Examination of Digital Evidence on Android-based LINE Messenger

By SUNARDI

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(3): 336-343
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

Examination of Digital Evidence on Android-based LINE Messenger

Imam Riadi[1], Sunardi[2], Ammar Fauzan[3]
[1]Department of Information System, Universitas Ahmad Dahlan
[2,3] Department of Informatics Engineering, Universitas Ahmad Dahlan
Jl. Prof. DR. Soepomo S.H., Warungboto, Umbulharjo, Kota Yogyakarta,
Daerah Istimewa Yogyakarta 55164
[1]imam.riadi@is.uad.ac.id, [2]sunardi@mti.uad.ac.id, [3]ammar1607048001@webmail.uad.ac.id

ABSTRACT

During the last decade, the number of Android smartphone users has been increased rapidly. Cybercrime is also increasing since internet was established. Instant messenger is one of internet-based application that become a new media for cybercrime. Attempts to against cybercrime can be seen from the number of forensic tools. The problem is forensic tools for mobile device available today are not completely forensically sound. Examination of digital evidence on the forensic tool is one thing offered by many vendors. However, the forensic tools have various ways of examination. This paper performed research on the examination ability of two mobile forensic tools that commonly used, Oxygen and MOBILedit, in an examination of digital evidence from LINE messenger application. Both forensic tools have its ability to examine digital evidence and can be used based on the examiner's needs. In this experiment, both forensic tools were assessed qualitatively based on a case study.

KEYWORDS

Android, forensic, digital, evidence, smartphone

1. INTRODUCTION

In September 2008, the very first Android smartphone was announced to the public although in 2007 the beta version of Android was launched internally in form of handset code-named "Sooner" [1]. Android smartphone is being popular during the last decade. The number of Android smartphones sold increased from about 220 million units in 2011 to around 1.2 billion in 2015 [2]. In 2018, Android has 13 names of version that always named by candy or dessert name.

The more Android versions the more various applications come up. One of them is instant messaging (IM) application. LINE messenger is one of IM that popular in Asian. LINE is ranked among the ten most successful mobile messenger applications in the world [2]. At the same time, LINE is the second most successful on the Asian market. Figure 1 shows the amount of monthly active LINE users worldwide in 2016. There are around 202.11 million average of LINE's active users in 4th quarter 2016.

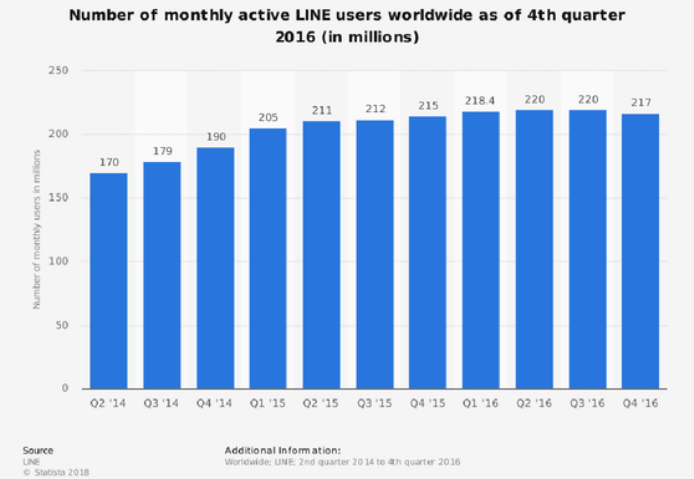

Figure 1. Number of monthly active LINE users worldwide in 2016

The widespread use of Android device makes it an inevitable source for forensic analysis both from the criminal and non-criminal point of view [3]. The widespread use of social networking applications also can increase the risk of cybercrime. One of cybercrime is being live nowadays is cyberbullying [4]. Cyberbullying is an aggressive behavior which refers to bullying behavior by a person through social media such as web, messaging, social networking, chat rooms, etc. [5]. The crime scene in an Android device is able to solve by the mobile device forensics techniques.

