Evidence Gathering of Line Messenger on iPhones

Article · July 2015

CITATION
1

READS
1,036

3 authors, including:

Vineeta Jain
Malaviya National Institute of Technology Jaipur
9 PUBLICATIONS **23** CITATIONS

SEE PROFILE

Evidence Gathering of Line Messenger on iPhones

Vineeta Jain, Divya Rish Sahu, Deepak Singh Tomar

Department of Computer Science, Maulana Azad National Institute of Technology, Bhopal (M P), India
Email: vineetajain.jecrc@gmail.com, divyarishi.sahu@manit.ac.in, deepaktomar@manit.ac.in

Abstract: The contemporary Smartphone has built-in Instant Messaging (IM) applications like Whatsapp, Line, etc, which facilitates users to send and receive chat messages, video, audio and images via Smartphone in real time. Apart from benefits offered by Instant Messaging (IM), it also suffers from few vulnerabilities which provide ground for attackers to launch attacks such as Man-in-the-middle attack (MITM). These applications leave traces and Evidences in phone. In order to identify crimes, it is essentially required to retrieve these traces and evidences by using appropriate forensic technique. The works carried out in this field deals with forensic analysis of Whatsapp, viber, ChatOn etc but not with forensic analysis of Line messenger, even though number of users of Line messenger is more than 500 million. In this work, evidence subjected to Line messenger has been extracted from iPhone running ios 6. This paper presents evidence gathering of Line IM application which proves beneficial for forensic analysts and practitioners as it assists them in course of mapping and locating digital evidences of Line messenger on iPhone.

***Keywords*:** Instant Messaging, Mobile Instant Messaging, Evidence Gathering, Forensic Models, Logs

Accepted On: 29.07.2015

1. Introduction

Decades back, the source of communication existing between humans has been letters, telegram, wireless radio, SMS etc. With the arrival of ICQ, a brand new approach of text-based online communication using laptops or PC known as instant messaging, emerged and developed promptly. The popularity of IM hiked with the launch of other IM such as AOL, Yahoo messenger, MSN messenger etc. In 2009, with the introduction of Whatsapp, a wave of technology known as Mobile instant Messaging (MIM) which is defined as the proficiency to use instant messaging application on Smartphone engulfed the existing technologies. Later, in 2010 and 2011 many MIM applications surfaced as well such as Line, Viber, WeChat, Kakao Talk etc.

In 2014, McKinsey and Company analyzed that the use of mobile instant messaging has increased from 5% to 85% [1]. Driven by the reducing cost and handiness of mobile data plans, along with the ease they provide to users, the use of MIM's has became widespread. All that glitters is not gold so is the case with MIM applications. They are misused to perform cyber crime activities such as tampering, phishing, threatening, identity fraud etc.

This paper explores the forensic evidences of Line messenger which is one of the most prominent and skill fully devised instant messaging application for IOS, android, tablet and desktop users. Line introduced in 2011 by Naver Corporation in South Korea [2]. It has over 560 million registered users [3]. It is recognized as being a "Fast and Light" messenger that is considered as the "The Number 1 Free App" in many countries, especially in South East Asia [2]. Despite the advantages imparted by LINE, it is vulnerable to threats. LINE IM application sends messages unencrypted over the internet. It makes LINE vulnerable to attacks such as Man-in-the-middle attack [4], eavesdropping, etc, which may lead to loss of confidential information such as login credentials, location coordinate etc. The results can be catastrophic.

This work attempts to examine the evidences of Line messenger stored in internal memory of iPhone. The logs and database of Line have been extracted from iPhone. Database entries are further preprocessed and studied to scrutinize attributes and determine forensically relevant evidences.

2. Related Work

The major requirement of a successful forensic analysis is its model. A forensic analyst need to incorporate an appropriate model based on the scenario. Therefore, applying feasible forensic model in a scenario has always been a concern of researchers and analysts.

2.1 Forensic Analysis Models

The first forensic model has been proposed by Politt [5]. This work is based on the use of computer forensics to exploit stored digital information. It includes four steps namely- Acquisition, Identification, Evaluation and Admission, of evidences.

