National College of Ireland

NETWORK TRAFFIC BASED ANALYSIS OF SECURE COMMUNICATION APPLICATION (LINE)

MSc Internship
Cyber Security

Padmaja Sekher
Student ID: X17135885

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name	:	Padmaja Sekher
Student ID	:	X17135885
Programme	:	Cyber Security **Year:** 2019
Module	:	Internship
Supervisor	:	Imran Khan
Submission Due Date	:	12/12/2019
Project Title:		Network Traffic based Analysis of Secure Communication Application (LINE)
Word Count:		……………………………………… **Page Count**…………………………………………….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	

Penalty Applied (if applicable):	

Network Traffic based Analysis of Secure Communication Application (Line)

Padmaja Sekher
X17135885

Abstract

The expanded utilization of social media has an effect in everyday life exercises. Because of the expanded use of texting applications, individuals' correspondences are changed in a totally extraordinary way. As the worry for individual's security began to expand, the application suppliers began to build their applications with protection highlights. These overhauls empower the individuals to convey in a safe way thus does the lawbreakers. Despite the fact that the exchanging the messages are being encoded, breaking down the system traffic of those correspondences can uncover a few intriguing data. In this paper, the protected system traffic of secure texting application LINE was investigated and the discoveries of data about included text message, voice/video call, client exercises and different examples about the application's use were introduced. [13]. These curios can be utilized in criminal examination in the realm of cybercrime and furnish the agent with data about the application client and their exercises.

.

1 Introduction

The cell phones have become irreplaceable part of the human life. Nearly everybody has one cell phone. With the progression of web, individuals began to discuss through the web. Some social media administrations and their texting applications give individuals numerous selections of correspondences from messages, voice calls to video calls. With the data privacy aspects among the clients has been increased, the secure information of an application turns into its one of a kind selling point. Numerous application suppliers began to give end to end encryption and this makes the entrance to access the content by an outsider troublesome. These protected highlights additionally began to pull in offenders. The criminal investigations are getting intricate if these protected applications are being encoded by encryption it's very difficult to analysis the data content from the encrypted network traffic. Henceforth the forensic network began to consider and investigate these secure applications which has encrypted connection and attempting to discover measurable artefacts that are left by those applications. The investigation of secure applications are of two sorts. One is breaking down the artefacts left by the applications on the host gadget for example smartphones. Second is examining the artefacts that can be found in their network traffic. The network traffic can be investigated for security vulnerabilities in the conventions utilized by the applications and for designs that are distinguished which can be utilized to extricate data about the clients and their exercises or following up the activities in the application around the world. In this paper, I have presented the detailed analysis of the network traffic behavior of the secure communication application (LINE) messaging application which has end to end encryption technique. Therefore, presented the findings of the data information regarding the application users and the involved parties. Hence, discussed about how the end to end encryption application leaves the artefacts in the system by analysis the network traffic between the involved parties. LINE is one of the widespread messaging applications in the world. It has more than 500 million users downloading this application in the play store and has a user count more than 700 million users in the worldwide. Line has a cross platform support and generally underpins around six stages like an android, IOS, BlackBerry, Firefox OS, Windows and mac OS. It is likewise one of the few messaging applications which rely on end to end encryption technique. With this sort of huge client base, the need to profile the client exercises or activities is significant, since the data contents can't be accessed by the third party which is ended to end encrypted by encryption techniques. The discoveries introduced in this paper will help the examiners who are exploring the cases which includes the utilization of the LINE delegate by lawbreakers/targets/criminals. All the more accurately, the commitments of this paper can be condensed as pursues:

- Analysis of the network traffic of LINE messaging application with the protected correspondence is examined for different client exercises or activities and their specific unique signatures are analyzed.
- Network traffic analysis is done for various operation system platforms have been discussed and profiling for client exercises/ user activities with unique signature is done.

The remaining of the paper is sorted out as pursues: In segment related works, inspecting of related existing work is detailed. In area Research methodology, the devices and the approach utilized for the examination is talked about. At this point, in specification segment it explained about the framework for analysis of LINE secure traffic is done. In section implementation, the analysis of LINE network traffic is analyzed in different platforms.

2 Related Work

Most of the popular instant messaging applications like WhatsApp, Telegram, Viber, LINE etc., have started to provide end-to-end encryption. The increase in the usage of these secure instant messaging apps made the forensic community to focus much on the artefacts or traces left by those secure apps. Many researchers worked on the artefacts that can be retrieved from the host smartphones which are left by the usage of those applications. Fazeel Ali Awan (2015) [1] and F. Norouzizadeh Dezfoul et al (2016) [2] explained the forensic artefacts that can be retrieved from the smartphones where the applications were used. They used the database files present in the image of the smartphone and retrieved the contacts, call history and duration etc. But the network artefacts that are left by those secure apps are being studied sparsely. Before the end-to-end encryption features, the traffic can be intercepted. Khulood Ali Al Zaabi (2016) [3] had showed the possible man-in- the-middle attack on LinkedIn applications and artefacts left by the application in the host device. But the applications are becoming secure day by day. And also, if the host device is not available for examination or the scenario of investigating the potential suspects without spooking them, we need a procedure to find the artefacts that are being left those suspects activities. For that, the analysis of network traffic of those instant messaging applications is important. Daniel Walnycky et al. (2015) [4] showed the deep analysis of both the device storage and net- work artefacts of 20 popular instant messaging applications. But they were focused on the net- work artefacts that were available unencrypted. They discarded the encrypted traffic. M.A.K. Sudozai et al. (2017) explored the secure traffic of instant messaging application Viber [5]. Viber is one of the applications which is providing end-to- end encryption. They identified the ports which were used by the Viber servers and separated the Viber traffic from the whole traffic. They used payload sizes to determine the user activities and voice/video calls. Another one of the most popular instant messaging application is WhatsApp. It has more than