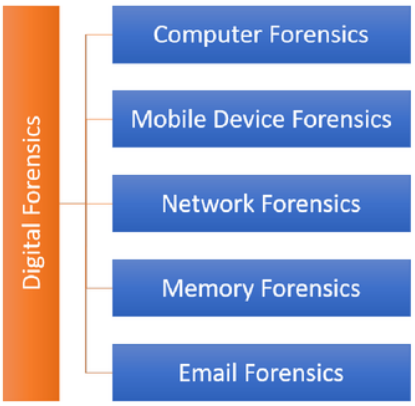

Figure 2. Branches of Digital Forensics

As seen as Figure 2, digital forensics has at least five branches of study fields. One of them is mobile device forensics. Mobile device forensics is a branch of digital forensic used for recovery of digital evidence from a mobile device.

The problem in the forensic field are many forensic tools that are not 100% as expected in their use. For this reason, NIST suggested a forensic tools testing on smartphones [6]. This also becomes a concern for the researchers. There are several research on this issue. Iqbal et. al. [7] studied the artifacts left by LINE messenger. The analysis was conducted on an iPhone running iOS6 and a HTC One Android v5. In this investigation, the text messages were successfully retrieved, but messages sent during a private messaging session were not retrieved in all scenarios. The authors use SQlite DB Browser to find database inside the mobile device.

Chang et. al [8] studied the identification of LINE's artifact. The authors focus on both the volatile memory and non-volatile memory artifacts inside a virtual machine. The author showed that this apps on volatile memory has proved that critical application data is present in the RAM and it can be extracted for further examination and analysis. The non-volatile memory analysis has shown that LINE messenger activities remain some artifacts in different locations.

Riadi, et. al. [9] studied about the technique of a forensic tools in identifying artifact in LINE messenger. The authors were able to show differences in two techniques of MOBILedit to identifying LINE's digital evidence on Android platform.

Based on the studies above and some background issues, the researchers have a reason to conduct the experiment about the ability of forensic tools in LINE's digital evidence examination. This article was focused on the analysis of MOBILedit and Oxygen forensic ability in examination process.

2. BASIC THEORY

2.1 Digital Evidence

Nowadays, mobile phones do not only transfer voice and text message, they have become a multipurpose device that can transfer multimedia files, perform video streaming, internet browsing and other operation that relates to data transfer [10]. The data transferring between electronic gadget to server leaving the digital trace, or it could be a digital evidence. Digital evidence is information stored or transmitted in the binary form that may be relied on in court [11]. It can be found in hard drive, flash drive, phones, mobile devices, routers, tablets, and instruments such as GPS [12]. Digital evidence is fragile, volatile and vulnerable if it is not handled properly [13]. Digital evidence is commonly associated with digital or electronic crime, such as pornography, prostitution, identity theft, phishing, or credit card fraud [14]. However, digital evidence is now used to prosecute all types of crimes, not just digital crimes.

2.2 Mobile Device Forensics

Mobile device forensics is a branch of digital forensics and refers to the preservation, data acquisition, examination, and analysis of mobile

devices such as cell phones, smartphones, music players, tablets, Global Positioning Systems (GPS), and other types of mobile devices [15]. Basically, it used to recover any data in the mobile device that recognized to be a digital evidence by Law. This is very useful in crime-proving in the court.

2.3 Cybercrime

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 [16]. Cybercrime can be happened in any electronic devices, like Android smartphone. Based on this understanding, cybercrime is formulated as an act against the law that is done by using a network of electronic devices as a tool or electronic device as an object, whether to gain profit or not, and there are elements harmful to others [17].

2.4 LINE Messenger

LINE is an instant messenger application launched in Japan since June 2011 [18]. LINE messenger is one of IM provides their users by phone number registration. There are many features in LINE messenger, such as private chat, group chat, stickers, etc. Despite the advantages imparted by LINE, it is vulnerable to threats. LINE IM application sends messages unencrypted over the internet [19].

2.5 Oxygen Forensic

This tool has several features which can be selected in a criminal case. Oxygen Forensic has the ability to perform logical acquisition and physical acquisition [20]. Oxygen Forensic Suite also has the capability to provide general information about the smartphone and the network that the device was connected to [14].

