Mobile Forensics Analysis of Line Messenger on Illegal Drug Transaction Case using National Institute of Standard Technology (NIST) Method

Aulia Putri Utami
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The rapid development of technology and information every year has caused an increase in the use of social media applications in the world to jump up to 40 percent due to the COVID-19 pandemic. The increase in the use of IM applications is followed by the development of the negative side of the use of technology, one of which is drug transactions. This study makes a simulation for cases of online drug transactions through the LINE service on an Android-based smartphone which is analyzed using the steps recommended by the National Institute of Standards and Technology. Simulation tests were carried out using Magnet AXIOM, Autopsy, and MOBILedit Forensics Express displayed with the DataReader program. Based on the test results, digital evidence in the form of LINE accounts, pictures, phone history, and geo-locations that have been deleted have been successfully recovered with the percentage of discovery using MOBILedit as much as 71%, Autopsy 57%, and Magnet AXIOM 43%. The results of word cloud visualization using text mining in the RStudio application also succeeded in detecting words related to drug cases, namely paket and gorila.

Keywords

Forensics, Mobile, LINE, Narcotics, NIST, Wordcloud

1. INTRODUCTION

The use of social media has grown very rapidly over time. Social media is a tertiary need whose needs must be met like a primary need and can be enjoyed anywhere and by anyone without exception [1]. Social media is a product in the form of internet-based interactive applications from the rapidly growing information revolution in the last ten years that has changed the way information and communication are managed [2]. One application that is experiencing rapid development is an instant messaging application [3]. One of the IM services that are currently being downloaded and used by users in Indonesia is LINE. The LINE application is available in both mobile and web versions, which allow to exchange information with other users in real-time uses text messages, voice messages, stickers, emoticons, and share files, such as documents, photos, songs, and videos, so that many people prefer to use IM applications to communicate compared to using electronic mail (e-mail) or Short Message Service (SMS). The increasing use of IM applications also increases the negative side of the use of social media applications that lead to crimes committed using computers, known as cybercrime. Cybercrime is a crime that uses a computer as a tool, target, or place of crime. Examples of cybercrime, such as child pornography, online fraud, bullying, identity fraud, illegal drug transactions, and others [4]. A worrying condition occurs when the cybercrime perpetrators are experts in anti-cybercrime actions so that if there is a new mode of cybercrime, it will be difficult to detect and solve by digital forensic investigators [5]. LINE has the potential to be used as a means of crime, one of which is conducting illegal drug transactions. If initially, dealers met in person to the transaction, now have shifted through online buying and selling patterns, sending goods using expedition services through a marketplace platform, exchanging messages through social media, then hiding them in t-shirts, cosmetics, or electronic goods. How to catch the suspect of digital crimes requires evidence at trial. One of the sciences to get digital evidence is to do digital forensics [6]. Based on the above background, this research will conduct a mobile forensic analysis to obtain digital evidence with scenarios of online illegal drug transactions through the mobile-based LINE application.

2. STUDY LITERATURE

2.1 Previous Study

Previous study conducted by (Wicaksana & Suhartana, 2020) with the title "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method" explained the forensic process carried out to obtain the results of the analysis of digital evidence that can be used. strengthen evidence of criminal cases in court. The conclusion is obtained based on several results from the stages of the method that have been carried out, the analysis process of data on Twitter social media can be said that digital evidence is in the form of valid data evidence [7].

Previous research was conducted by (Riadi, Umar, & Aziz, 2019) with the title "Web Forensics Instant Messaging Services Using the Association of Chief Police Officers (ACPO) Method" which researched the stages of forensic investigation of digital crime cases that occurred in the application. WhatsApp, LINE and Telegram are web-based using the Association of Chief Police Officers method. The conclusion is obtained from the results of calculations with the existing formula, WhatsApp gets an index number of 80%, LINE is 60%, and Telegram is 40% so that WhatsApp is the application with the highest success rate of digital forensics [8].

Previous research conducted by (Umar & Sahiruddin, 2019) entitled "NIST Method For Forensic Analysis of Digital Evidence on Android Devices" describes the forensic process using two forensic tools Wondershare dr.Fone for Android and Oxygen Forensics Suite 2014 to obtain digital evidence in the form of Contact data, call logs, and messages that have been deleted on an android smartphone. The conclusion obtained is based on the results of research from the Samsung

Galaxy J1 Ace smartphone that recovery with the Wondershare tool only reaches 30%, while the results of recovery with Oxygen forensics reach 73% of deleted data can be restored. Thus, the data from the recovery of digital evidence with the Oxygen tool is highly recommended as evidence in proving criminal cases in court [9].

Previous research conducted by (Ikhsan & Hidayanto, 2016) with the title "Forensic Analysis of Whatsapp and LINE Messenger on Android Smartphones as a Reference in Providing Strong and Valid Evidence in Indonesia" describes the process of investigating digital evidence from the WhatsApp and LINE applications on the Android operating system by creating regular conversation scenarios and deleting. It is concluded that digital data evidence has been successfully obtained using manual methods and additional applications. The data that was successfully obtained were contacts, conversations, media, and backup databases. WhatsApp is an application that is used as a reference in digital forensics, while LINE Messenger is a safer application because it is more difficult to carry out a digital forensic analysis [10].

The last previous research conducted by (Fitriana, Khairan & Marsya, 2020) with the title "Application of the National Institute Of Standards And Technology (NIST) Method in Digital Forensic Analysis for Handling Cyber Crime" describes the forensic process to obtain evidence by conducting simulations or scenarios that utilize the WhatsApp messenger application to handle cybercrime cases. The conclusion obtained is based on the pornography case that has been simulated previously and due to the disappearance of evidence, according to legal experts, the perpetrator gets a sentence based on the law that has been set the first is the legal aspect for pornography cases which are subject to law article 27 paragraph (1) The ITE Law and the second case, namely the disappearance of evidence, will be subject to Article 282 of the Criminal Code [4].

