# Evidence Gathering and Identification of LINE Messenger on Android Device

*By* ABDUL FADHIL

| | | | |
|---|---|---|---|
| WORD COUNT | 2994 | TIME SUBMITTED | 29-NOV-2019 02:50AM |
| | | PAPER ID | 52514418 |

# Evidence Gathering and Identification of LINE Messenger on Android Device

Imam Riadi
Department of Information Systems
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
imam.riadi@is.uad.ac.id

Abdul Fadlil
Department of Electrical Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
fadlil@mti.uad.ac.id

Ammar Fauzan
Master of Informatics Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
fauzan.ammar@gmail.com

***Abstract*—Smartphone's usage and their applications become popular in our society, nowadays. One of the most influential applications in our social life is the instant messaging application. LINE messenger is one of the popular instant messaging applications around Asian country. LINE has about 60 – 70 percent active users per month from 144 million accounts in Japan, Taiwan, Thailand, and Indonesia. Like most other instant messengers, LINE services are able to keep their user's personal files such as text chats, pictures or photos, and video. These files have the valuables and specific information about the user. In the law enforcement, this kind of information can be an authentic evidence to solve crime cases. In this paper will show the ability of a forensic tool in acquisition digital evidence on Android device. The work is separated into two tests, the application analysis acquisition, and full content acquisition. The digital evidence also has been identified, such as text chats, pictures, the name of the sender and the recipient, and the chat time (timestamp).**

***Keywords-messenger; evidence; acquisition; forensic; Android***

## I. INTRODUCTION

Android's smartphone has some interesting applications that popular in our society. One of them is the instant messaging application. It is different from SMS that only provide text message delivery. Instant messaging (IM) applications are able to deliver text messages, pictures, videos, and other files, instantly. There are many names of the instant messaging application based on Android platform. The main factors of its widespread use are because of the ease of use, fun experience, and free cost.

LINE messenger is one of instant messaging application that popular in the Asian country. Exactly 67.3 percent of the monthly active user from 144.7 million accounts in Japan, Taiwan, Thailand, and Indonesia [1]. LINE is basically point-to-point communication system between users. It supports group chat, private chat, and bot chat. Group chat and private chat are for chatting between users while the bot chat is for advertising purpose.

The widespread use of IM application also brings some problems. One of them is cybercrime, especially cyberbullying. Cyber bullying in some social network application is reach about 25 until 70 percent, while suicide victims around 55 percent [2]. Cybercrime is a serious issue nowadays. Not only bullying, fraud, stalking, and pornographic are also easier occur in IM. It also happens in some instant messaging applications like BBM, Whatsapp, and LINE messenger. According to United Nations's comprehensive study, Cybercrime is a limited number of acts against the confidentiality, integrity, and availability (CIA) of computer data or systems [3]. Figure 1 shows CIA triad that is a guide for measures in information security against cybercrime. It can be said that the information security is the main focus on cybercrime issue.

Cybercrime can be happened in any electronic devices, like Android smartphone. The crime scene in an Android device is able to solve by the investigator with some mobile forensic techniques. Mobile forensics is one of the forensic digital branches that learn on how to perform evidence recovery from a smartphone device [4] Gathering evidences and identify them is one important step to assist law enforcement.

The digital evidence gathered from Android device must be represented as much as possible. The support evidence can be expected to assist law enforcement in solving the cases of digital crimes [5]. The set of information in any Android devices is usually similar. There are Personal Information Management (PIM) applications, messaging, e-mail, and web browsing. NIST [6] mentions 17 potential evidences on the mobile device, such as date/time, text messages, photos,

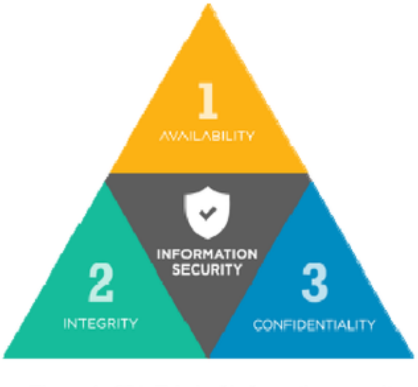


Figure 1. CIA Triad of information security

outgoing, incoming and missed call logs, instant messaging, etc.

