LINE IM app Forensic Analysis

Asif Iqbal [1], Hanan Alobaidli [2], Ahmed Almarzooqi [3], Andy Jones [4]
Athena Labs [1, 2], Zayed University [1], De Montfort University [3, 4], Edith Cowan University [4]
asif@babariqbal.com [1], andrew.jones@dmu.ac.uk [4]

***Abstract*— The Instant Messaging (IM) application is one of the most widely used communication methods in the world. It is used by a wide range of age groups and backgrounds. Its extensive use in everyday life provides unique opportunities but means that it can also be used to commit crime such as cyber bullying or by becoming a medium for criminals' communication. It can, however, also be used by forensic investigators to profile the users behavior. This makes it essential for forensics researchers to study artifacts left by such applications. This paper studies the artifacts left by one such popular application - LINE. The aim of this paper is to provide a road map for forensic investigators when dealing with LINE IM application artifacts. The artifacts are discussed in two parts: the first examines regular chatting mode and the second, private chatting.**

Keywords—Investigation; Forensics; IM; LINE; Artifacts

I. INTRODUCTION

Communication is an essential aspect of human relationship and for that reason, through the ages, technological development has taken place to facilitate it. In recent decades the evolution of computing and networking technologies have enabled computer mediated communication (CMC) tools such as email and instant messaging (IM) applications in computing devices. The latter gained its popularity and widespread usage as a result of features such as synchronous real time communication and awareness of users' presence [1]. Examples of such applications include MSN, ICQ, AOL and Yahoo Messenger. These applications have continued to evolve and were the first to migrate to the smartphone environment through the downsizing of the existing IM applications. Following that move, a number of standalone applications such as whatsApp, Tango, Viber, Blackberry Messenger and LINE were developed. The ease of use, availability, and low cost of these applications were the main factors of its wide spread use. These factors also appealed to criminals along with the ease with which they could achieve anonymity in these applications. The use of these applications by criminals can be divided into two main groups, a communication channel for real life crimes such as murders and thefts, and a medium to perform crimes such bullying, cyberstalking and phishing attacks [2] [3].

Smartphones and IM applications may hold the data that can provide evidence of the activities carried out through them through the use of digital forensics investigation methods. The use environment of the IM applications can provide evidence beyond the direct communication undertaken. This evidence can be used to profile the behavior of its user and may even allow the investigator to anticipate the users' actions along with their authorship of the communication [3] [4] [5]. One of the difficulties faced by forensics investigators in this field is the diversity of smartphones and mobile IM applications. Each device and application has its own acquisition requirements and potential sets of evidence. This research aims to provide a road map of forensics artifacts of LINE IM application.

LINE is a proprietary instant messaging application that was launched in Japan in June 2011 [6]. It was developed to on run mobile devices and evolved to cover a varied spectrum of electronic devices. To date the electronic devices that can be used to run LINE include the iPhone, Android, Windows Phone, Blackberry and Nokia smartphones, along with PCs as well as Mac computers [7] and Firefox OS [8]. Recently, in April 2015, LINE announced that its application can now also be used on Apple watches [9]. The features of this app include text/ voice chat, photo, video and location sending, video/voice calls, group chat and timeline. It also supports several languages such as English, Arabic, French, German, Indonesian, Italian, Japanese, Korean, Malay, Portuguese, Russian, Simplified Chinese, Spanish, Thai, Traditional Chinese, Turkish and Vietnamese. According to an infographic by the KRDS social media marketing company [10] in 2013, LINE was available in 193 countries with 300 Million registered users. By 2015 the number of users has doubled to over 600 Million users worldwide and is expected to reach 700 million users by the end of 2015 [11].

The aim of this research is to provide a forensic analysis of the artifacts left by the LINE instant messaging application on an Android device. A manual analysis of an image acquired from an Android device running the LINE application was undertaken. The results of this analysis yielded the file structure of the application along with the identification of its forensics artifacts.

The paper is organized as an introduction to Mobile IM and LINE IM, followed by a literature review of IM application forensics investigations. Section 3 discusses the research methodology while sections 4 and 5 discuss the acquisition and analysis of the forensics artifacts respectively. Section 6 provides the conclusions from this work.