2.2 Digital Forensics

The term forensics is a scientific process based on science in collecting, analyzing, and presenting various evidence in court proceedings related to the existence of a legal case [11]. Another definition of digital forensics is the application of computer science and technology for legal evidence, which in this case is proof of crime using computer equipment so that digital evidence can be obtained that can be used to catch the suspect of the crime [12]. One of the benefits of digital forensics is to understand computer systems and other digital devices better [13].

2.3 Digital Evidence

In the investigation carried out, there must be evidence that is stored, either evidence of information or data. Digital evidence is defined as information and data of value for investigations that are stored, received, or transmitted by electronic devices. Digital evidence can be defined as electronic information collected when investigating a case involving digital devices, such as e-mail, online banking transactions, photos, web history as well as audio and video [14].

2.4 Mobile Forensics

Mobile forensics is a branch of digital forensics which deals with the recovery of digital evidence or data from mobile devices under forensics. The use of mobile phones such as smartphones with various types and operating systems for crime is increasing and mobile forensics can help crime cases related to mobile devices, especially smartphones [15]. In mobile forensics, data taken from smartphones can be used as digital evidence. This evidence can be used as a basis when investigating a case by law enforcement agencies [16].

2.5 Android

Android is an operating system for Linux-based mobile devices that includes an operating system, middleware, and applications. Android provides an open platform for developers to create applications. On the other hand, Google releases Android codes under the Apache license, a software license, and an open platform for mobile devices. Android smartphones can be used by everyone with various features that are increasingly varied with the ease of getting applications from the play store that can be downloaded for free. [17].

2.6 Narcotics

Narcotics are substances or drugs that can be natural, synthetic, or semi-synthetic which can cause side effects in the form of decreased consciousness, hallucinations, and excitability. These drugs can cause addiction if used excessively. The use of these substances is a painkiller and provides peace of mind. Misuse can be subject to legal sanctions [18].

2.7 Instant Messenger

Instant Messenger (IM) or commonly called a chat application is a software that facilitates the sending of short messages, a form of direct communication between two or more people using typed text. Text is sent through a computer connected to a network, such as an internet [19]. Instant Messaging is an online chat application that offers real-time text messages and the transmission of audio, video, and image files via the internet [20].

2.8 LINE

LINE is a cross-platform mobile messenger application with approximately 164 million monthly active users globally in 2020. The LINE service is operated by LINE Corporation, the Japanese subsidiary of South Korean internet search giant Naver Corporation. LINE can perform activities such as sending text messages, sending pictures, videos, voice messages, and making calls, reading news, and so on. LINE is claimed to be the best-selling messenger application in 42 countries [21]. LINE can be installed on iOS, Android, BlackBerry, Windows Phone, Windows PC, Mac OS X, Nokia Asha Series, and Firefox OS operating systems.

2.9 Cybercrime

Cybercrime is a crime committed by using a computer or internet network as a tool, target, and place of crime. Examples of cybercrime actions, such as child pornography, bullying, identity fraud, online fraud, illegal drug transactions, and others [22]. 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. The second category of non-violence is computer equipment that does not have a direct physical impact but provides systemic harm to a person.

2.10National Institute of Standards and Technology

National Institute of Standards and Technology is a method that has four stages in resolving and investigating cybercrime cases in the digital forensic process. The first stage is

Collection, Examination, Analysis, and Reporting.

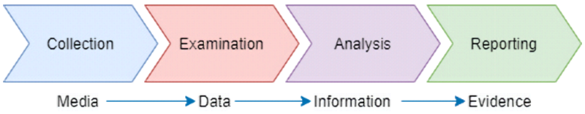


Figure 1. The Stages of NIST Method

Based on Figure 1, it can be explained that the Forensic Analysis stage is as follows:

1. Collection is labeling, identification, recording, and retrieval of data from relevant data sources according to the following procedures to maintain data integrity.
2. Examination is the processing of the data collected in the use of forensic combinations of various scenarios, either automated or manual, as well as assessing and outputting the data according to requirements while maintaining the integrity of the data.
3. Analysis is an analysis of examination results using technically justified and legal methods.
4. Reporting is reporting the results of the analysis which includes the description of the actions taken [6].

2.11Text Mining

Text mining is the application of data mining concepts and techniques to find patterns in text. According to garudacyber.co.id, the definition of text mining is the process of exploring and analyzing large amounts of unstructured data text which is assisted by the use of software that can identify concepts, patterns, topics, keywords, and other attributes in the data.

2.12Word cloud

According to technopedia.com, word cloud or also called a tag cloud is a logical arrangement of keywords in textual content that visually describes the subject of a website, blog or other text.

3. METHODOLOGY

3.1 Research Scenario

The research scenario compiled is used to carry out the forensic process on an Android-based smartphone to obtain and analyze evidence. The simulation is carried out using a smartphone as evidence for the acquisition process using forensic tools. Figure 2 shows the simulation flow of drug buying and selling transactions through LINE. The simulation begins when the buyer contacts the seller via LINE to buy drugs. The seller then sends the drug package using an expedition service. After being contacted by the seller that the package was delivered, the buyer visits and picks up the package at the courier service. Then the police arrested the suspect while taking the package and confiscated evidence in a smartphone used for drug transactions. The smartphone was forensically carried out by investigators to find all evidence of the conversation between the buyer and the suspect to be used as digital evidence. The flow of simulation can be seen in Figure 2.