McKemmish [6] proposed a forensic model that focuses on Identification, Preservation, Analysis and presentation of digital evidences. In addition to steps, McKemmish model specifies four rules of computing namely- minimal handling of original, account for any change, comply with rules of evidence and not to exceed our knowledge on the subject. Electronic evidence satisfies all the four rules as – image of evidences is created and then analyzed; original evidences are not used and tampered; the evidences which are potentially harmful are only considered as evidences; evidences cannot be generated.

In order to make forensic process more effective by providing clear definitions and complete terminology, Palmer [7] proposed a forensic model in 2001 during the first Digital Forensic Research Workshop (DFRWS). The model may be applied to majority of forensic investigations concerning digital systems and networks. It comprises of seven phases- Identification, Preservation, Collection, Examination, Analysis, Presentation and Decision. Researchers considered it as a combination of Pollit and McKemmish model.

In order to make a model which is independent of particular technology or electronic crime, Carr, Grunch and Reith [8] proposed an extension of Palmer model. This model incorporates both non-digital and electronic technologies within the abstraction. It includes nine steps namely- Identification, Preparation, approach, Preservation, Collection, Examination, Analysis, Presentation and Returning evidences. It excludes decision phase.

Spafford and Carrier [9] suggested an entirely different forensic model which groups investigation phases in two groups namely- physical and digital. In addition to digital evidences, it also considers non-digital evidences which are collected by physically monitoring the crime scene.

Shahzad et. al., [10] proposed an extension to Reith's abstract digital forensics model [8]. In order to maintain integrity of evidences, this model considered preservation of evidences as an umbrella activity. The steps involved in proposed model include - preparation and planning, collection, examination, analysis, reporting, presentation, archiving and returning evidence.

The introduction of new models is motivated due to the future scope uncovered by already existing models.

- Pollitt model marked the beginning of use of digital evidences for investigation purpose. The model only talks about identification of evidences. The analysis of identified evidences is left for future work.
- In order to remove the deficiency of Pollitt model, McKemmish proposed a model which included analysis phase. But the analysis phase is improperly defined as it does not say anything about examination of evidences.
- In order to remove drawback of McKemmish model arrived Palmer model which is a combination of both the Pollitt and McKemmish models. But it contains duplication as the preparation and approach strategy are taking similar things in account and preparation phase is entirely dependent on strategy.
- In the existing models, physical investigation aspect has not been considered. This phase has been taken in account in Carrier and Spafford model. But the deployment phase of this model is ambiguous as it is concerned with confirmation of evidence which is not possible before analysis.
- One of the important aspects of forensic process is preservation of evidences during the entire process as a little bit of tampering may give modified results. Keeping this point in mind, Shahzad et al proposed a model that considered preservation phase as an umbrella activity.

The field of forensics is growing unabated and analysts are coming up with new models by removing the drawbacks of already existing models and taking into account every minor detail that need to be considered during an investigation.

2.2 Forensic Analysis of IM Applications

Forensic analysis of instant messaging applications have been a focus of many researchers as they are exposed to threats like man in the middle attack, sniffing, hijacking, etc,

which leads to loss of sensitive information like usernames, passwords, credit card details, etc.

Mahajan et. al., [11] performed forensic analysis of whatsapp and viber on 5 android phones using two ways namely- by using UFED (Universal Forensic Extraction Device) and manual analysis. It has been observed that the number of artifacts captured by manual analysis is more than the artifacts captured by UFED. In Whatsapp, UFED extracts information only about sent and received messages, timestamps and profile pictures of Whatsapp contacts. Whereas, by manual analysis, it has been found that Whatsapp stores information in two databases containing two tables each. In viber, no artifact has been extracted by UFED. Whereas, in manual analysis it has been found that viber logs are saved in two separate files namely- Viber_data and Viber_messages.

Cosimo Anglano [12] carried out Whatsapp forensics on Android in 2014 using YouWave virtualization platform which is used to imitate the behavior of android. In addition to examining the attributes of Whatsapp database individually, the artifacts are linked together to obtain inferences. The important information obtained by linking attributes includes- Information regarding addition or deletion of contact in whatsapp from the database of contacts; confirmation of delivery of a message to its destination; identifying whether the user joined or left the group before or after a specific time; determining the timestamp when a given user has been added to the list of contacts, etc.

Asif et. al., [13] examined the artifacts of Samsung ChatOn application on IPhone and android phones in 2013. In iPhone, ChatOn database is stored in file ChatOnClientApp.sqlite and seven tables from the database have been analyzed to find evidences. In android, ChatOn.db file stores the database of ChatOn. In android also, seven tables have been analyzed to identify evidences.