1 billion users across the globe. This wide scale of user base shows the importance of the artefacts that can be extracted regarding this application. F. Karpisek et al. (2015) [6] decrypted the WhatsApp encrypted traffic using pidgin plugin. They decrypted many valuable information like WhatsApp phone numbers, phone call metadata like duration, timestamp and WhatsApp voice codec. Fu- Ching Tsai et al. (2018) [7] explored the net- work artefacts of WhatsApp traces. They found the end parties of a WhatsApp call using Wire- shark. They proposed the voice calls follow STUN protocol and filtered and analyzed those packets to find end parties IP addresses. Instead of analyzing the packets and their patterns, Machine learning techniques were also used to extract information about those secure apps. Zhenlong Yuan et al. (2014) [8] explored the net- work artefacts of skype using sequence signatures of the packets and infer information using ma- chine learning techniques. Scott E. Coull and Kevin P. Dyer (2014) [9] analyzed the encrypted iMessage service and used machine learning techniques to infer information about the underlying operating systems and the language used. Nikunj Malik et al (2017) [10] explored the ICMP pings to the smartphones and used the inter packet space of the traffic to profile the operating system of the device. M.A.K.Sudozai et al. (2018) [11] proposed a framework for profiling the secure apps from the encrypted traffic. They proposed to identify the ports used by the servers and their IP ranges using a firewall and analyze the behavior of the network traffic for various user activities. It was proposed as a common framework and can be applied to any secure instant messaging applications.

3 Research Methodology

This section citates about the various tools which are used to helps to analysis the result and discussed about the methodology used to obtain the results. Line is one of the messaging applications which serves many facilities to the user such as texting, voice call, video call ,emojis and sharing the contact information and location accuracy. This application also provides end to end encryption in the aspects of data privacy of the users. In addition, an overview of LINE’s encryption protocols is explained in this paper. According to this survey, LINE is using a specific method called Letter Sealing method to encrypt the messages and VoIP services. These services enable end to end protocol. LINE works on ECDH (Elliptic Curve Diffie - Hellman) for over curve 25519 for key exchange. Encryption is done using Advanced Encryption Standard (AES) -256 in CBC mode and hashing the values are done by SHA-256 algorithm for hashed values. For the LINE's messaging application VoIP encryption protocol, the curve uses are secp256rl. The main purpose of this is to convert RTP to SRTP sessions [20]. LINE provides text messages, video/voice call, location accuracy, file sharing and much more features added on to this application. These provided end to end services to the user. In order to identify the user activities using the application can be identified by following the TCP and UDP flows, byte patterns, and payload sizes of the pattern. For analyzing the large amount of network traffic, samples were collected. Wire- shark is used for analyzing the network traffic. Device used were Lenovo idea-pad 33OS which runs with windows 10 with the processor Intel i5-8250U. The devices and the Line version used in the study was discussed below.

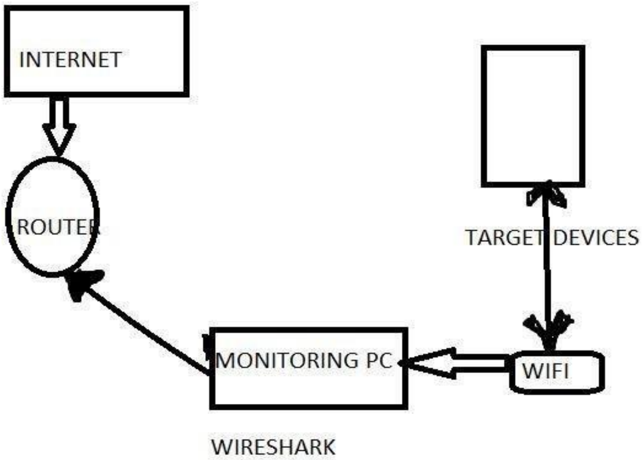

Figure 1 Environmental setup

For this study, the environmental lab setup is shown in the **Figure 1**. Wire-shark is used to analyze the network traffic. To monitor the network traffic we use monitoring device as Lenovo idea-pad 33OS in which it has an internet access. The mobile hotspot in the monitoring device is connected to the target mobile devices. The target mobile devices are installed with the LINE messaging application. The background process is blocked. The user activities are profiled, and the network traffic analysis is done by wire-shark is examined for the study.