II. LITERATURE REVIEW

Various works that have been published have targeted IM applications artifacts on smartphones, such as Tango, WhatsApp and Viber. Along with that other researchers have focused on the artifacts left by social media applications such as Twitter and Facebook. This section will discuss this research and it's identified artifacts. WhatsApp is a prominent IM

application that is very widely used and which is available on a range of different smartphones. Mahajan et al.[12] studied the forensic artifacts left by both whatsApp and Viber IM applications on an Android device. Their analysis of WhatsApp artifacts resulted on the identification of received and outgoing IM messages along with their timestamp, sent and received images with the timestamp of each action along with the sent and received videos with their respective timestamps. The artifacts recovered from the Viber IM application included Viber numbers, the total number of calls made by the user, the date and duration of call, messages to Viber users in plain text and the phone numbers to whom messages were sent. This research test environment consisted of 5 Android devices covering three versions of the Android OS which are Froyo (2.2), GingerBread (2.3.x) and Ice-Cream Sandwich (4.0.x). Anglano [13] also discussed the forensic analysis of the whatsApp instant messaging on Android smartphones. The researcher was able to reconstruct the list of contacts and the chronology of the messages that have been exchanged by users. Through the correlation of multiple artifacts, evidence inferring information such as when a specific contact has been added, as well as identifying the deleted contacts and their time of deletion can be recovered. Other inferred information included the identification of which messages have been deleted, when these messages have been exchanged, and the users that exchanged them. The Anglano [13] analysis was more detailed than in [12] and yielded more artifacts that were not found in [12].

Another IM application studied was Tango VoIP. The forensics investigation was undertaken to study Tango artifacts left on a device using iOS version 6.1.3 and an Android version 2.3.5 (Gingerbread) device [14]. On an iOS device, the Tango directory was found under the name ‘sgiggle’ instead of Tango. Several databases under the ‘sgiggle’ directory were encrypted such as ‘tc.db’ which included tables such as conversations, messages, profiles and receipts. The TangoCache.db database file under the appData file contained a list of URLs pointing at the media files (images and videos) exchanged via Tango and which are stored and available in Tango’s file servers. The information in this database file was in plain text. The same structure of artifacts was also found on the android device, with the only difference being the availability of the TCStorageManagerMediaCache location locally with the same media files identified under TangoCache.db whereas in the iOS device this folder and the identified media were not found locally on the device.

Iqbal et. al. [15] studied the artifacts left by the ChatON IM application. The analysis was conducted on an iPhone running iOS6 and a Samsung Galaxy Note running Android 4.1. The recovered artifacts on the iOS device included Information about all of the user's contacts or “buddies”, information about user’s phone contacts and records for every open chat session as well as messages within those sessions. As well as user profile information and whether the account is linked to Facebook, which can be useful for an investigation to cross reference the user behavior on both communication platforms. Similar information was found on the Android device but under a different directory and database naming structure.

Other research has focused on the artifacts left by social media applications such as Facebook and foursquare as shown in [16] and [17]. To our knowledge, no detailed analysis of LINE artifacts on Android devices has been undertaken, hence this research aims to fill the gap and provide a road map of LINE forensic artifacts.

III. METHODOLOGY

The NIST guideline states that all tools and devices used to create the test environment should be listed. Along with that it states that the process used to perform the investigation is listed as well. This section will provide details about the methodology used in the research.

A. Tools used

1- HTC One Android v5

2- SQLite DB browser

3- Windows 8.1 and Linux platforms were used for analysis

B. Scenario

In order to have a base line of the expected forensics artifacts a use case scenario needs to be stated. In this research we have created a detailed scenario of the actions undertaken using the LINE application, which was used as a road map of the expected information to be recovered. The created scenario is as follows:

1- Created account for LINE

2- Received an automated message from LINE

3- Added a new friend to the account

4- Use the text chat feature with the following messages: Hello, Hi, How are you?, fine, Testing line app for android

5- Send and receive stickers

6- Create a new group testgroup101, invite user ai to the new group, ai joined the group,

7- Voice call contact ai, duration 0:0:20, video call contact ai , duration 0:0:25

8- Share photo with contact ai

9- Send 6 sec voice message to contact ai

10- Receive voice message from contact ai

11- Shared location with contact ai

12- Post a timeline message with settings (only me)

13- Post a timeline message (line, line, line)

14- Like and comment on user ai's timeline message

15- Add an official account, Line Rewards

16- Send a hidden message, “Hidden Message”

17- Receive hidden picture, “Secret”, receive picture with text “Secret” written on piece of paper.

18- Receive hidden picture with text “Secret force close” written on a piece of paper and force close application.