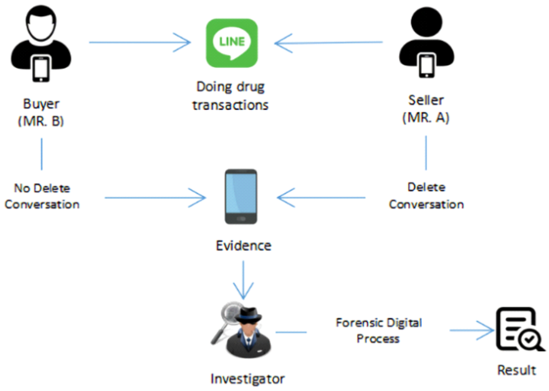


Figure 2. Flow of Case Simulation

The scenario is as follows:

a. Create a LINE account (MR. B as a buyer and MR. A as a seller).

b. MR. B adds a friend (MR. A).

c. MR. B starts a conversation to make a transaction on the M. A.

d. MR. A deleted some conversation and call history.

The scenario includes the features found on LINE that are used by the suspect to carry out and cover up transactions, including send and receive messages, send and receive images and documents, send and receive geo-locations, and delete the message and call history. Investigators will carry out forensic processes on smartphones in airplane mode to avoid adding, subtracting or modifying data.

3.2 Research Stages

The research stage is the flow to collect data or digital evidence from mobile-based LINE services needed for this research. The flow of searching for digital evidence can be seen in Figure 3.

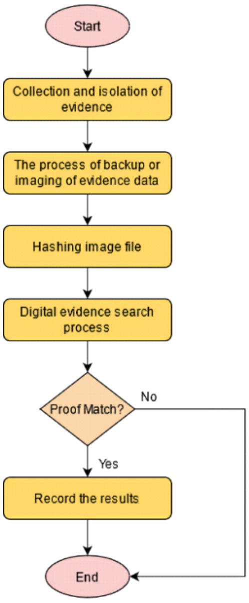

Start
Collection and isolation of evidence
The process of backup or imaging of evidence data
Hashing image file
Digital evidence search process
Proof Match?
No
Yes
Record the results
End

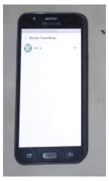
Figure 3. Flow of Search for Digital Evidence

The explanation of the flowchart in Figure 4 is the first stage of the study was carried out by collecting evidence in the form of a smartphone used to conduct transactions. The second stage is to acquire data on a smartphone to get data on the LINE application. After the data acquisition is complete, it is necessary to perform forensic imaging on the acquired data. Furthermore, the results of the duplication of data will be analyzed to obtain the necessary evidence. After getting the evidence, the investigator records the results and reports based on the results of the analysis that have been obtained in the previous stage. Department of Commerce through the National Institute of Standards and Technology provides recommendations in the process of handling electronic and/or digital evidence that can be presented in court or for individual needs at investigative institutions [23].

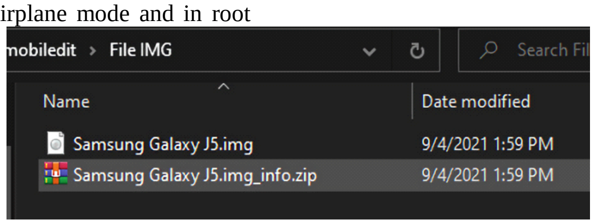
3.2.1 Collection

The collection is the first stage in the forensic process to identify sources that are considered potential to be used as evidence. The evidence that was obtained in this research scenario was an Android-based smartphone with the LINE application installed which the suspect admitted was used to buy drugs. The smartphone used by the suspect is a Samsung Galaxy J5 2015 in Figure 4 with airplane mode and in root condition and the smartphone used by the buyer is a Samsung Galaxy M21 in Figure 5 with the condition is turned on and connected to the internet as shown in Table 1.

Table 1. **Smartphone Evidence**

No.	Evidence	Image	Description
1.	MR. B's *Smartphone*	**Figure 4**. MR.B's Smartphone Evidence	Samsung Galaxy M21 is connected to the internet and not rooted
2.	MR. A's *Smartphone*	 **Figure 5**. MR.A's Smartphone Evidence	Samsung Galaxy J5 2015 in airplane mode and in root condition

The next step is to secure the evidence by conducting the smartphone isolation process by activating airplane mode to avoid data modification and rooting the smartphone by installing the SuperSU application on the smartphone using ODIN and TWRP recovery. The stage in taking digital evidence on a smartphone has a high risk so that if an error occurs, the data and information on the smartphone can be unreadable (corrupt) or lost. Therefore, to avoid this, it is necessary to carry out a backup or imaging process on a smartphone that is used as evidence, this is also called a logical acquisition [24]. The tool used to carry out the imaging process is MOBILedit Forensic Express, as shown in Figure 6.



Name	Date modified
Samsung Galaxy J5.img	9/4/2021 1:59 PM
Samsung Galaxy J5.img_info.zip	9/4/2021 1:59 PM

Figure 6. The Results of Imaging File Process

Figure 6 is the result of the imaging process on the Samsung Galaxy J5 2015 smartphone.

3.2.2 Examination

The examination is the stage where the data collection process is carried out on the LINE application installed on the suspect's smartphone related to the case of illegal drug transactions. The examination process uses three forensic tools, namely Magnet AXIOM, Autopsy, and MOBILedit Forensic Express which is displayed with the DataReader program.

3.2.2.1 MOBILedit Forensic Express

The examination process with MOBILedit Forensic Express tool can use an image file or extracting data from a smartphone directly. In this study, data acquisition on the suspect's smartphone uses an image file that has been created in the collection process. MS Excel report output format was selected for analysis using DataReader as a CMD program and word cloud visualization.