4 Design Specification

This area includes the broad forensic examination done on the secure LINE traffic on the different platforms including android, windows, mac OS, iOS gadgets. The analysis is based on the signature like byte patterns and payload sizes of the packets in the network traffic. The specific signatures were found based on the corresponding user activities like voice/video calling, text messages, file sharing, emojis, contact information, profile information and location based accuracy.

These analyses can be done on various platforms and the findings are evaluated.

4.1 Three-way handshake protocol:

A three-way handshake protocol is a method used in a TCP/IP network to establish the connection between a client and server to exchange SYN and ACK (acknowledgement) packets before the communication of actual data starts.

iOS ip address: 192.168.137.228
Android ip address: 192.168.137.97

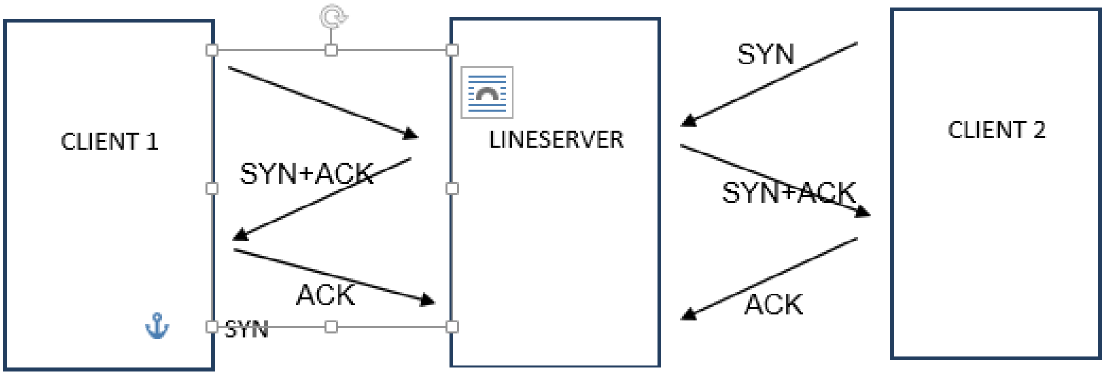

Figure 2 **Mapping with Line Server using three-way handshake protocol**

Platform	**OS version**	**Device model**	**LINE version**
Android	9.1.0	OnePlus 5,Note 9	8.10.2
iOS	13.1	iPhone xr,8 plus	8.8.0
Windows	10	lenovo ideapad 330S	5.8.0

Fig ure 3 The devices used for analysis

In **Figure 3,** this details about the devices which are used to analysis the network traffic

In **figure 2** depicted above explains when client initiates a communication, a pairing is done with the line server using the three-way handshake protocol. Once the destination client receives the communication sent by client 1, client 2 creates a connection with line server using the three-way handshake protocol again.

As Instant Messaging apps are becoming widespread, it is essential to find the forensic artefacts that are being left by the usage of those secure apps [16]. In this paper, the behavior of LINE secure traffic is extensively studied and signatures for various LINE user activities were observed based on the patterns in the traffic. A large number of simulations were done to derive conclusions about the user activities signatures. The accuracy and the reliability of the traffic profiling was increased by analyzing in different platforms with different devices in various networks [18]. Through necessary screenshots and tables, detection of LINE secure traffic and their user activities classification into voice/video calls, text messaging and file sharing is demonstrated in this paper.

5 Implementation

5.1 Android and IOS:

5.1.1 ATTACHMENTS:

There are different types of attachments that can be sent using LINE application. They are images, videos, other file types like pdf, txt, docx , html etc., contacts, and locations. There are also other user activities like sending emoji stickers, viewing profile information etc. All observed byte patterns and their related events are given below.