The last three scenario actions were related to the “Hidden chat” feature provided by LINE which created a timeout type private message system similar to the SnapChat application. This feature takes place in a separate 1-to-1 chat room. The information that can be sent in this separate chat room is as follows; text, stickers, location info, contact info, and images. But the user is not able to send other information such as Video messages, voice messages, snap movies, albums, and notes. The company stated that the messages are sent in a secure state, and can only be viewed when the receiver taps on the sent message. The message content will only be displayed for a pre-set amount of time after which it will be deleted automatically when it exceeds the time set. Finally, after the recipient has finished viewing the hidden messages they will be deleted from the chat room as well as from the LINE servers. On the other hand, unopened messages are automatically deleted from LINE’s servers after a two week period [21, Line blog Hidden chats]. The feature can be used by suspects to ensure the confidentiality of their conversation or enables a suspect to contact victims without leaving a trace of their conversation (cyber bullying). As a result there is a need to investigate possible remnants that are left when using this feature.

C. *Acquisition*

In this stage an image of the Android device is taken, using an acquisition method similar to [18, 19 and 20] and an image of the android device was acquired. The acquisition required the preparation of a forensics workstation along with the android device. The workstation preparation included ensuring the availability of a payload that could be injected into the android device using the Android Debug Bridge (ADB). The payload was injected into a temporary location. This payload is then executed on the device in order to get a temporary root access after rebooting it. An image of the data partition was acquired using the DD utility which was included with the payload sent to the device. DD is a Unix tool that is used to create a bit by bit image of the targeted data source.

Through this process it was possible to create a physical image of the data partition that could be used to analyze the data on the Android device.

D. *Analysis*

This stage involved the analysis of the acquired image during the acquisition state. A detailed description of the acquired data found in this stage is presented in the Analysis section of the paper.

IV. ANALYSIS

This section the paper discusses the recovered artifacts based on the stated use case scenario.

There are two main locations for the recovered LINE artifacts. One contains text based artifacts while the other contains media content. All chat database and text data was recovered from “/data/data/jp.naver.line.android/”, see Figure 1. Media such as voice data and photos were recovered from “/sdcard/Android/data/jp.naver.line.android/”. It should be noted that the latter directory is accessible without the need of “rooting” the android device, and is generally known as “Main Storage” under most graphical file browsers available on

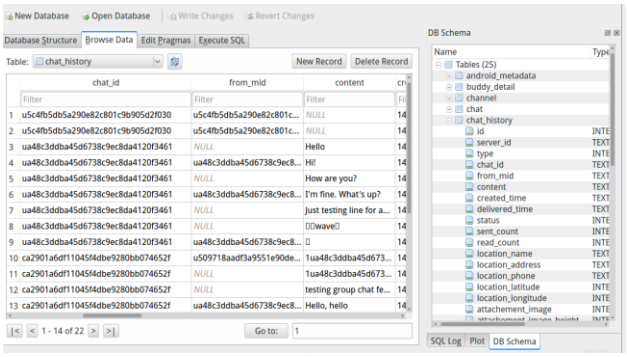

Fig. 1 Chat history information in the database

Google's Play Store.

Data from regular activities i.e. messaging and media sharing was completely recovered. While the data from private messaging feature “Hidden Message” was only partially recovered.

A. *Regular artifacts*

All the regular chat activities were successfully recovered from the above mentioned locations. The first location “/data/data/jp.naver.line.android/” contained two sub directories. The first subdirectory contained text based chat artifacts related to regular chat activities, while the other sub directory contained artifacts related to the private messaging feature of LINE, see Table 1.

TABLE I DATA RECOVERED FROM SUBDIRECTORIES OF “/DATA/DATA/JP.NAVER.LINE.ANDROID/”

Database	***Description***
databases/	This directory holds sqlite database files used by the app
naver_line.db	This file stored chat data in Sqlite 3 file database format, It's structure is discussed below
naver_line_private_chat.db	This file contains data from private messaging feature of the program called “Hidden Message” inside the app. This file and the “Hidden Message” feature are discussed in the next section.

The “naver_line.db” contained information related to regular chat activities such as contact information and chat messages see Table 2.

