, 2014, [Online]. Available: <http://eprints.binadarma.ac.id/2191/>.