Yang et al [14] observed the likelihood of identifying Viber communication content via the Random Access Memory (RAM) in Android devices. It has been deduced that in addition to retrieving partial evidence via the RAM, there is also a possibility of presence of evidences after resetting the device.

3. Methodology

The objective of this study is to gather evidences of Line messenger from iPhone by extracting database and logs and studying the attributes of database. The methodology used for evidence gathering of Line messenger is shown in Figure 1.

4. Tools and Technology

The process of evidence gathering has been performed on iPhone 4 with ios version 6.1.4. iTunes has been used to synchronize data, applications, and media files between iPhone4 and the host computer. UFED Physical Analyzer has been used to browse the application data and files saved in the memory of iPhone4. SQLite database browser has been used to create, design and edit SQLite database files

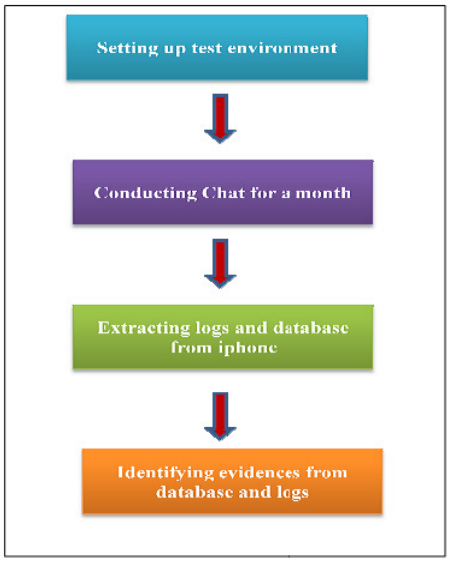

Fig 1: Methodology used for evidence gathering

5. Implementation and Analysis

The methodology explained in section 4 is applied on iPhone 4 to extract database and identify evidences by exploring the attributes

5.1 Set up Test Environment

In order to identify evidences of Line messenger, a test environment has been established, which contained 2 iPhones having ios version 6.1.4 with Line messenger installed on both of them. 2 accounts on Line messenger have been created. It is to be noted that both the iPhones are not jailbroken (rooted). The reason is that, even if the device is jailbroked, numbers of evidences acquired are either same to the case of jailbroked device or less than that due to autonomous

environment. The test environment is shown in Fig. 2.

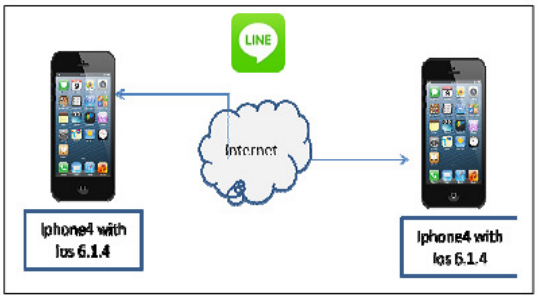

Fig. 2. Test environment

5.2 Conducting Chat for a month

In order to scrutinize attributes correctly, database with large number of entries is required. To get a large database, chatting is conducted between the 2 iPhones used in set up environment, for about a month and all the features of Line messenger have been used while chatting such as voice and video calls, sending and receiving multimedia content, downloading in-built applications of Line messenger etc. So that no value of any attribute is missed during analysis. Snapshot of two phones during chatting is shown in Fig. 3.

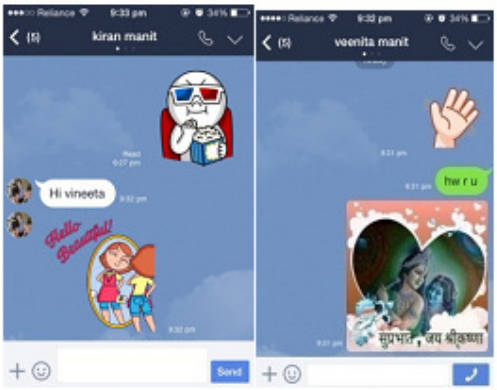

Fig. 3. Snapshots of chat performed between 2 iPhones using 2 accounts on Line messenger

5.3 Extracting Logs and Database

Initially, iTunes has been installed on the computer followed by installation of UFED Physical analyser. IPhone is connected to the computer by using USB cable. iTunes syncs the device with the computer and then device is identified by UFED analyser in which the entire file system of the device is visible. The logs of Line messenger have been extracted from location:

Extraction Summary/Installed Applications/Chats.