TABLE II STRUCTURE OF “/DATA/DATA/JP.NAVER.LINE.ANDROID/DATABASES/NAVER_LINE.DB”

Table	***Column***	***Information***
contacts	m_id	Unique identifier of each contact
	name	String that holds the full name of the contact.

	server_name	Unique username chosen by the contacts during creation of his/her account
chat	chat_id	Each chat session is stored with a unique identifier.
	from_mid	Same as m_id used in contacts table. Indicates which contact sent the message, incase of message sent by the user this field is null.
	content	If the user send or receives a text message, its contents are stored in this field. If the message sent/received is a media file, this field is NULL. In case of a video or audio call this field holds the call's duration in milliseconds. If the sent/received message is a location, the value of this field is "location".
	created_time and delivered_time	Holds timestamp of message creation and delivery time respectively
	location_name, location_address, location_latitude, location_longitude	If the message is of type location; these fields hold location data i.e. name, latitude, longitude etc. These fields are NULL for any other message type
	attachment_local_uri	If the message is an image or a video, this field holds the uri of cached media file stored on the device. These files are stored in various subdirectories of "/sdcard/Android/data/jp.naver.line.android/storage".
groups	id	Unique identifier of the chat group
	name	Name of the group as specified during creation of the group.
	creator	Id of creator of the group, NULL incase the group was created by the user.
	created_time, updated_time	Timestamps of creation and last update (last message sent) to the group.

The second main directory contained the media data sent and received during the chat session see Table 3.

TABLE III DIRECTORY CONTAING THE MEDIA DATA OF A CHAT SESSION

Directory	***Description***
temp	Temporarily holds media files received in chat session.
storage/mo/{chat_id}/	chat_id is unique chat identifier as stored in the database. This directory holds all the media files transferred during the chat session. Photos are stored in JPEG encoded files, while the audio is stored in acc format.

B. "Hidden Message" Artifacts

Based on the scenario implemented, not all hidden messages were recovered during this investigation. There were no artifacts left in the "naver_line_private_chat.db" sub directory when this feature was used normally, as the messages are deleted after the end of the set message timeout duration. That being said there were some artifacts recovered when the application was force closed before the timeout duration is over. See Fig 2, see Table 4. It must be noted that recovery of these artifacts does not require root access on the device as these were stored in an area accessible to regular users; which renders the private messaging feature useless.

TABLE IV SUBDIRECTORY CONTAINING THE MEDIA DATA SENT DURING A PRIVATE CHAT SESSION

Directory	***Description***
storage/mo/{chat_id}+private/	chat_id is a unique chat identifier as stored in the database. This directory holds all the photos transferred during the "Hidden Message" private messaging session. The photos are stored in JPEG format.

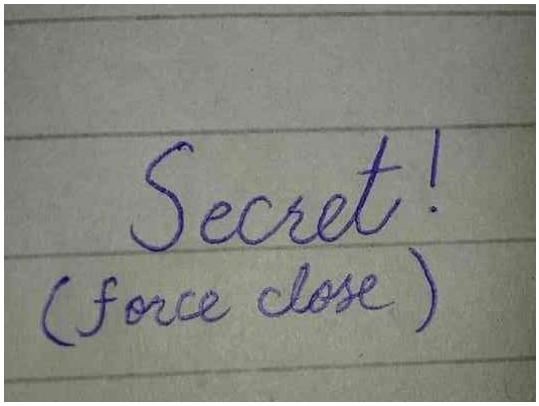

Fig. 2 Recovered image sent during a private chat session, the application was foreclosed before the end of the timeout duration

V. CONCLUSION AND FUTURE WORK

The market for instant messaging applications is evolving rapidly. Applications such as WhatsApp, BBM messenger, Skype and LINE are some of the commonly used applications. With the tremendous use of such applications in people's daily life, it may be used to commit crimes or fall into a scenario where identifying the forensic artifacts left by these application is important to identify and prove the actions undertaken. In this paper we have discussed the artifacts that are left by the LINE instant messaging application, both the regular messaging artifacts and private messaging artifacts. In this investigation, the regular chat messages were successfully retrieved, but messages sent during a private messaging session were not retrieved in all scenarios. According to the description of the "Hidden messages" feature in LINE these messages are deleted from the device and the LINE servers after the end of the set message timeout duration. As a result, this feature could be used by criminals to ensure the confidentiality of their conversations. However, there are scenarios where artifacts of these conversations can be found on the device. In this investigation, artifacts sent using this feature were recovered when the application was force closed before the end of the set timeout.

Private messaging is being introduced into Instant messaging applications such as BBM messenger in order to attract a new user base, but these features can be used by criminals or used in actions such as cyber bullying. As these messages are designed to be deleted after being seen it would be difficult to prove that they were sent in the first place. A future research perspective should include the analysis of different private messaging artifacts left by a group of different instant messaging applications. This analysis also needs to be undertaken on

different mobile platforms, as a change of the platform can affect the location and availability of the artifacts.