## II. Literature Review

### A. Digital Evidence

Digital evidence is information stored or transmitted in the binary form that may be relied on in court [7]. Digital evidence is fragile, volatile and vulnerable if it is not handled properly [8]. The change of data can be influenced the result. It is necessary to keep the device in isolation mode. The purpose is to avoid any data from wiping and altering by any condition. The simple move to do this isolation is termed the airplane mode on Android device. Digital evidence can be found in hard drive, flash drive, phones, mobile devices, routers, tablets, and instruments such as GPS [9].

### B. Mobile Forensic

Mobile Forensic is a science field that studies the process of digital evidence recovery using the appropriate way from a mobile device. It is the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods [10]. Mobile Forensic is needed because mobile-based (e.g. smartphone device) services are increasing and getting more users, with the growing popularity of mobile computing and mobile commerce [8]. Mobile phone forensic analysis involves either manual or automatic extraction of data to be carried out by the mobile phone forensic examiners [11]. Analyzing digital evidence stored on a Android device is one of mobile forensic challenges in law enforcement.

### C. Acquisition and Extraction

Data acquisition from an Android device can be largely divided into the software-based method and hardware-based method [12]. The acquisition is basically a gathering evidence process in order to preserve authentic digital evidence. Extraction is the method to acquire data from the data source. The extraction method can be derived from the physical extraction and logical extraction. Physical extraction is a bit-by-bit copy of the mobile device with the maximum amount of "deleted data or files" recovered [13]. Logical extraction is a method of forensics that principally extracts allocated data from a mobile device and is typically acquired by accessing data in the file system [14].

### D. Android

Android is an open-source OS developed by the Google, based on the Linux kernel and designed primarily for touchscreen devices [15]. Android is an operating system created initially for mobile devices, such as smartphones and tablets, but nowadays it has become ubiquitous and popular in other 'smart' devices, e.g., cars, televisions, and watches. Its kernel is Linux-based, but also includes components that are not typically found in a Linux kernel. The Android operating system is a stack of software components which is roughly divided into five sections and four main layers as shown below in the architecture diagram as shown in Figure 2 [16].