2.6 MOBILedit Forensic

MOBILedit is a forensic tool that has the ability to perform logical acquisition and physical acquisition like Oxygen Forensic. This software is good enough to be used to obtain phone system information and other information such as contacts, text messages, and picture. MOBILedit supports extraction and viewing data from different sources such as; Contact book, call history, text and multimedia messages, files, calendars, notes, reminders, raw application data, IMEI, operating systems, firmware including SIM details (IMSI), ICCID and location area information [3].

3 TOOLS AND METHODOLOGY

The main objective of this study is to evaluate the performance of some existing mobile forensics tools in acquiring data, from LINE messenger application, such as text, picture, audio, and video. In this section, we discuss the materials used and methods adopted for evaluation.

3.1 Tools Requirements

The materials, hardware, and software, used to achieve the objective of the study include:

Table 1. Tools requirements

Tools	Specification
Asus Zenfone C	Android 4.4.2 (KitKat), Internal 8 GB, Removable GSM/HSPA Network, Dual SIM, Rooted
LINE messenger	Ver. 6.60
Workstation	ASUS Intel Core i3 processor, RAM 4 GB, HDD 500GB, OS: Win 10
USB Cable	Ver. 2.0
Oxygen Forensics	Oxygen Forensics Ver. 6.4
MOBILedit	MOBILedit! Forensic version 9.0

This study was focused on data that could be acquired from a smartphone. The technique of extracting data is the physical acquisition. It means the smartphone must be rooted already in gaining data easier. LINE messenger is unable to extract nicely with the logical acquisition.

3.2 Research methodology

The research used the steps as in Figure 3. The steps of the research are divided into four: device

acquisition, LINE messenger examination, data analysis, and conclusion.

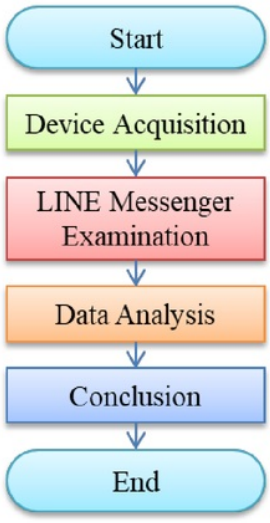

Figure 3. Research Methodology

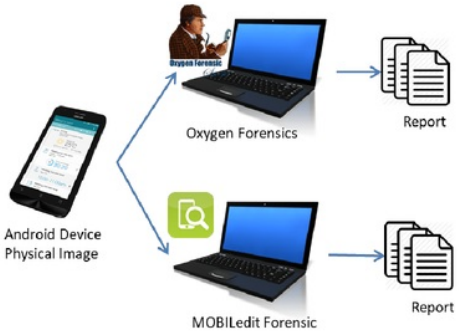

Figure 4. The Brief process of acquisition

- Device acquisition: Figure 4 shows the brief process of acquisition performed. The data from gadget was recovered and sorted in a list of each category.
- LINE Messenger examination: The researchers will perform forensic analysis on smartphone devices using the Oxygen forensics, and MOBILedit forensic. The forensic analysis will be conducted under closed conditions in the sense that smartphone devices will be converted into Airplane Mode to maintain data integrity.
- Data Analysis: The performance of each forensic tool will be analyzed using a comparison table.
- Conclusion: classifying the ability of each forensic tool.

4 RESULT AND DISCUSSION

4.1 Oxygen Forensic

Oxygen Forensic has the ability to perform logical acquisition and physical acquisition. Oxygen Forensic successfully obtains smartphone device information. Figure 5 shows LINE messenger chat text artifacts obtained using Oxygen forensic. Text message artifact from LINE messenger can be generated only from the physical acquisition. Oxygen forensic also able to perform timeline analysis that can be used by the expert to explain the conversation history from all calls, messages, calendar events, geo-data, and applications activities in a chronological way, as seen as in Figure 6. This feature is very useful for doing timeframe analysis that defined by U.S. Department of Justice (DOJ) as determining when events occurred on the system by reviewing any logs and time stamps in the file system [6].