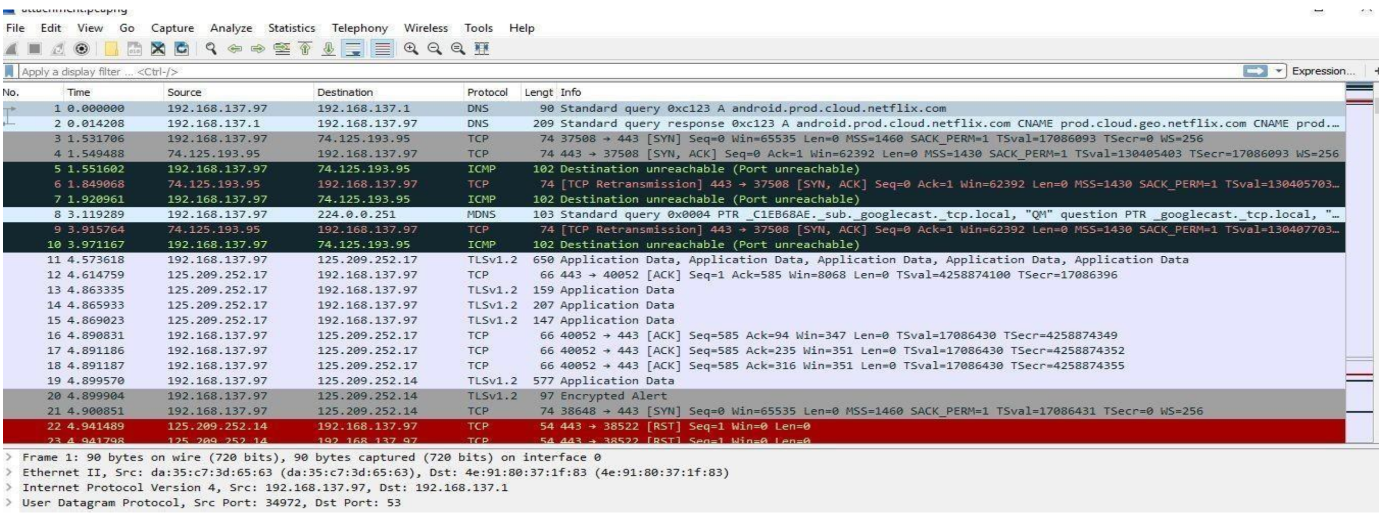

Figure 4 Analysis of network traffic while sending attachments

This **Figure 4** explains about the network traffic analyzed while sending the attachment file between two devices using Line application.

5.1.2 EMOJI

Emoji are the smileys used in instant messages and web pages. These are more like emoticons.

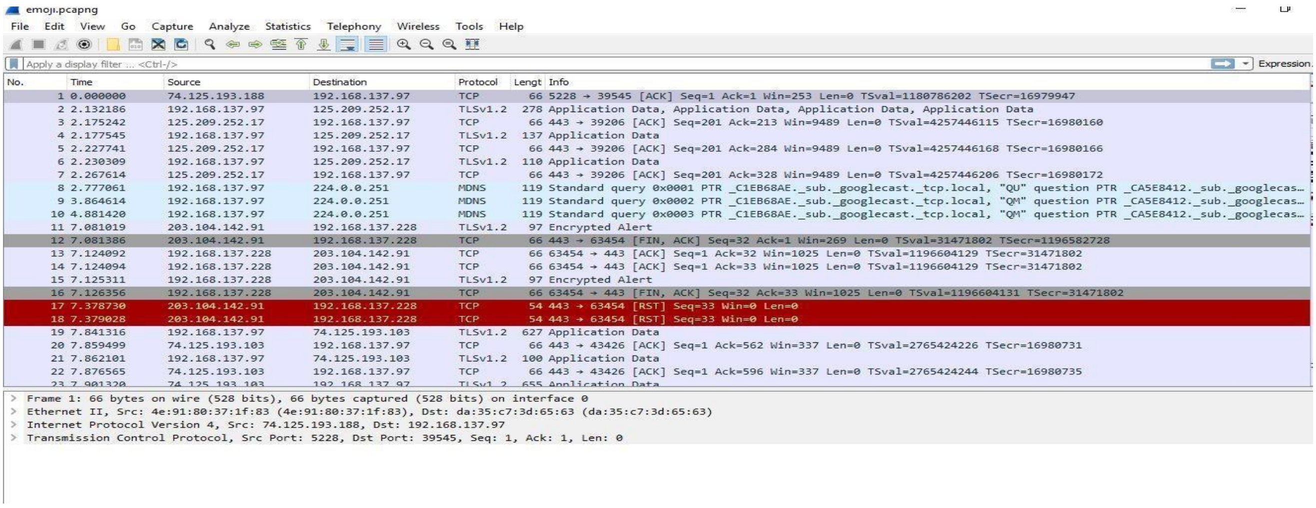

Figure 5 Traffic analysis while sending emoji

This Figure 5 shows the traffic analyzed while sending the emoji using Line application.

5.1.3 CALLING (VIDEO CALL AND VOICE CALL)

One of main difference between the voice and video calls in the LINE app traffic was the packet sizes. Among the hundreds of samples traffics, it was constantly observed that voice call packets will be between 50 bytes to 250 bytes. Packets of video calling will be between 800 bytes to 1200 bytes. When changing from video to voice call or vice versa, the change in packet sizes were also observed clearly.