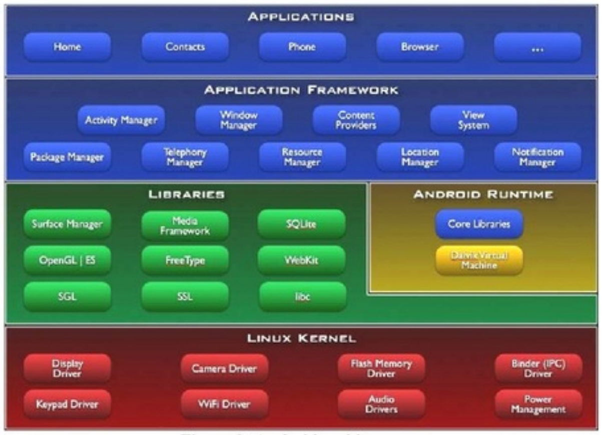


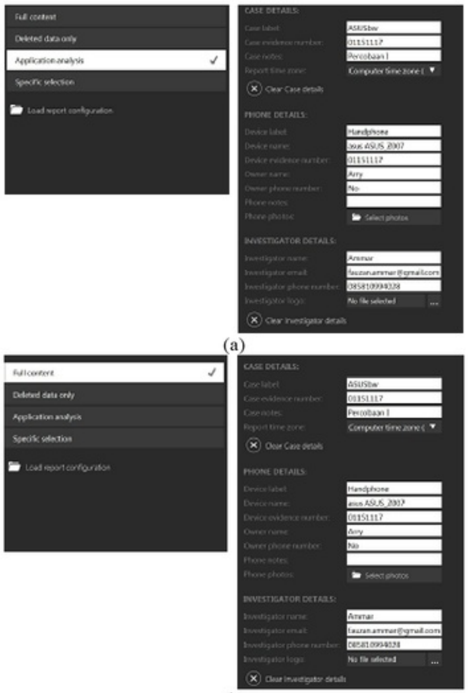
Figure 2. Android architecture

### E. LINE messenger

LINE messenger is one of IM provides their users by phone number registration. The users also can create an account in LINE by using a Facebook account. There are many features in LINE messenger, such as private chat, group chat, stickers, and hidden message. Iqbal et al. found that "Hidden messages" feature in LINE are deleted from the device and the LINE servers after the end of the set message timeout duration [17]. So, they thought this feature could be used by criminals to ensure their conversations can are still hidden.

### F. MOBILedit Forensic

MOBILedit is a forensic tool that allows investigators to logically obtain. This tool uses several connectivity



Full content
Deleted data only
Application analysis ✓
Specific selection
Load report configuration

CASE DETAILS:
Case label: ASUSbw
Case evidence number: 01151117
Case notes: Percobaan I
Report time zone: Computer time zone ( ▼
Clear Case details

PHONE DETAILS:
Device label: Handphone
Device name: asus ASUS_Z007
Device evidence number: 01151117
Owner name: Amy
Owner phone number: No
Phone notes:
Phone photos: Select photos

INVESTIGATOR DETAILS:
Investigator name: Ammar
Investigator email: fauzan.ammar@gmail.com
Investigator phone number: 085810994028
Investigator logo: No file selected ...
Clear investigator details

(a)

Full content ✓
Deleted data only
Application analysis
Specific selection
Load report configuration

CASE DETAILS:
Case label: ASUSbw
Case evidence number: 01151117
Case notes: Percobaan I
Report time zone: Computer time zone ( ▼
Clear Case details

PHONE DETAILS:
Device label: Handphone
Device name: asus ASUS_Z007
Device evidence number: 01151117
Owner name: Amy
Owner phone number: No
Phone notes:
Phone photos: Select photos

INVESTIGATOR DETAILS:
Investigator name: Ammar
Investigator email: fauzan.ammar@gmail.com
Investigator phone number: 085810994028
Investigator logo: No file selected ...
Clear investigator details

(b)

Figure 3. Screenshots of MOBILedit Forensic setting : (a)Test 1 (b)Test 2

Identify applicable sponsor/s here. *(sponsors)* mechanisms, especially wireless connectivity rather than similar tools. This software is good enough to be used to obtain phone system information and other information such as contacts and text messages. Figure 3 shows about reporting settings in MOBILedit forensic. MOBILedit forensic is one of forensic tool that has been tested by National Institute of Standards Technology (NIST). This tool can run the process of examination, reporting, and logical extraction acquisition [6].

## III. Tools and Methodology

The researchers want to acquire expected digital evidence from LINE messenger on Android device. To ensure the authenticity of the data that has been acquired, recording a hash value on the data imaging results needs to be conducted [18]. In this particular work, the forensic tool and the device are not totally representative of the real condition (cybercrime investigation). The purpose of this work is only to enrich forensic study. Some forensic tool testing might be conducted in CFTT program by NIST [19].

### A. Tools

The forensic tool in this research is the main equipment, but it must be supported by other tools to get a good result. The tools that used in this research can be seen in Table 1.

TABLE 1. Tools for forensics research

| No. | Tools | Description |
|---|---|---|
| 1. | Workstation | Asus A455L Laptop, Intel Core i3 2.0 GHz Windows OS |
| 2. | Handset / Android Device | Asus Zenfone C Z007 Android ver. 4.4.2, Rooted |
| 3. | USB Cable | USB ver. 2.0 |
| 4. | Forensic Tool | MOBILedit ver. 9.0 |

### B. Methodology

The purpose of this research is to gather digital evidence and identify them. The method is using two kinds of extraction techniques. MOBILedit has two kinds of this extraction: application analysis extraction and full content extraction. We want to analyze and identify the two different digital evidences from one forensic tool. Figure 4 show a simulation of data extraction process in the forensic tool.