REFERENCES

[1] To, P. L., Liao, C., Chiang, J. C., Shih, M. L., Chang, C. Y. March (2008). An empirical investigation of the factors affecting the adoption of Instant Messaging in organizations. In: Computer Standards & Interfaces, vol. 30, issue 3, pp. 148-156

[2] Horsman, G., & Conniss, L. R. (2015). An investigation of anonymous and spoof SMS resources used for the purposes of cyberstalking. Digital Investigation, 13, 80-93.

[3] Orebaugh, A., Allnutt, J. (2010) Data Mining Instant Messaging Communications to Perform Author Identification for Cybercrime Investigations, In Book: Digital Forensics and Cyber Crime, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 99-110

[4] Iqbal, A., Al Obaidli, H., Marrington, A., & Jones, A. (2014). Windows Surface RT tablet forensics. Digital Investigation, 11, S87-S93.

[5] The United Nations Office on Drugs and Crime. Comprehensive study on Cybercrime. Technical Report. United Nations; (2013). Available at http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[6] LINE, About (2015) Retrieved on August, 4th 2015, from http://linecorp.com/en/company/info

[7] LINE, Retrieved on August, 4th 2015, from http://line.me/en-US/

[8] FireFox, LINE, Retrieved on August, 4th 2015, from https://marketplace.firefox.com/app/line

[9] LINE, LINE for Apple Watch is Here! Take LINE with You Wherever You Go (2015) Retrieved on August, 4th 2015, from http://official-blog.line.me/en/archives/1025254803.html

[10] Digital Strategy Consulting, Top 10 instant messaging apps in the world (infographic), (2013) Retrieved on August, 4th 2015, from http://www.digitalstrategyconsulting.com/intelligence/2013/12/top_10_instant_messaging_apps_in_the_world_infographic.php

[11] Bahk Eun-ji, Number of Line users to top 700 mil. this year, Koreatimes, (2015) Retrieved on August, 4th 2015 from http://www.koreatimes.co.kr/www/news/tech/2015/02/419_173201.html

[12] Mahajan, A., Dahiya, M. S., Sanghvi, H. P. April (2013) Forensic Analysis of Instant Messenger Applications on Android Devices. In: International Journal of Computer Applications, vol. 68, No.8

[13] Anglano, C. September (2014) Forensic analysis of WhatsApp Messenger on Android smartphones, Digital Investigation, Volume 11, Issue 3, Pages 201-213, ISSN 1742-2876

[14] Le-Khac, N., Sgaras, C., Kechadi, M. (2014) Forensic Acquisition and Analysis of Tango VoIP, International Conference on Challenges in IT, Engineering and Technology (ICCIET 2014), Phuket, Thailand

[15] Iqbal, Asif, Andrew Marrington, and Ibrahim Baggili. "Forensic artifacts of the ChatON Instant Messaging application." Systematic Approaches to Digital Forensic Engineering (SADFE), 2013 Eighth International Workshop on. IEEE, 2013.

[16] Levinson, A.; Stackpole, B.; Johnson, D. (2011) Third Party Application Forensics on Apple Mobile Devices, System Sciences (HICSS), 2011 44th Hawaii International Conference on , vol., no., pp.1,9, 4-7

[17] Tso Y-C, Wang S-J, Huang C-T, Wang W-J. iphone social networking for evidence investigations using itunes forensics. In: Proceedings of the 6th international conference on ubiquitous information management and communication. ICUIMC'12. ACM; 2012. p. 1–7 [Article 62]

[18] Lessard J, Kessler GC.: Android forensics: simplifying cell phone examinations. In: Small Scale Digital Device Forensics Journal, vol. 4, No. 1, September (2010)

[19] Iqbal, B., Iqbal, A., Guimaraes, M., Khan, K., & Al Obaidli, H. (2012, October). Amazon Kindle Fire from a Digital Forensics Perspective. In 2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (pp. 323-329). IEEE.

[20] Iqbal, A., Alobaidli, H., Marrington, A., & Baggili, I. (2014). Amazon Kindle Fire HD Forensics. In Digital Forensics and Cyber Crime (pp. 39-50). Springer International Publishing.

[21] LINE, New "Hidden Chat" Feature Released, Enables Sending of Time-Limited Messages, (2014) Retrieved on August, 4th 2015 from http://official-blog.line.me/en/archives/1006361166.html