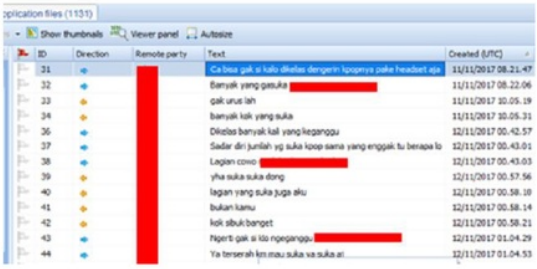

Figure 5. Chat text result from Oxygen acquisition

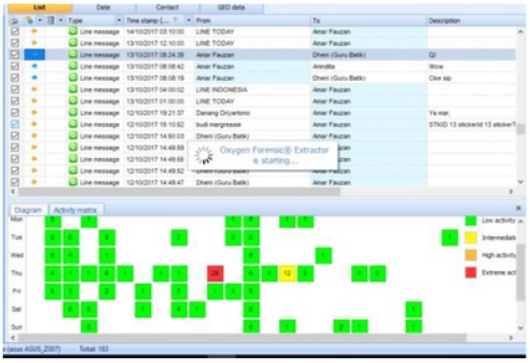

Figure 6. Timeline analysis feature in Oxygen Forensic

4.2 MOBILedit Forensic

Just like oxygen forensic, MOBILedit forensic also has the ability to perform the logical and

physical acquisition. MOBILedit Forensic successfully obtains smartphone device information. MOBILedit was able to identify the IMEI number of both mobile phones, IMSI and ICCID of the registered SIM cards.

MOBILedit was succeeded to gain contact information, text message, and picture from LINE messenger while video artifact was unable to perform in MOBILedit acquisition. The picture artifact as in Figure 7 has a brief information about the path of the file, size of the file, created and modified the file. The picture file can be a clue to investigate the production of this file.

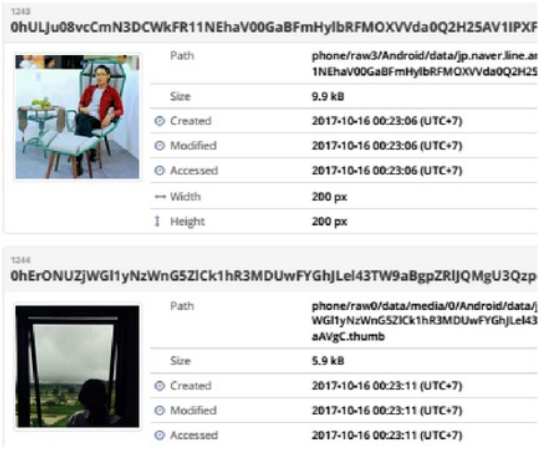

Figure 7. Image Artifact from LINE messenger

Figure 8. Text conversation in LINE Messenger

Figure 9. Deleted contact data

Figure 8 is a piece of text conversation in LINE messenger. The text conversation also shows an incoming picture and outgoing picture that occur in this section of chat. But in this text conversation, there is a problem in sorting the chronological timeline.

MOBILedit was also success to gain deleted contact data as seen as in Figure 9. This particular data can be a clue to accuse the suspect statements about the deleted contact.

Table 2. The comparison result of the forensic tools

No.	Type of file	Oxygen Forensics	MOBILedit Forensic
1	Text messages	√	√
2	Picture/photo	X	√
3	Video	X	X
4	Audio	X	X
5	Contact Information	√	√
6	Document	X	X
7	Call logs	X	X
8	Deleted data	X	√

As in Table 2, we can see the difference result from both forensic tools ability in digital evidence examination. Both of them were successful to recover text messages and contact information from LINE messenger. MOBILedit forensic seems more has advantage than Oxygen forensics in the amount of file examined. Nevertheless, Oxygen has the advantage in data analysis features, those are timeline and social graph.