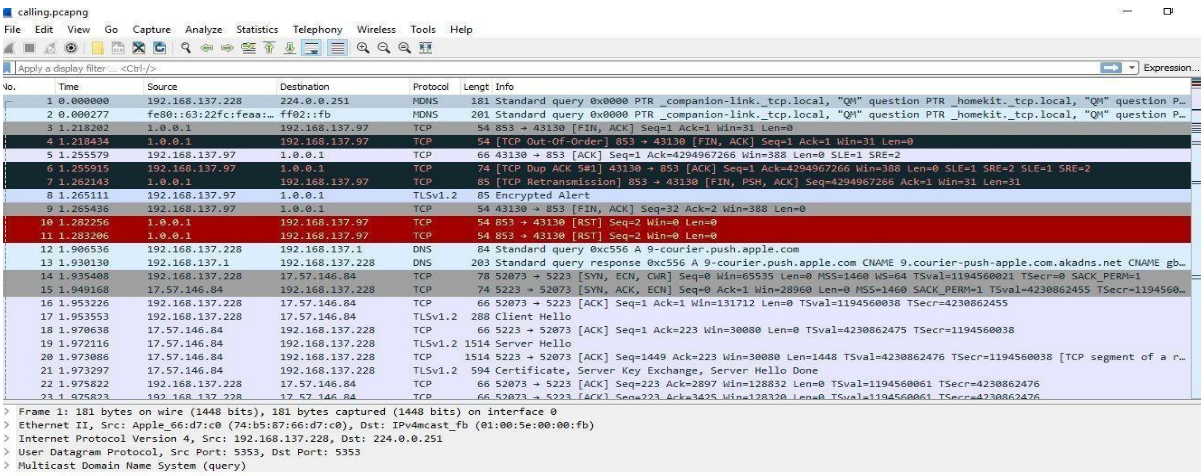

Figure 6 network traffic analysis during video and voice call

This **Figure 6** shows the network traffic while doing voice call and the packet size are increased if it changes to video call. The video or voice call are analyzed by the packet size.

5.1.4 TEXT

In Text messages, there are two different events. They are user start typing and user sending the message. For both these events, two different signatures were observed during the behavior analysis.

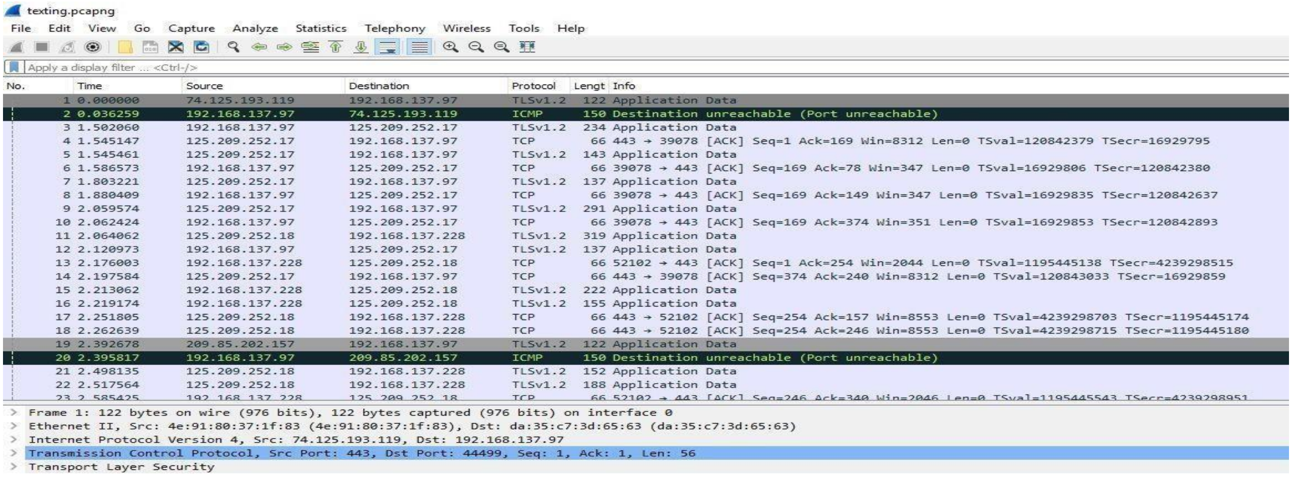

Figure 7 Network traffic analysis while sending text messages

The **Figure 7** shows the traffic between two devices while sending the text messages. The signature are analyzed while sending the text.

6 Evaluation

6.1 Android and IOS :

As presented during the implementation part, both android and iOS applications have same signatures for various user activities. Those signatures are:

Table 1 signature of user activities

Event	**Payload size (bytes)**	**From**	**To**
User starts typing	234 66	Client Server	Server Client
User sends the	137	Server	Client
message	66	Client	Server

End of voice/video call	147 66	Server Client	Client Server
Sending Attachments (image, video, other file types, contacts)	577 66 427 66	Client Server Server Client	Server Client Client Server
Start typing emoji stickers	162 66	Client Server	Server Client
Sending Emoji sticker	137 66	Client Server	Server Client

In the above **Table 1** these signatures are table as examination is conducted on hundreds of network samples on both android and iOS devices.