At this location, the log of all the applications installed is available from which relevant logs have been scrutinized for evidence gathering. Database of Line messenger stored in file "talk.sqlite" has been extracted from location:

Extraction Summary/Installed Applications/ Chats/Databases/Cookies/

The file is copied and pasted in the system for studying the values of every attribute and identifying evidences that are crucial for any forensic investigation. Snapshot of logs of all the applications when viewed in UFED analyser is shown in Fig. 4. A tuple in Log file of installed applications shows details of an activity performed using an application.

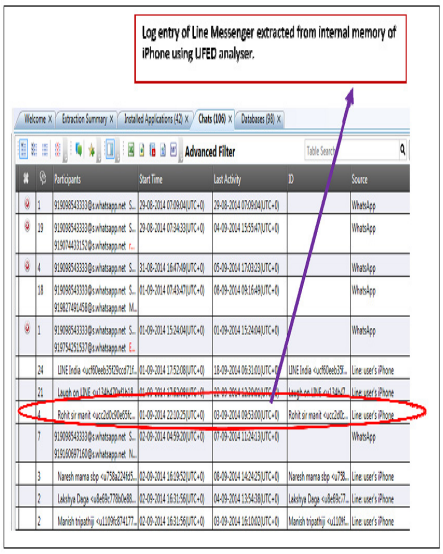

Fig. 4: Snapshot of Logs of all applications installed on device

The highlighted log entry is the entry of Line messenger of among all the extracted logs from iPhone. The first column of Log entry shows the number of messages exchanged during the conversation. The participant attribute signifies the partner with who chat has been done. The name is followed by an alphanumeric value which is a unique ID provided by Line server to all its users. The attribute start time shows timestamp value of when the conversation has begun and attributes Last activity shows the timestamp of when the conversation has finished. The source shows the application which has been used for conducting chat. Here, source is Line user's iPhone. The database view of file "talk.sqlite" in UFED physical analyser is shown in Fig. 5.

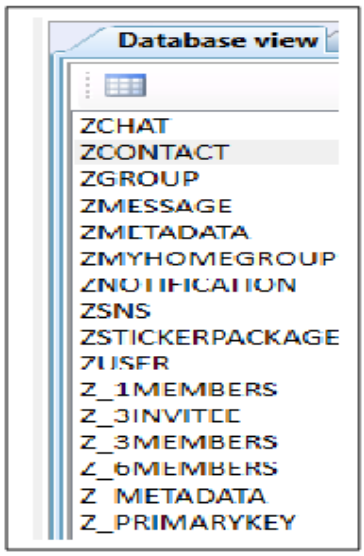

Fig 5. Database view of file "talk.sqlite"

5.4 Identifying Evidences

The database extracted from the device contained 16 tables. Out of 16 tables, 5 tables have been identified forensically relevant because in remaining tables all the attributes either do not contain any value such as ZSNS, ZNOTIFICATION etc, or do not provide any relevant information for any crime investigation such as ZSTICKERSPAGE (which contains information about sticker packages) etc or contains redundant information such as Z_3MEMBERS (stores information about partners of chat which is already present in ZMESSAGE table), etc. The list of relevant tables of database used for forensic investigation in this research is shown in Table 1.

Table 1. Forensically Relevant Tables in Line Messenger Database

Table No.	Table	Content
1	ZCONTACT	Information about all contacts in address book of user
2	ZUSER	Information about all contacts using Line in address book
3	ZCHAT	Carries information about number of chats done by user
4	ZMESSAGE	Information about all the messages exchanged through Line
5	ZGROUP	Information about groups user is a member of

Database of Line messenger stores many types of information about user (such as information about contacts stored in device, information about exchanged messages etc.) through its attributes in tables. The importance of every attribute of all the forensically relevant tables has been evaluated to identify whether they can act as evidence during a forensic analysis or not. Some attributes has been identified as potential evidences as they deliver crucial information for analysis whereas some attributes have no worth for an analysis process. The next section describes the evidences and their importance for forensic analysis process.