3.2.2.2 Magnet AXIOM

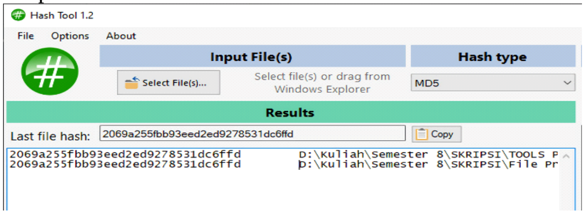
At Magnet AXIOM, investigators can retrieve data or load evidence from image files or certain files and folders or use the device directly. In this study, image file that has been created using the MOBILedit Forensic Express will be used in other forensic tools. The Magnet AXIOM forensic tool is divided into AXIOM Process and the AXIOM Examine. The AXIOM Process is used to carry out the data acquisition process in the search for evidence, while the AXIOM Examine is used to display all the results obtained from the acquisition process using the AXIOM Magnet Process.

3.2.2.3 Autopsy

The next digital evidence collection process uses a free forensic application, namely Autopsy. The acquisition process with Autopsy also uses image files from the MOBILedit Forensic Express collection process.

3.2.3 Analysis

The stage of this research is to analyze the data obtained from the acquisition results from the examination stage in each of the forensic tools used. Before performing the analysis, a copy of the backup file to be analyzed needs to be hashed to determine the similarity of the data to the original file. The hashing process uses the Hash Tool application.



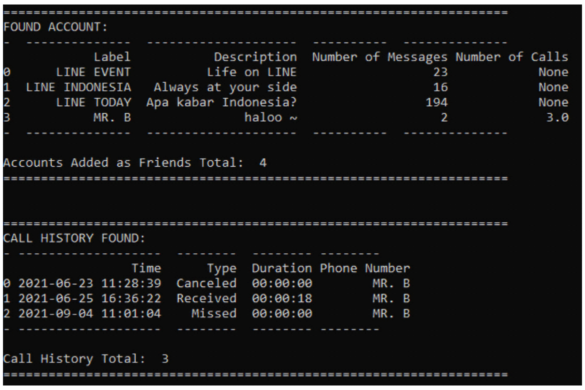
```
Last file hash: 2069a255fbb93eed2ed9278531dc6ffd

2069a255fbb93eed2ed9278531dc6ffd        D:\Kuliah\Semester 8\SKRIPSI\TOOLS P
2069a255fbb93eed2ed9278531dc6ffd        D:\Kuliah\Semester 8\SKRIPSI\File Pr
```

Figure 7. The Result of Hash Process on Excel File Report

Figure 7 shows the result of hash process file with code **2069a255fbb93eed2ed9278531dc6ffd** in both files so that it can be proven there is no data change when the file is copied to another folder.

3.2.3.1 MOBILedit and DataReader

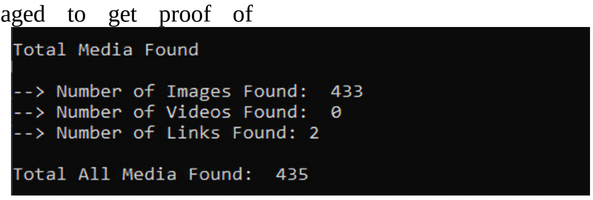
DataReader is a program made in the Python language to open and read the contents of files in Excel format obtained from the examination stage. This program can display the contents of the excel file that is input by the user. DataReader displays the LINE accounts added as friends by MR. A with call history. It's found four accounts added as friends, one of which is an MR B's account with a total of 2 messages, one call canceled, one call received, and one call miss call with MR. A as shown in Figure 8.



```
==================================================================
FOUND ACCOUNT:
-  -------------  -------------------  ---------  -------------
           Label          Description  Number of Messages Number of Calls
0     LINE EVENT         Life on LINE                 23            None
1 LINE INDONESIA  Always at your side                 16            None
2     LINE TODAY Apa kabar Indonesia?                194            None
3          MR. B              haloo ~                  2             3.0
-  -------------  -------------------  ---------  -------------

Accounts Added as Friends Total:  4
==================================================================



==================================================================
CALL HISTORY FOUND:
- ------------------  --------  -------- --------
                 Time      Type  Duration Phone Number
0 2021-06-23 11:28:39  Canceled  00:00:00        MR. B
1 2021-06-25 16:36:22  Received  00:00:18        MR. B
2 2021-09-04 11:01:04    Missed  00:00:00        MR. B
- ------------------  --------  -------- --------

Call History Total:  3
==================================================================
```

Figure 8. Proof of the Suspect's Accounts and Call History on DataReader

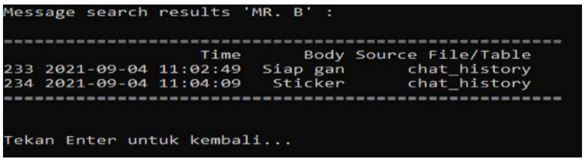
DataReader also displays media statistics with a total of 433 images found, 0 videos, and 2 geographic locations from Google Maps. DataReader managed to get proof of geolocation with a total of 2 links from Google Maps. Media statistics can be seen in Figure 9.



```
Total Media Found

--> Number of Images Found:  433
--> Number of Videos Found:  0
--> Number of Links Found: 2

Total All Media Found:  435
```

Figure 9. Proof of the Suspect's Link Geolocation on DataReader

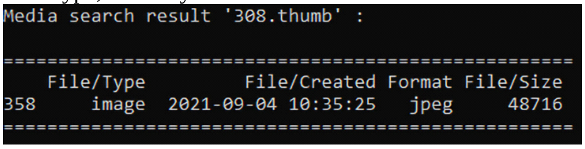
DataReader managed to find evidence of messages that were not deleted with MR. B messages by entering the name of the recipient of the message, in this experiment using the name MR. B as shown in Figure 10.



```
Message search results 'MR. B' :

==============================================================
                   Time        Body Source File/Table
233 2021-09-04 11:02:49   Siap gan        chat_history
234 2021-09-04 11:04:09    Sticker        chat_history
==============================================================


Tekan Enter untuk kembali...
```

Figure 10. Proof of the Suspect's Non-deleted Chat on DataReader

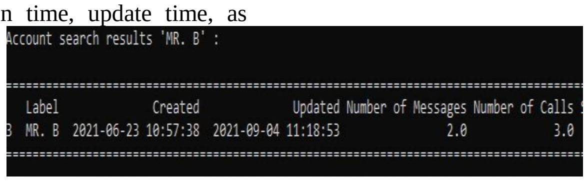
In this experiment, one of the pieces of evidence is an image of an account number with the name 308. thumb and displays the results in the form of an image file type, delivery time September 4, 2021, jpeg image file format, and file size as shown in Figure 11.



```
Media search result '308.thumb' :

================================================
    File/Type         File/Created Format File/Size
358     image  2021-09-04 10:35:25   jpeg     48716
================================================
```

Figure 11. **Proof of the Suspect Deleted Image on DataReader**

In this experiment, an account with the name MR. B display the account name, account creation time, update time, as shown in Figure 12.