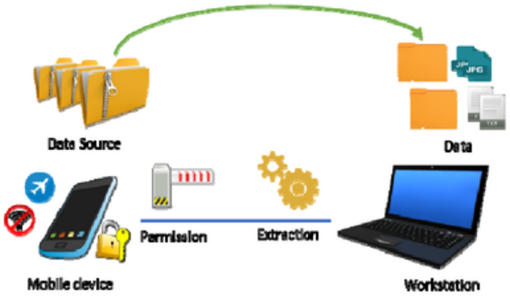


Figure 4. Data extraction process in mobile forensic

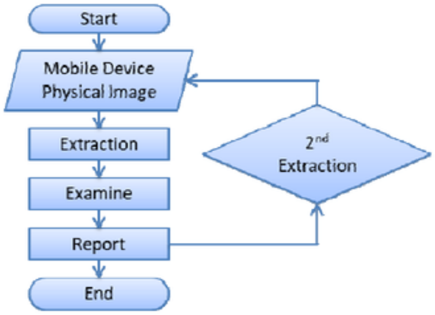


Figure 5. Research methodology

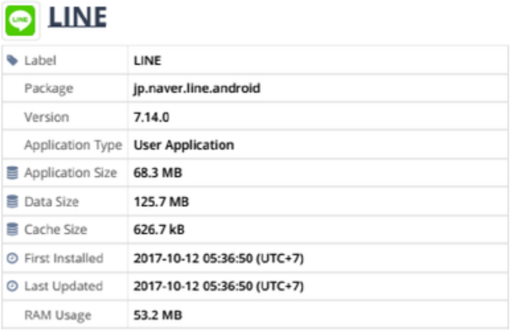
Data extraction process may take some time to complete. First extraction and second extraction processes in Figure 5 show different processing time. It proved by data extraction log. Some forensic tools come with reporting feature, so analyzing and identify process can be done by observing the report. For a better preparation, prepare working folder on separate media (hard drive) to keep evidence files and data can be recovered or extracted.

## IV. Result and Discussion

The result of the process is some potential evidence from two extraction processes: application analysis extraction (extraction I) and full content extraction (extraction II).

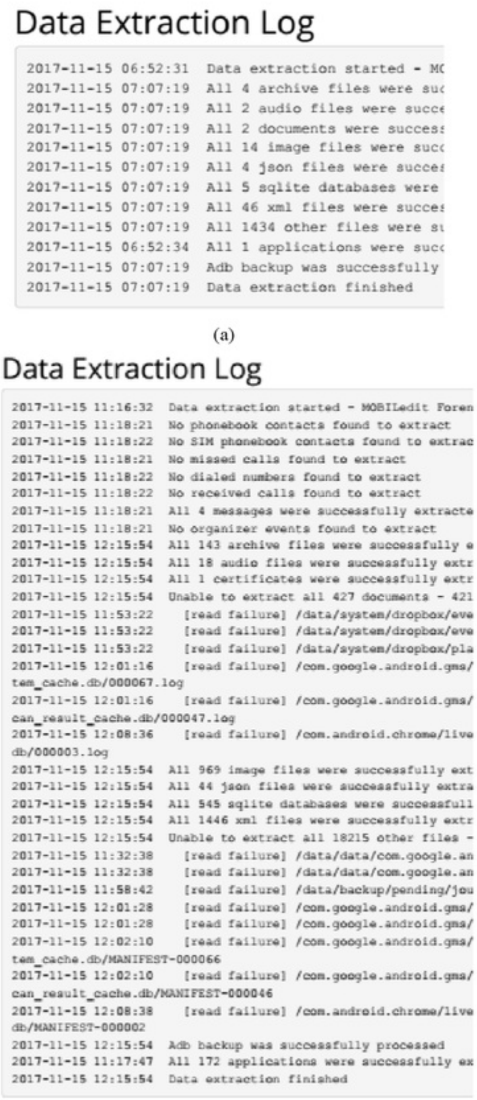
IM application that used in this research is LINE messenger version 7.14. As shown in Figure 6, LINE messenger in the mobile device has 125.7 MB data size and 626.7 kB chance size. RAM used in the extraction process on the first test (application extraction) is 53.2 MB. This RAM usage is different from the second test (full content extraction), that is 94.5 MB.