5.4.1 Contact Information

In case of a crime, contact information may have evidentiary value as it enables forensic analyst to determine the details of Line account of the person with whom user has been in contact with. 2 tables have been extracted from "talk.sqlite" database file - ZCONTACT and ZUSER, which stores the information of the users.

1. ZCONTACT: ZCONTACT stores information about all contacts in address book of Smartphone, irrespective of whether they are line users or not. 16 attributes have been extracted from it out of which 4 attributes has been identified as evidences as the remaining attributes do not offer any significant information for forensic process such as ZSORTABLENAME (it contains names of contacts in lowercase which is also present in ZNAME attribute), ZPHONENUMBER (carries phone number of contact which is also stored in ZKEY attribute), etc. .

When a contact is added in address book, its timestamp value is stored in an attribute named ZCREATEDATA which may be used in building chain of evidences. Contacts are uniquely identified by their phone numbers. ZKEY attribute stores phone numbers which are unique and not null thus provides unique identification to users. ZMID attribute contains a unique alphanumeric value e.g. u8783b61241a34d818113df139bdd9406, provided by Line servers for those contacts which are Line users. This field is only assigned to users of Line from all contacts. It is used as reference for creating correlation between attributes of different tables. ZNAME attribute stores the name of contact which is used to identify with whom user has been contact with. The list of attributes of ZCONTACT table that are forensically investigated in this paper is shown in Table 2.

Table 2. Attributes of ZCONTACT table

Attribute name	Description
ZCREATED AT	Contains Timestamp of when the contact has been added in address book of phone
ZKEY	Contains phone number
ZMID	Contains Alphanumeric value for contacts which are Line users
ZNAME	Carries Name of the contact

2. ZUSER: ZUSER contains information about contacts having Line accounts. 34 attributes has been unraveled out of which 4 has been considered as evidence because rest do not impart useful information for an investigation such as ZADDRESSBOOKNAME (it contains name of contact as in address book of phone which is similar to ZNAME), etc.

Each record stores the profile name (attribute ZNAME) which is used for identification purposes in case of a crime. ZISUNREGISTERED attribute is used to classify users as currently registered and unregistered users. If the user is not currently registered on line, the field contains value '1', else '0'. It is useful to determine fraud messages through classifying actual users. ZPROFILEIMAGE attribute carries the profile picture and ZPICTUREURL attribute contains the URL of the picture. Profile pictures if set by the users in Line account are also stored in the database. Profile pictures may act as crucial evidence in case of crime. It helps to identify a person, for example, if profile pictures shows face of the Line user or location or any item which possibly can be uniquely associated with that user, it may be used to identify the person.

Line messenger allows the user to block anyone from contacts, i.e. no communication can be performed with blocked user till the block is removed. From the investigation point of view it can be crucial to determine whether a contact was blocked or not at a given time, in order to confirm that a message sent by a contact is actually received by the user at that time. It is crucial for fake message detection

ZBLOCKING field in ZUSER table contains value 1 if a user blocks a line contact, otherwise, 0. There is no information to tell whether the user of the device under analysis has been blocked or not by anyone of his/her contacts.

The list of forensically relevant attributes of ZUSER is shown in Table 3.

Table 3: Attributes of ZUSER table

Attribute name	Description
ZISREMOVED	If the contact has been removed from user's friend list in Line, it carries value=1, else value=0
ZISUNREGISTERED	If the contact has been using Line but currently is unregistered , it carries value=1, else value=0
ZNAME	Carries name of the contact stored on Line server
ZPICTUREURL	Contains URL of profile picture

5.4.2 Information About Exchanged Messages

The messages between users can be evidence from forensic point of view. It is even possible to reconstruct the entire chat history in order to find traces of the crime being committed. 2 tables have been extracted from database of Line messenger that stores chat information: ZCHAT and ZMESSAGE.

1. ZCHAT: ZCHAT conveys information about number of chats done by a user storing one record per chat. 17 attributes have been extracted from which 2 attributes have been obtained as evidences for any forensic investigation as the rest stores obsolete information for forensic experts such as ZINPUTEXT (it do not contain values), ZINVITERMID (it is also empty), etc.

The chats are uniquely identified by Z_PK attribute that is used in reconstructing the chat history in case of a crime. The messages exchanged during chats are stored in table ZMESSAGE. Z_PK attribute acts as a reference for ZMESSAGE table in determining relation between message and chat. ZUNREAD attribute stores an integer value depicting the number of unread messages in a specific chat. It is used to identify delivery status of a message during an investigation. ZMID attribute is used to identify partners of a chat in a forensic inspection. The attributes of ZCHAT table that are important from forensics point of view is shown in Table 4.