5 CONCLUSION AND FUTURE WORK

Based on the forensic tool experiment in digital evidence from Android-based LINE messenger

examination that has been discussed, it can be concluded:

Oxygen forensics was good to perform timeline analysis. This is useful for the examiner in an investigation. Oxygen forensic success to gain text messages, but it failed to gain any picture or video files from LINE messenger acquisition. MOBILedit was able to gain text messages, pictures, and also deleted contact data. In the examination process, MOBILedit was failed to sorting the chronological conversation on LINE messenger. However, it still good considering there is a timestamp section in each text message.

There are a lot of forensic tools that have not been tested in a specific case as same as in LINE messenger. A future research perspective should include the analysis of different instant messaging applications by a group of different forensic tools. This analysis also needs to conduct on different mobile platforms because it can affect the result.

REFERENCES

[1] J. Callaham, "The history of Android OS: its name, origin and more," *Androidauthority.com*, 2018. [Online]. Available: https://www.androidauthority.com/history-android-os-name-789433/. [Accessed: 27-Apr-2018].

[2] Statista, "Global smartphone sales by operating system from 2009 to 2017 (in millions)," *Statista.com*, 2018. [Online]. Available: https://www.statista.com/statistics/263445/global-smartphone-sales-by-operating-system-since-2009/. [Accessed: 27-Apr-2018].

[3] N. R. Roy, A. K. Khanna, and L. Aneja, "Android phone forensic: Tools and techniques," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 2017, pp. 605–610.

[4] 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.

[5] D. Satalina, "Cyberbullying Behavior Tendency Of Extrovert And Introvert Personality Type," *J. Ilm. Psikol. Terap.*, vol. 2, no. 2, pp. 294–310, 2014.

[6] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on mobile device forensics," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014.

[7] A. Iqbal, H. Alobaidli, A. Almarzooqi, and A. Jones, "LINE IM app Forensic Analysis."

[8] M. S. Chang and C. Y. Chang, "Forensic Analysis of LINE Messenger on Android," *J. Comput.*, vol. 29, no. 1, pp. 11–20, 2018.

[9] I. Riadi, A. Fadlil, and A. Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device," *Int. J. Comput. Sci. Inf. Secur. (IJCSIS),* vol. 16, no. June, pp. 201–205, 2018.

[10] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, N. F. B. M. Sani, and F. Daryabar, "Digital forensics trends and future," *Int. J. Cyber-Security Digit. Forensics*, vol. 2, no. 2, pp. 48–76, 2014.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] G. C. Kessler, "Are mobile device examinations practiced like 'forensics'?," *Digit. Evid. Electron. Signat. Law Rev.*, vol. 12, pp. 3–9, 2015.

[16] UNODC, "Comprehensive Study on Cybercrime," Vienna, 2013.

[17] J. Clough, *Cybercrime Principles*. Cambridge: Cambridge University Press, 2010.

[18] 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.

[19] V. Jain, D. R. Sahu, and D. S. Tomar, "Evidence Gathering of Line Messenger on iPhones," *Int. J. Innov. Eng. Manag.*, vol. 4, no. 2, pp. 1–9, 2015.

[20] 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, 2017.

Examination of Digital Evidence on Android-based LINE Messenger

ORIGINALITY REPORT

12%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.mecs-press.org Internet	81 words — 3%
2	Nihar Ranjan Roy, Anshul Kanchan Khanna, Leesha Aneja. "Android phone forensic: Tools and techniques", 2016 International Conference on Computing, Communication and Automation (ICCCA), 2016 Crossref	54 words — 2%
3	commons.erau.edu Internet	42 words — 2%
4	www.dfirlabs.com Internet	26 words — 1%
5	garuda.ristekdikti.go.id Internet	23 words — 1%
6	www.statista.com Internet	21 words — 1%
7	www.ipstc.org Internet	20 words — 1%
8	cdfs.com.au Internet	13 words — 1%
9	situskabar.blogspot.com Internet	9 words — < 1%
10	ijarcsse.com	

Internet

8 words — < 1 %

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		