6.1.1 Signature for Attachments:

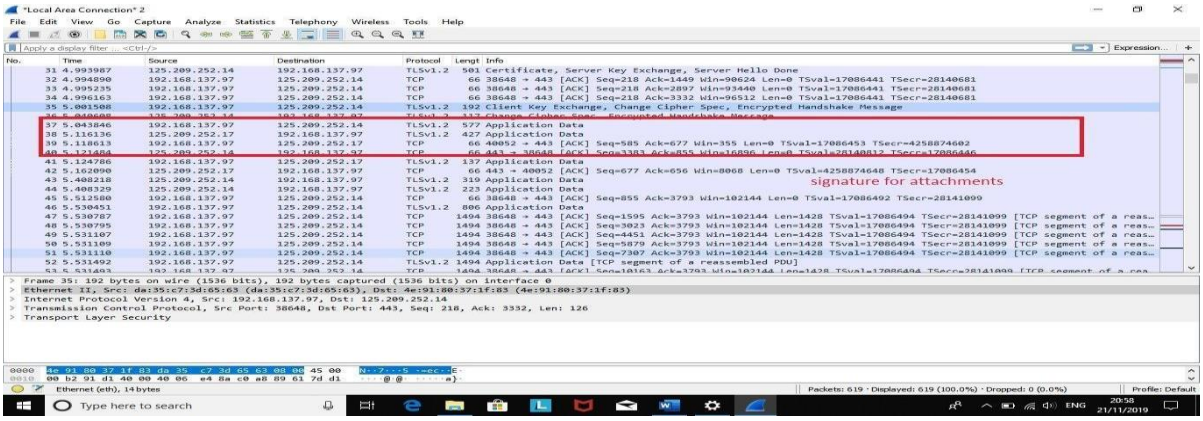

Figure 8 Signature for attachments

This screenshot, **Figure 8** illustrates about the signature found while sending attachments from two devices. IP address (iOS): **192.168.137.228** and (Android): **192.168.137.97** .192.168.137.97 send the attachment to 192.168.137.228. The signature found for sending attachments is **577 is from client to server66 ACK message from server to client 427 is from server to client 66 ACK message from client to server.**

6.1.2. Signature for Emoji:

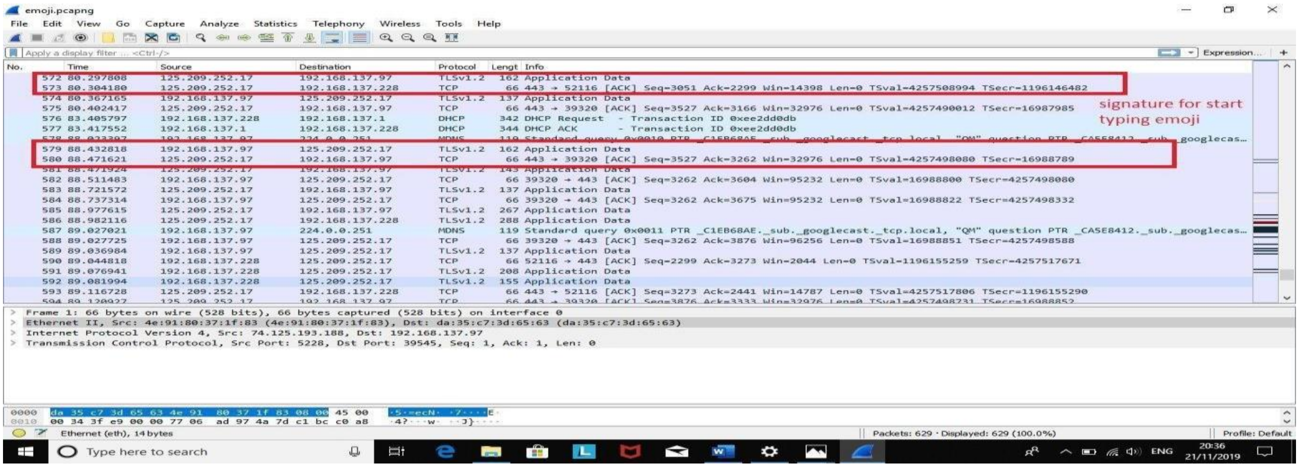

Figure 9 Signature for emoji

This above **Figure 9** shows about the signature found while sending the emoji from two devices. IP address (iOS): **192.168.137.228** and (Android): **192.168.137.97 .** 192.168.137.97 send the emoji to
192.168.137.228. The signature found for sending emoji is **162 is from client to server .Client starts typing emoji 66 ACK message from server to client**
137 is from client to server. when the client hits the send button. 66 ACK message from server to client