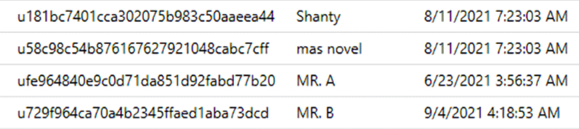
```
Account search results 'MR. B' :

=====================================================================================
  Label           Created            Updated Number of Messages Number of Calls
3  MR. B  2021-06-23 10:57:38  2021-09-04 11:18:53              2.0           3.0
=====================================================================================
```

Figure 12. Proof of the Suspect's Account on DataReader

The results of the analysis using MOBILedit displayed with the DataReader program managed to show evidence in the form of accounts and conversation texts that were not deleted, call history and photos, and geo-locations deleted by the MR.A's account.

3.2.3.2 Magnet AXIOM

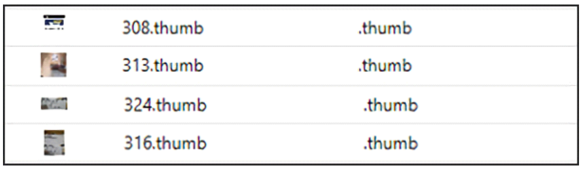
Evidence that was found from the acquisition process on the LINE application using the Magnet AXIOM application was found in the form of an account and contact MR.B with Line ID **u729f964ca70a4b2345ffaed1aba73dcd** and MR. A obtained from the naver_line database. The evidence can be seen in Figure 13.



u181bc7401cca302075b983c50aaeea44	Shanty	8/11/2021 7:23:03 AM
u58c98c54b876167627921048cabc7cff	mas novel	8/11/2021 7:23:03 AM
ufe964840e9c0d71da851d92fabd77b20	MR. A	6/23/2021 3:56:37 AM
u729f964ca70a4b2345ffaed1aba73dcd	MR. B	9/4/2021 4:18:53 AM

Figure 13. **Proof of the Suspect's Account on Magnet AXIOM**

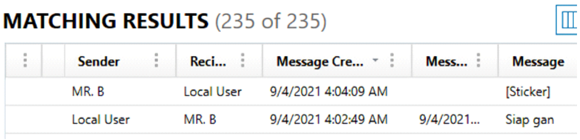
It was also found pictures deleted by the suspect such as account numbers and photos of drug content packages consisting of images **308.thumb**, **313.thumb**, **316.thumb**, and **324.thumb** which can be seen in Figure 14.



	308.thumb	.thumb
	313.thumb	.thumb
	324.thumb	.thumb
	316.thumb	.thumb

Figure 14. **Proof of the Deleted Image on Magnet AXIOM**

Magnet AXIOM also managed to get evidence in the form of chats that were not deleted. Deleted chats were not recovered successfully. The evidence can be seen in Figure 15.



MATCHING RESULTS (235 of 235)

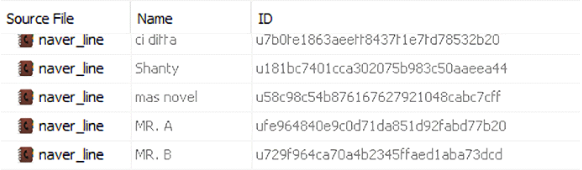
	Sender	Reci...	Message Cre...	Mess...	Message
	MR. B	Local User	9/4/2021 4:04:09 AM		[Sticker]
	Local User	MR. B	9/4/2021 4:02:49 AM	9/4/2021...	Siap gan

Figure 15. **Proof of Non-deleted Chat Magnet AXIOM**

The results of the analysis using Magnet AXIOM managed to get three digital evidences, including MR accounts. B, deleted pictures, and non-deleted chats. Chats, geo-locations, call histories, and pdf files were not recovered successfully.

3.2.3.3 Autopsy

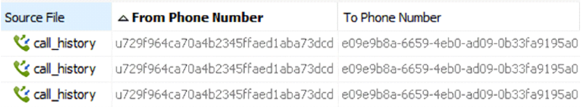
Autopsy managed to get a phone history using LINE which was intentionally deleted by the suspect. Autopsy managed to find the MR. B' account and contact with ID LINE **u729f964ca70a4b2345ffaed1aba73dcd.** The evidence can be seen in Figure 16.



Source File	Name	ID
naver_line	ci ditta	u7b0fe1863aeeff8437f1e7fd78532b20
naver_line	Shanty	u181bc7401cca302075b983c50aaeea44
naver_line	mas novel	u58c98c54b876167627921048cabc7cff
naver_line	MR. A	ufe964840e9c0d71da851d92fabd77b20
naver_line	MR. B	u729f964ca70a4b2345ffaed1aba73dcd

Figure 16. Proof of the Suspect's Account and Contact Autopsy

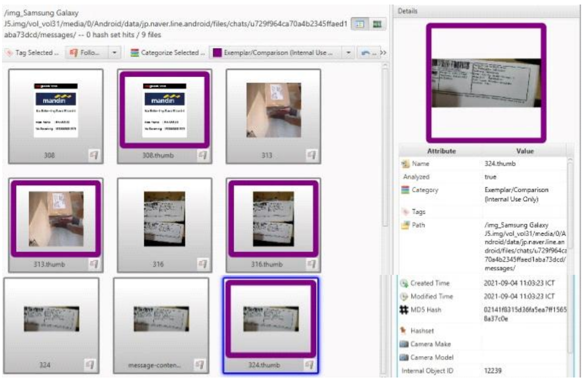
There are three call histories between MR. A and MR. B. LINE phone history. The evidence can be seen in Figure 17.