From data extraction log, it is clearly different in the duration of the process. In the first test as seen in Figure 7 (a), data extraction completed in 14 minutes 48 seconds. In the full content extraction, the process complete in 59 minutes 22 seconds as seen in Figure 7 (b). Application analysis extraction


LINE

| | |
|---|---|
| Label | LINE |
| Package | jp.naver.line.android |
| Version | 7.14.0 |
| Application Type | User Application |
| Application Size | 68.3 MB |
| Data Size | 125.7 MB |
| Cache Size | 626.7 kB |
| First Installed | 2017-10-12 05:36:50 (UTC+7) |
| Last Updated | 2017-10-12 05:36:50 (UTC+7) |
| RAM Usage | 53.2 MB |

Figure 6. LINE messenger data extraction in MOBILedit



Data Extraction Log

```
2017-11-15 06:52:31  Data extraction started - MC
2017-11-15 07:07:19  All 4 archive files were suc
2017-11-15 07:07:19  All 2 audio files were succe
2017-11-15 07:07:19  All 2 documents were success
2017-11-15 07:07:19  All 14 image files were succ
2017-11-15 07:07:19  All 4 json files were succes
2017-11-15 07:07:19  All 5 sqlite databases were
2017-11-15 07:07:19  All 46 xml files were succes
2017-11-15 07:07:19  All 1434 other files were su
2017-11-15 06:52:34  All 1 applications were succ
2017-11-15 07:07:19  Adb backup was successfully
2017-11-15 07:07:19  Data extraction finished
```

(a)

Data Extraction Log

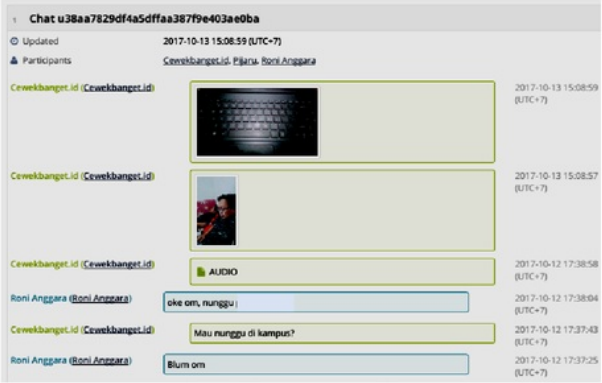
```
2017-11-15 11:16:32  Data extraction started - MOBILedit Foren
2017-11-15 11:18:21  No phonebook contacts found to extract
2017-11-15 11:18:22  No SIM phonebook contacts found to extrac
2017-11-15 11:18:21  No missed calls found to extract
2017-11-15 11:18:22  No dialed numbers found to extract
2017-11-15 11:18:22  No received calls found to extract
2017-11-15 11:18:21  All 4 messages were successfully extracte
2017-11-15 11:18:21  No organizer events found to extract
2017-11-15 12:15:54  All 143 archive files were successfully e
2017-11-15 12:15:54  All 18 audio files were successfully extr
2017-11-15 12:15:54  All 1 certificates were successfully extr
2017-11-15 12:15:54  Unable to extract all 427 documents - 421
2017-11-15 11:53:22    [read failure] /data/system/dropbox/eve
2017-11-15 11:53:22    [read failure] /data/system/dropbox/eve
2017-11-15 11:53:22    [read failure] /data/system/dropbox/pla
2017-11-15 12:01:16    [read failure] /com.google.android.gms/
tem_cache.db/000067.log
2017-11-15 12:01:16    [read failure] /com.google.android.gms/
can_result_cache.db/000047.log
2017-11-15 12:08:36    [read failure] /com.android.chrome/live
db/000003.log
2017-11-15 12:15:54  All 969 image files were successfully ext
2017-11-15 12:15:54  All 44 json files were successfully extra
2017-11-15 12:15:54  All 545 sqlite databases were successfull
2017-11-15 12:15:54  All 1446 xml files were successfully extr
2017-11-15 12:15:54  Unable to extract all 18215 other files -
2017-11-15 11:32:38    [read failure] /data/data/com.google.an
2017-11-15 11:32:38    [read failure] /data/data/com.google.an
2017-11-15 11:58:42    [read failure] /data/backup/pending/jou
2017-11-15 12:01:28    [read failure] /com.google.android.gms/
2017-11-15 12:01:28    [read failure] /com.google.android.gms/
2017-11-15 12:02:10    [read failure] /com.google.android.gms/
tem_cache.db/MANIFEST-000066
2017-11-15 12:02:10    [read failure] /com.google.android.gms/
can_result_cache.db/MANIFEST-000046
2017-11-15 12:08:38    [read failure] /com.android.chrome/live
db/MANIFEST-000002
2017-11-15 12:15:54  Adb backup was successfully processed
2017-11-15 11:17:47  All 172 applications were successfully ex
2017-11-15 12:15:54  Data extraction finished
```