Table 4. Attributes of ZCHAT Table

Attribute name	
ZUNREAD	Contains number of unread messages in a specific chat
ZMID	Contains unique Alphanumeric value given by Line server to contacts

2. ZMESSAGE: This table contains all the sent and received messages transmitted between sender and receiver. 16 attributes have been extracted from which 11 attributes have been regarded as evidences because the remaining attributes do not provide any substantial information for an inspection such as ZMESSAGETYPE (it is empty), etc.

Every message has a unique ID stored in ZID attribute which provides unique identification to every message. ZSENDER attribute contains the ID of the sender. The ZID attribute is associated with Z_PK attribute of ZUSER table, from where details of sender can be retrieved which is displayed in Fig. 6.

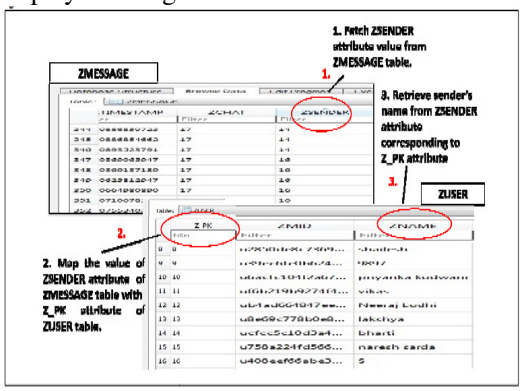

Fig. 6. Retrieving the name of sender of messages using ZMESSAGE and ZUSER tables

Chronology of messages is built through ZTEXT and ZTIMESTAMP attributes. ZTEXT attribute contains the contents of the message exchanged. ZTIMESTAMP carries the timestamp of every message sent or received.

Line messenger allows user to send geographical coordinates of present location using GPS or Wi-Fi. The latitude and longitude values of the location are stored in ZLATITUDE and ZLONGITUDE attributes respectively which are used to determine the location of the sender.

ZTHUMBNAIL attribute contains the information such as size of the file, about media files being sent and received. Media files may contain hidden information and can act as potential evidence from forensics point of view.

ZREADCOUNT attribute specifies status of sent message. If message has been read it carries value=1, else value=0. ZSENDSTATUS attribute stores information regarding delivery of a message to its destination. If the message has been delivered successfully it contains value=1, else value=0. These two attributes are used in determining the state of a message during a investigation. The attribute of ZMESSAGE table that are forensically important is shown in Table 5.

Table 5. Attributes of ZMESSAGE Table

Attribute name	Description
ZREADCOUNT	If the received message is read by the user it contains value=1, else value=0
ZSENDSTATUS	If the message sent has been delivered contains value =1, else value=0
ZTIMESTAMP	Contains timestamp of when message has been sent or received
ZCHAT	Specifies which message belongs to which chat
ZSENDER	Carries information about sender
ZLATITUDE	Contains latitude values of location sent and received
ZLONGITUDE	Contains longitude values of location sent and received
ZID	Contains Unique ID of every message
ZTEXT	Stores message content
ZTHUMBNAIL	Contains images exchanged

5.4.3 Analyzing Group Information

Group information of Line messenger is obtained by extracting ZGROUP table. This table is analyzed to verify membership of user during a suspicious message transmission.

1. ZGROUP: It contains information about groups, user is a member of. 12 attributes have been extracted from which 4 attributes have been contemplated as evidences because of the insignificant information contained by them from forensics point of view.

Each group is provided a unique alphanumeric ID by Line server stored in ZID attribute. ZCREATEDTIME contains the time user has been added to the group which is used to identify whether the user has been member of a group during a crime or not. If the user has not accepted the invitation to join the group, ZISACCEPTED attribute contains value=0, else value=1. It is used to confirm membership of user in a group. ZNAME attribute contains name of the group which is used for identification purposes during a crime. The attributes of ZGROUP table which have been forensically analyzed in this paper is shown in Table 6.