Source File	△ From Phone Number	To Phone Number
call_history	u729f964ca70a4b2345ffaed1aba73dcd	e09e9b8a-6659-4eb0-ad09-0b33fa9195a0
call_history	u729f964ca70a4b2345ffaed1aba73dcd	e09e9b8a-6659-4eb0-ad09-0b33fa9195a0
call_history	u729f964ca70a4b2345ffaed1aba73dcd	e09e9b8a-6659-4eb0-ad09-0b33fa9195a0

Figure 17. Proof of the Suspect's Call Histories Autopsy

Autopsy also managed to get the photo deleted by the suspect. There are four images with the names **308.thumb**, **313.thumb**, **316.thumb**, and **324.thumb**. The evidence can be seen in Figure 18.

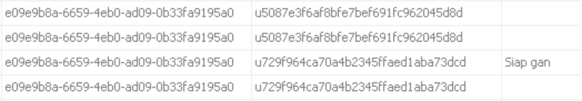


/img_Samsung Galaxy J5.img/vol_vol31/media/0/Android/data/jp.naver.line.android/files/chats/u729f964ca70a4b2345ffaed1aba73dcd/messages/ -- 0 hash set hits / 9 files

Attribute	Value
Name	324.thumb
Analyzed	true
Category	Exemplar/Comparison (Internal Use Only)
Tags	
Path	/img_Samsung Galaxy J5.img/vol_vol31/media/0/Android/data/jp.naver.line.android/files/chats/u729f964ca70a4b2345ffaed1aba73dcd/messages/
Created Time	2021-09-04 11:03:23 ICT
Modified Time	2021-09-04 11:03:23 ICT
MD5 Hash	02141f8315d36fa5ea7ff15658a37c0e
Hashset	
Camera Make	
Camera Model	
Internal Object ID	12239

Figure 18. Proof of the Deleted Image Autopsy

Autopsy also managed to get evidence in the form of chats that were not deleted. Deleted chats were not recovered successfully. The evidence can be seen in Figure 19.



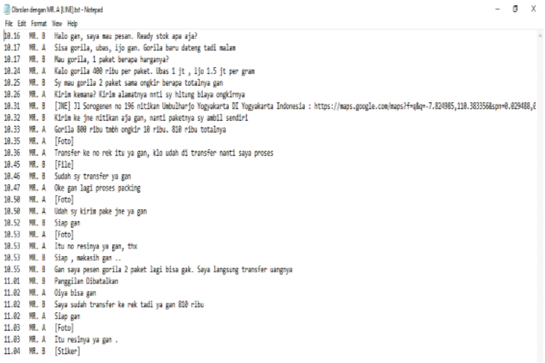
e09e9b8a-6659-4eb0-ad09-0b33fa9195a0	u5087e3f6af8bfe7bef691fc962045d8d	
e09e9b8a-6659-4eb0-ad09-0b33fa9195a0	u5087e3f6af8bfe7bef691fc962045d8d	
e09e9b8a-6659-4eb0-ad09-0b33fa9195a0	u729f964ca70a4b2345ffaed1aba73dcd	Siap gan
e09e9b8a-6659-4eb0-ad09-0b33fa9195a0	u729f964ca70a4b2345ffaed1aba73dcd	

Figure 19. Proof of the Non-deleted Chat Autopsy

The results of the analysis using Autopsy managed to get four digital evidences, including MR.B accounts and contacts, deleted pictures, call history, chats that were not deleted. Geo-locations and pdf files were not recovered successfully.

3.2.3.4 Word cloud Analysis

The conversation data between the suspect and the drug dealer will be analyzed using text mining with Python programming language on the RStudio application which functions to count the number of each word and displays a visual of the word. The next stage is pre-processing which is an important step, because this step is used to prepare data text so that it is ready for text processing [25]. The text mining stage analyzes the complete conversation obtained from the MR B's smartphone by extracting LINE chat history which generates chat files with MR. A [LINE] with .txt file format which can be seen in Figure 20.


Obrolan dengan MR. A [LINE].txt - Notepad
File Edit Format View Help

```
10.16   MR. B   Halo gan, saya mau pesan. Ready stok apa aja?
10.17   MR. A   Sisa gorila, ubas, ijo gan. Gorila baru dateng tadi malam
10.17   MR. B   Mau gorila, 1 paket berapa harganya?
10.24   MR. A   Kalo gorila 400 ribu per paket. Ubas 1 jt , ijo 1.5 jt per gram
10.25   MR. B   Sy mau gorila 2 paket sama ongkir berapa totalnya gan
10.26   MR. A   Kirim kemana? Kirim alamatnya nnti sy hitung biaya ongkirnya
10.31   MR. B   [JNE] Jl Sorogenen no 196 nitikan Umbulharjo Yogyakarta DI Yogyakarta Indonesia : https://maps.google.com/maps?f=q&q=-7.824985,110.383356&spn=0.029488,
10.32   MR. B   Kirim ke jne nitikan aja gan, nanti paketnya sy ambil sendiri
10.33   MR. A   Gorila 800 ribu tmbh ongkir 10 ribu. 810 ribu totalnya
10.35   MR. A   [Foto]
10.36   MR. A   Transfer ke no rek itu ya gan, klo udah di transfer nanti saya proses
10.45   MR. B   [File]
10.46   MR. B   Sudah sy transfer ya gan
10.47   MR. A   Oke gan lagi proses packing
10.50   MR. A   [Foto]
10.50   MR. A   Udah sy kirim pake jne ya gan
10.52   MR. B   Siap gan
10.53   MR. A   [Foto]
10.53   MR. A   Itu no resinya ya gan, thx
10.53   MR. B   Siap , makasih gan ..
10.55   MR. B   Gan saya pesen gorila 2 paket lagi bisa gak. Saya langsung transfer uangnya
11.01   MR. B   Panggilan Dibatalkan
11.02   MR. A   Oiya bisa gan
11.02   MR. B   Saya sudah transfer ke rek tadi ya gan 810 ribu
11.02   MR. A   Siap gan
11.03   MR. A   [Foto]
11.03   MR. A   Itu resinya ya gan .
11.04   MR. B   [Stiker]
```