(b)

Figure 7. Data extraction log from (1) first test and (2) second test.

in MOBILedit only focus on extract any files related to LINE messenger application, such as audio files, documents, image files, SQLite databases, XML files, and other files. In the second test, full content extraction completed its process with more various data, such as phonebook contact, missed calls, incoming and outgoing calls.

In this test, some potential evidence has been acquired totally. The Android device contains LINE messenger artifact such as contact, text messages, picture, audio, and timestamps. Data acquisition on this test uses physical extraction because LINE messenger's data cannot acquire in logical extraction. Rooting on the device meant that the data obtained can be maximally extracted.



Chat u38aa7829df4a5dffaa387f9e403ae0ba

Updated 2017-10-13 15:08:59 (UTC+7)

Participants Cewekbanget.id, Pijaru, Roni Anggara

Cewekbanget.id (Cewekbanget.id) 2017-10-13 15:08:59 (UTC+7)

Cewekbanget.id (Cewekbanget.id) 2017-10-13 15:08:57 (UTC+7)

Cewekbanget.id (Cewekbanget.id) AUDIO 2017-10-12 17:38:58 (UTC+7)

Roni Anggara (Roni Anggara) oke om, nunggu 2017-10-12 17:38:04 (UTC+7)

Cewekbanget.id (Cewekbanget.id) Mau nunggu di kampus? 2017-10-12 17:37:43 (UTC+7)

Roni Anggara (Roni Anggara) Blum om 2017-10-12 17:37:25 (UTC+7)

Figure 8. Text message artifact

Potential evidence obtained from both extraction tests shows the difference. Significant differences exist in the number of image and audio files. Both of these proofs may be helpful in cases of the crime requiring a transfer of images or voice mail. While the evidence in the form of text messages obtained fairly complete. However, there is less actuality in reporting the text of the conversation, the sequence or chronology of unordered text conversations as seen in Figure 8. This is according to the researchers is the weakness possessed by MOBILedit as a forensic tool.

The weakness of MOBILedit in chronological order of this text message can be seen in the picture. The disagreement in the chronology of the message text will be a problem in the trial, as it is not actual and weak in constructing arguments. Therefore, the use of other forensic tools needs to be done in order to be a benchmark and present stronger evidence in court. The result of the identification of digital evidence acquired by MOBILedit can be seen in the Table 2.