Group messages includes message of every member involved in the group at the time of group chat and stored in database. It does not store information about number of members involved during a group chat. However, it can be

calculated by keeping track of control messages that are generated automatically when a member leaves or joins a group. Control messages are stored in ZMESSAGE table as a record with timestamp. So, whether a member has been present during a group or not can be determined.

Table 6. Attributes of ZGROUP

Attribute name	Description
ZISACCEPTED	If the user has accepted the request to join group, it contains value=1, else value=0
ZCREATEDTIME	Time when the group has been created
ZID	Contains Unique alphanumeric ID of the group assigned by Line server
ZNAME	Contains Name of the group

5.4.4 Scenario

In this section it has been explained how attributes present in database of Line messenger may be used to identify evidences during a forensic investigation

Suppose there are 2 users Alex and Bob, doing chat using Line messenger on iPhone. Alex threatens Bob by sending some objectionable content. Bob reports it to Police. The Police seize the phones of Alex and Bob to investigate about the messages. Forensic experts extracts database of Line messenger from both the iPhones and observe entries of ZUSER (to confirm identity of user), ZCHAT (to confirm that whether chat has been done between both the users or not) and ZMESSAGE (to confirm the text of messages exchanged) tables of both the phones to confirm the crime. It is important to extract information from both the phones as Alex may have entered false entries in database of his phone. In this way, crime is proved by extracting evidences from Line messenger. The complete scenario is shown in Figure 7.

Fig 7. Scenario where evidences extracted from iPhones has been used to prove a crime

6. Conclusion

The most popular feature of Smartphone in present time is IM application. But the use and misuse of these applications go hand in hand. This paper focuses on Evidence Gathering of Line IM application on iPhones. In this work, extraction of attributes stored by the database of Line messenger has been explored. Cellebrite UFED tool has been used for database extraction and by exploring every attribute of the database, evidences has been gathered such as timestamps and senders of sent and received messages in plaintext, which can prove very fruitful for forensic analysts and experts at the time of forensic investigation. Logs that are generated by Line messenger are extracted which may aid practitioners to develop chronology of events happened during a conversation. As Line messenger is a multi platform IM application, so Evidence Gathering of Line IM application on other platforms has been left for future work.

References:

[1] N. Y. City, Messaging Apps : The New Face of Social Media and What It Means For Brands Messaging Apps : The New Face of Social Media, 2014. http://ipglab.com/wp-content/uploads/2014/04/MessagingApps_Whitepaper_Final.pdf.

[2] Esen Sagynov, The Story behind LINE App Development!. Blog in curbid, dev platform category http://www.cubrid.org/blog/dev-platform/the-story-behind-line-app-development/ , 2011.

[3] Statista, Number of LINE app's registered users from December 2011 to October 2014 (in millions), 2015.

[4] Don Sambandaraksa, LINE vulnerable to man-in-the-middle attack :, 2013.

[5] M. M. Pollitt, Computer Forensics: An Approach to Evidence in Cyberspace, in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp. 487-491, 1995.

[6] McKemmish, R.: What is Forensic Computing? Canberra Australian Institute of Criminology ,1999.

[7] G. Palmer, DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research, Digital Forensics Workshop (DFRWS), Utica, New York, 2001.

[8] M. Reith, C. Carr & G. Gunsh, An Examination of Digital Forensics Models, International Journal of Digital Evidence, Vol. 1, No. 3, 2002.

[9] B. Carrier & E. H. Spafford, Getting Physical with the Digital Investigation Process, International Journal of Digital Evidence, Vol. 2, No. 2, 2003.

[10] Saleem, S., Popov, O., & Bagilli, I., Extended Abstract Digital Forensics Model with 2PasU. Procedia Computer Science, 35, 812–821, 2014.

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

[12] Anglano C., Forensic analysis of WhatsApp Messenger on Android smartphones. In: Proceeding of the 14th Annual DFRWS Conference, 2014.

[13] A. Iqbal, A. Marrington, and I. Baggili, Forensic artifacts of the ChatON instant messaging application, In 8th International Workshop on Systematic Approaches to Digital Forensic Engineering, Hong Kong, Nov. 2013.

[14] H. Chu, S. Yang, S. Wang, and J. Park, The Partial Digital Evidence Disclosure in Respect to the Instant Messaging Embedded in Viber Application Regarding an Android Smart Phone, In Proceedings of the 4th FTRA International Conference on Information Technology Convergence and Services (ITCS-12), pp. 171–178, 2012.