6.1.3. Signature for Texting :

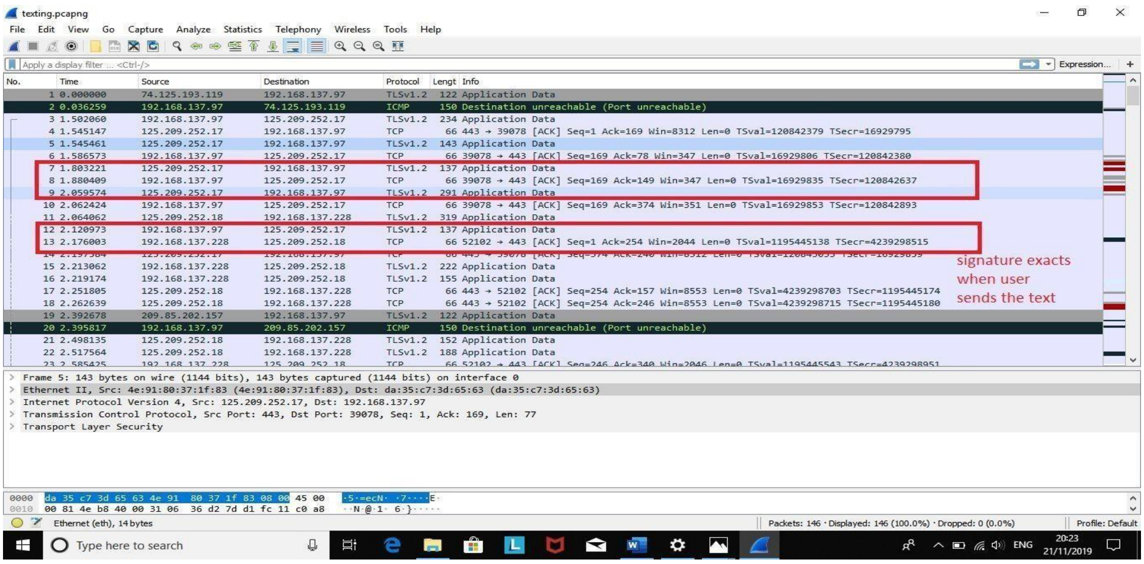

Figure 10 Signature for text messages

This screenshot, Figure 10 details about the signature found while sending text from two devices. IP address (iOS):192.168.137.228 and (Android): 192.168.137.97 192.168.137.97 send the text to 192.168.137.228. The signature found for sending the text messages is 234 is from client to server. When the client starts typing the text 66 ACK message from server to client .137 is from server to client. When the sender hits the send button 66 ACK message from client to server.

6.1.4. Signature for Calling:

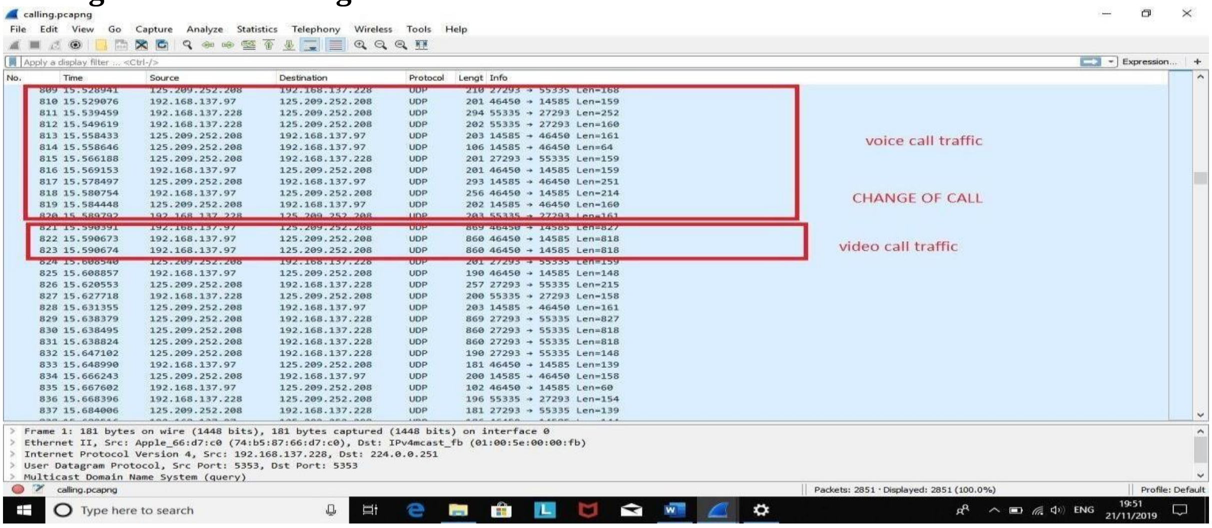

Figure 11 Signature for video and voice call

In Figure 11 explains about the signature found for the video and voice call traffic. This can be analyzed by packet size. For filtering the voice and video call traffic, the packets size can be used. Filter(Voice call)- frame.len <= 250 && frame.len >= 50
Filter(Video call)- frame.len <= 1200 && frame.len >= 800

Windows

Windows is one of the most popular and common operating system used across the world. LINE has provided a windows desktop application .The various user activities and their signatures are given below.

6.1.5 Voice and video call

For voice & video calling feature, the signature doesn't change from the android and IOS traffic [15]. The voice call data payload stays between 50-250 bytes and video call packets stay between 800-1200 bytes in size. When changing from video to voice call or vice versa, the change in packet size were also observed clearly.

Other User Activities:

Unlike android/iOS applications, the windows LINE application doesn't have different signature for different user activities. Because, for both sending and receiving, the activities like text messages, attachment files and emoji's have same signature [19]. Hence, profiling those activities will be harder than the android/iOS traffic. But they can be classified based on the position of the signature chunk in that session. There are also few different signatures for activities like profile viewing. The various signatures according to the windows LINE application are:

Event (send/receive)	Payload size (bytes)	Position	From	To
text message	110 56 116 56	At the end of the session	Client Server Client Server	Server Client Server Client
Attachments (audio/video files)	110 56 116 56	Beginning of the session	Client Server Client Server	Server Client Server Client
Attachments (other file types, contacts)	110 56 116 56	End of the session	Client Server Client Server	Server Client Server Client

Table 2. Signatures of Windows LINE app.