In addition to the extraction process done in MOBILedit, this tool can perform the reporting process. Reporting done by MOBILedit can be presented in several forms, namely: HTML, PDF, and Excel. While the extraction results can be changed to form Backup file, Export file, and Cellebrite UFDR (for UFED reader). This backup file can be examined repeatedly.

TABLE 2. Evidence Comparison from Data Extraction

| Evidence | Description | |
|---|---|---|
| | Extraction I | Extraction II |
| Contact Information | 83 contacts | 83 contacts with profile picture |
| Text Message | 51 messages | 51 messages |
| Photos / Images | 14 images | 969 images |
| Audio | 2 files | 18 files |
| Application's File | 1 file | 172 files |

## V. Conclusion

In this research, the better result produced by full content extraction from MOBILedit forensic tool. Although the text message and timestamp from two reports has similarity, the full content extraction process is able to show more specific data, especially in contact information evidence. Full Content extraction was able to show the profile picture of the contacts. There are various forensic tools that can be used by the examiner to acquire digital evidence. The evaluation of forensic tools can be conducted to get an overview forensic tool ability.

## VI. Future Work

After the researchers know about the ability of MOBILedit forensic to do some extraction processes, the next research about forensic tools must be done. MOBILedit report has some weakness in the data sorting. Maybe other forensic tools have more advantage then MOBILedit. We suggest evaluation of Oxygen forensic or Belkasoft can be conducted in the future work. Both of them are widely used in the mobile forensics.

## References

[1] J. T. Quigley, "Despite growing pains, Line made more than $1b in revenue last year," *techinasia.com*, 2016. [Online]. Available: https://www.techinasia.com/line-annual-revenue-2015. [Accessed: 08-May-2018].

[2] Hariani and I. Riadi, "Detection Of Cyberbullying On Social Media Using Data Mining Techniques," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 3, pp. 244–250, 2017.

[3] Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, and Unodc, "Comprehensive Study on Cybercrime," *United Nations Office on Drugs and Crime*, 2013. [Online]. Available: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. [Accessed: 05-Nov-2017].

[4] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017.

[5] I. Riadi, Sunardi;, and A. Firdonsyah, "Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 16, no. 4, pp. 198–205, 2017.

[6] R. Ayers, W. Jansen, and R. Ayers, "Guidelines on Mobile Device Forensics Guidelines on Mobile Device Forensics," *NIST Spec. Publ. 800-101*, 2014.

[7] D. J. Daniels and S. V Hart, "Forensic Examination of Digital Evidence : A Guide for Law Enforcement," *U.S. Dep. Justice Off. Justice Programs Natl. Inst. Justice Spec.*, vol. 44, no. 2, pp. 634–111, 2004.

[8] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 3, no. 5, pp. 29–36, 2017.

[9] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "International Journal of Advanced Research in Digital Forensics," vol. 7, no. 4, pp. 274–276, 2017.

[10] A. Zareen and S. Baig, "Challenges , Analysis and Tools Classification," no. May, pp. 47–55, 2010.

[11] K. Curran, A. Robinson, S. Peacocke, and S. Cassidy, "Mobile Phone Forensic Analysis," vol. 2, no. 2, 2010.

[12] Z. Li, B. Xi, and S. Wu, "Digital forensics and analysis for Android devices," in *International Conference on Computer Science & Education (ICCSE 2016)*, 2016, pp. 496–500.

[13] J. Kong, "Data Extraction on Mtk-Based Android Mobile Phone Forensics," *J. Digit. Forensics, Secur. Law*, vol. 10, no. 4, pp. 31–42, 2015.

[14] N. Y. P. Lukito, F. A. Yulianto, and E. Jadied, "Comparison of data acquisition technique using logical extraction method on Unrooted Android Device," *2016 4th Int. Conf. Inf. Commun. Technol. ICoICT 2016*, vol. 4, no. c, 2016.

[15] M. T. Ahvanooey, P. Q. Li, M. Rabbani, and A. R. Rajput, "A Survey on Smartphones Security : Software Vulnerabilities , Malware , and Attacks," vol. 8, no. 10, pp. 30–45, 2017.