Figure 20. **Chat Between MR.A and MR. B as the Suspect**

The results of the application of the text mining process display the number of words used in the conversation. The highest number of words include **gan (bro)**, **gorila (narcotics)**, **transfer**, and **paket (package)**. These words can be seen in Table 2.

Table 2. Word Frequency Using Text Mining

Word (Indonesian)	Word (English)	Frequency
Gan	Bro	16
Gorila	Gorilla	7
Ribu	Thousand	5
Transfer	Transfer	5
Paket	Package	4

The results of the words that have been obtained from the text mining process are then visualized in word cloud. This word cloud visualization process uses the word cloud library which displays the case in Figure 21.

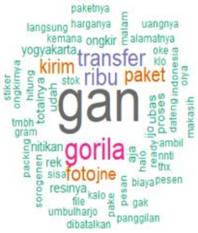


Figure 21. **Word Cloud Visualization**

3.2.4 Reporting

3.2.4.1 Comparison of Forensic Tool Results

Reporting is the stage for reporting the results of the analysis that has been carried out, including a summary of the smartphones found and a comparison of the extraction results from the forensic tools used. Information on evidence that will be reported is two units of Android-based smartphones with details of the Samsung Galaxy J5 2015 model SM-J500G with Android version 6.0.1 and the Samsung Galaxy M21 with Android version 11. The application analyzed for this research case is the LINE application installed on the Samsung Galaxy M21 smartphone with the original scenario without deleting the contents of the conversation with evidence details, such as one account, 20 conversations, 4 images, 3 call history, two geo-location, and 1 PDF file as shown in Table 3.

Table 3. The Original Evidence of Samsung Galaxy M21

Name	Evidence Obtained					
	Chat	**LINE Account**	**G-Loc**	**Call**	**PDF File**	**Img**
Total Evidence	20	2	2	3	1	4

The second evidence found was a Samsung Galaxy J5 2015 which required a mobile forensic process because the contents of the conversation were deleted by the suspect using three different forensic tools. The results of the forensic process from the three forensic tools were compared with the original evidence from the Samsung Galaxy M21 as shown in Table 4.

Table 4. Comparison of Evidence Found from Samsung Galaxy J5 2015

Digital Evidence Obtained	Forensic Tools		
	MOBILedit + DataReader	Magnet AXIOM	Autopsy
Chat	2	13	2
Deleted Chat	x	x	x
Account	2	2	2
Geolocation	2	0	0
Call history	3	0	3
Image	4	4	4
PDF File	x	x	x

Table 4 shows the differences in digital evidence obtained from forensic tools such as MOBILedit Forensics Express, Magnet AXIOM, and Autopsy. MOBILedit Forensic Express managed to get five digital pieces of evidence, Magnet AXIOM managed to get three digital pieces of evidence, and Autopsy got four digital pieces of evidence out of a total of 6 digital pieces of evidence that match the original evidence. In Magnet AXIOM, 13 chats were found but not visible, so information was given in the Chat column, not in the Deleted Chat column in Table 4.

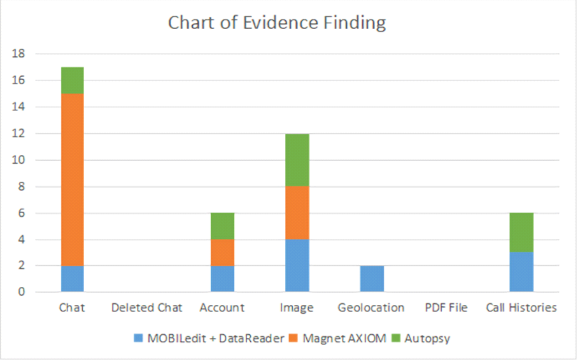


Figure 22. Chart of Digital Evidence Discovery Comparison

Based on table 4, a graph can be made as in Figure 22. This graph displays a comparison of the digital evidence obtained which shows that MOBILedit is the forensic tool that obtains the most evidence. It can be concluded that MOBILedit is a forensic tool that is recommended for use in the LINE messenger mobile application.

3.2.4.2 Word cloud Visualization Results

Based on the results of word cloud visualization using text mining in sub-chapter 2.2.3.4 of the conversation, the most frequently use words were successfullly obtained. However, the results of the analysis are still difficult to identify words related to drugs. Therefore, an R script command was made to match keywords according to case scenarios and then given different colors to make it easier to find words related to words that are often used for drug transactions between several words with these keywords as shown in Figure 23.

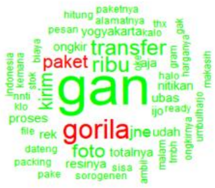


Figure 23. Word cloud Visualization Results with Keyword Match

Words in red are keywords related to narcotics and can be used to strengthen existing evidence, while words in green are words that are not related to narcotics. Word cloud also makes it easier for investigators to find words that are not commonly used in everyday conversation, for example in Figure 23 the words **ubas** and **ijo** are used for methamphetamine and marijuana drugs by narcotics traffickers in Indonesia.