[16] J. A. Shaheen, M. A. Asghar, and A. Hussain, "Android OS with its Architecture and Android Application with Dalvik Virtual Machine Review," vol. 12, no. 7, pp. 19–30, 2017.

[17] A. Iqbal, H. Alobaidli, A. Almarzooqi, and A. Jones, "LINE IM app Forensic Analysis," *12th Int. Conf. High-capacity Opt. Networks Enabling/Emerging Technol. (HONET-ICT 2015) poster*, no. IM, 2015.

[18] A. Prayogo, I. Riadi, and A. Luthfi, "Mobile Forensics Development of Mobile Banking Application using Static Forensic," *Int. J. Comput. Appl.*, vol. 160, no. 1, pp. 5–10, 2017.

[19] National Institute of Standards and Technology, "Mobile Device Tool Specification Version 2.0," 2016.

# Evidence Gathering and Identification of LINE Messenger on Android Device

ORIGINALITY REPORT

21%

SIMILARITY INDEX

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | eprints.bournemouth.ac.uk<br>Internet | 52 words — 2% |
| 2 | thesai.org<br>Internet | 44 words — 2% |
| 3 | archive.org<br>Internet | 36 words — 1% |
| 4 | www.scribd.com<br>Internet | 32 words — 1% |
| 5 | nvlpubs.nist.gov<br>Internet | 30 words — 1% |
| 6 | Imam Riadi, Sri Winiarti, Herman Yuliansyah. "Development and evaluation of android based notification system to determine patient's medicine for pharmaceutical clinic", 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), 2017<br>Crossref | 30 words — 1% |
| 7 | ijarcsse.com<br>Internet | 29 words — 1% |
| 8 | fmwn.nigona.pw<br>Internet | 27 words — 1% |
| 9 | www.ijcaonline.org<br>Internet | 25 words — 1% |

| | | |
|---|---|---|
| 10 | docplayer.net<br>Internet | 22 words — 1% |
| 11 | Milad Taleby, Qianmu Li, Mahdi Rabbani, Ahmed Raza. "A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks", International Journal of Advanced Computer Science and Applications, 2017<br>Crossref | 21 words — 1% |
| 12 | www.slideshare.net<br>Internet | 21 words — 1% |
| 13 | imamriadi.com<br>Internet | 21 words — 1% |
| 14 | www.researchgate.net<br>Internet | 19 words — 1% |
| 15 | Zhi Li, Bin Xi, Shunxiang Wu. "Digital forensics and analysis for Android devices", 2016 11th International Conference on Computer Science & Education (ICCSE), 2016<br>Crossref | 19 words — 1% |
| 16 | pdfs.semanticscholar.org<br>Internet | 16 words — 1% |
| 17 | slidelegend.com<br>Internet | 16 words — 1% |
| 18 | sm.asisonline.org<br>Internet | 15 words — 1% |
| 19 | Anton Yudhana, Sunardi, Priyatno. "Development of Door Safety Fingerprint Verification using Neural Network", Journal of Physics: Conference Series, 2019<br>Crossref | 11 words — < 1% |
| 20 | Majeed Raji, Hayden Wimmer, Rami J. Haddad. "Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools", SoutheastCon 2018, | 9 words — < 1% |

| | | |
|---|---|---|
| | 2018<br>Crossref | |
| 21 | docshare.tips<br>Internet | 8 words — < 1% |
| 22 | dione.lib.unipi.gr<br>Internet | 8 words — < 1% |
| 23 | Imam Riadi, Abdul Fadlil, Ammar Fauzan. "A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger", International Journal of Advanced Computer Science and Applications, 2018<br>Crossref | 7 words — < 1% |

| | | | |
|---|---|---|---|
| EXCLUDE QUOTES | ON | EXCLUDE MATCHES | OFF |
| EXCLUDE BIBLIOGRAPHY | ON | | |