4. CONCLUSION

The steps in digital forensic using the National Institute of Standards and Technology stages can be applied to the digital evidence retrieval process with the LINE application from an Android-based smartphone device. The results of the experiment show that the forensic tools MOBILedit Forensic Express and DataReader managed to obtain evidence of deleted accounts, images, geo-locations, and non deleted chat as much as 71%. Autopsy obtains evidence of deleted accounts, pictures, call history, and non deleted chats as much as 57%. AXIOM magnets get proof of deleted accounts, pictures also non-deleted chats as much as 43%. Word cloud visualization using the text mining method succeeded in identifying word matches between keywords and all conversations related to drug cases.

5. REFERENCES

[1] S. RACHMIE, “The *Role* of *Forensic Digital Science* on. *Investigating Website Hacking Cases*,” *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.

[2] E. Ramadhan and D. Mualfah, “WeChat Application Digital Evidence Investigation Using Integrated Digital Forensics Process Model (IDFPM) Framework Based on SNI 27037:2014,” vol. 4, no. June, 2021.

[3] A. Wirara, B. Hardiawan, and M. Salman, “Identification of Digital Evidence on Mobile Device Acquisition of Instant Messaging Application 'WhatsApp,'” *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020, doi: 10.20885/teknoin.vol26.iss1.art7.

[4] M. Fitriana, K. A. AR, and J. M. Marsya, “Application of the National Institute of Standards and Technology (NIST) Methods in Digital Forensic Analysis for Handling Cyber Crime,” *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.

[5] M. Riskiyadi, “Forensic Investigation of Digital Evidence In Exposing Cybercrime,” *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[6] A. Yudhana, I. Riadi, and I. Anshori, “Facebook Messenger Digital Evidence Analysis Using the NIST Method,” *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[7] I. G. N. Guna Wicaksana and I. K. Gede Suhartana, “Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method,” *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 4, p. 381, 2020, doi: 10.24843/jlk.2020.v08.i04.p03.

[8] I. Riadi, R. Umar, and M. A. Aziz, “Web Forensics Instant Messaging Service Using Association of Chief Police Officers (ACPO) Methods,” *Mob. Forensics*, vol. 1, no. 1, p. 30, 2019, doi: 10.12928/mf.v1i1.705.

[9] R. Umar and Sahiruddin, “NIST Method for Forensic Analysis of Digital Evidence on Android Devices,” *Pros. SENDU_U_2019*, pp. 978–979, 2019.

[10] S. Ikhsani and C. Hidayanto, “Forensic Analysis of Whatsapp and LINE Messenger Provides Strong and Valid Evidence in Indonesia,” *J. Tek. Its*, vol. 5, no. 2, pp. 728–736, 2016.

[11] F. Sulianta, *Forensic Computer*. Jakarta: Elex Media Komptindo, 2008.

[12] M. N. Al-Azhar, *Digital Forensic: A Practical Guide to Computer Investigation*. Jakarta: Salemba Infotek, 2012.

[13] M. S. Asyaky, “Analysis and Comparison of Digital Evidence Instant Messenger Applications On Android,” *J. Penelit. Tek. Inform.*, vol. Vol. 3 No, no. 1, pp. 220–231, 2019.

[14] T. D. Larasati and B. C. Hidayanto, “Live Forensics Analysis for Comparison of Instant Messenger Applications on Windows 10 Operating System,” *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.

[15] M. N. Faiz, R. Umar, and A. Yudhana, “Live Forensics Analysis For Comparison Of Email Security On Proprietary Operating Systems,” *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 242–247, 2016, doi: 10.33096/ilkom.v8i3.79.242-247.

[16] I. Z. Yadi and Y. N. Kunang, “Forensics On Android Platform,” *Konf. Nas. Ilmu Komput.*, pp. 141–148, 2014, [Online]. Available: ac.id/2191/.

[17] Anwar Ahmadi, I. Akbar, and H. Mandala Putra, “Comparison of Forensic Tool Results on Android Smartphone Image Files Using the NIST Method,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.

[18] H. BNN, “Understanding Drugs and the Dangers of Drugs for Health,” 2019. https://bnn.go.id/pengertian-narkoba-dan-bahaya-narkoba-bagi-kesehatan/ (accessed Jan. 02, 2021).

[19] F. Musyafi and I. Afrianto, “Building a Chat Application with a Mobile-Based Automatic Translator (Membangun Aplikasi Chatting dengan Penerjemah Otomatis Berbasis Mobile),” vol. 4, no. 2, 2015.

[20] A. Fauzan, I. Riadi, and A. Fadlil, “Digital Forensic Analysis on Line Messenger for Cybercrime Handling,” *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017, [Online]. Available: http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752.

[21] S. R. Department, “LINE - statistic & facts,” *Statista Research Department*, 2021. https://www.statista.com/topics/1999/line/ (accessed Mar. 26, 2021).

[22] M. Sobri, Emigawaty, and N. R. Damayanti, *Introduction to Information Technology - Concepts and Theories*. Yogyakarta: Penerbit Andi, 2017.

[23] M. W. Indriyanto, D. Hariyadi, and M. Habibi, “Digital Forensics Investigation and Analysis on Whatsapp Group

Chats using Nist Sp 800-86 And Support Vector Machine," vol. 3, no. 2, pp. 34–38, 2020.

[24] R. Umar, A. Yudhana, and M. Nur Faiz, "Performance Analysis of Live Forensics Methods for Random Access Memory Investigations in Proprietary Systems," *Pros. Konf. Nas. Ke- 4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhammadiyah*, pp. 207–211, 2016.

[25] R. Agrawal, "Importance of Text Data Preprocessing & Implementation in RapidMiner," no. January, 2018, doi: 10.15439/2017KM46.