From the above **Table 2 signatures of windows LINE app**, it is clear that profiling the user activities of windows LINE application will be tricky, since most of the user activities share the same signature [14] with few differences. Hence it is important to note those few differences like position of the signature chunk to successfully profile those activities.

6.3 IOS to IOS

6.3.1. ATTACHMENTS

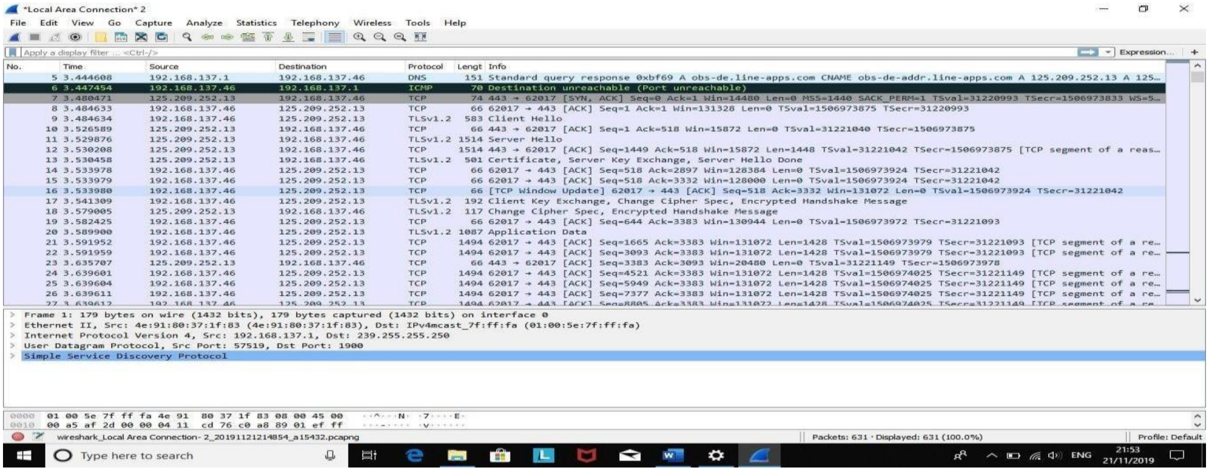

Figure 12 signature for attachment in IOS

This above **Figure 12** shows about the signature found while sending the attachment from two devices. IP address (iOS): **192.168.137.228** and (iOS): **192.168.137.46** 192.168.137.46 send the attachment to 192.168.137.228. The signature found for sending attachments is **583 is from client to server . 66 ACK message from server to client 501 is from server to client. 66 ACK message from client to server.**

6.3.3 TEXT

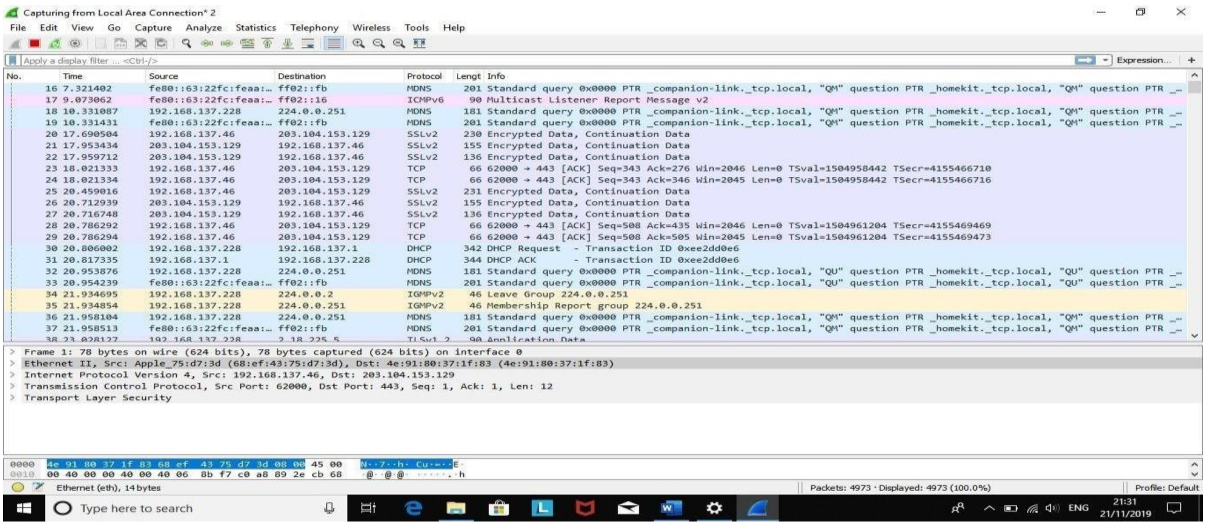

Figure 14 signature for text in IOS

This above **Figure 14** shows about the signature found while sending the text from two devices. IP address (iOS): **192.168.137.228** and (iOS): **192.168.137.46** 192.168.137.46 send the text to 192.168.137.228. The signature found for sending text messages is **231 is from client to server .**

66 ACK message from server to client 136 is from server to client.

66 ACK message from client to server.

6.3.4 VIDEO AND VOICE CALLING

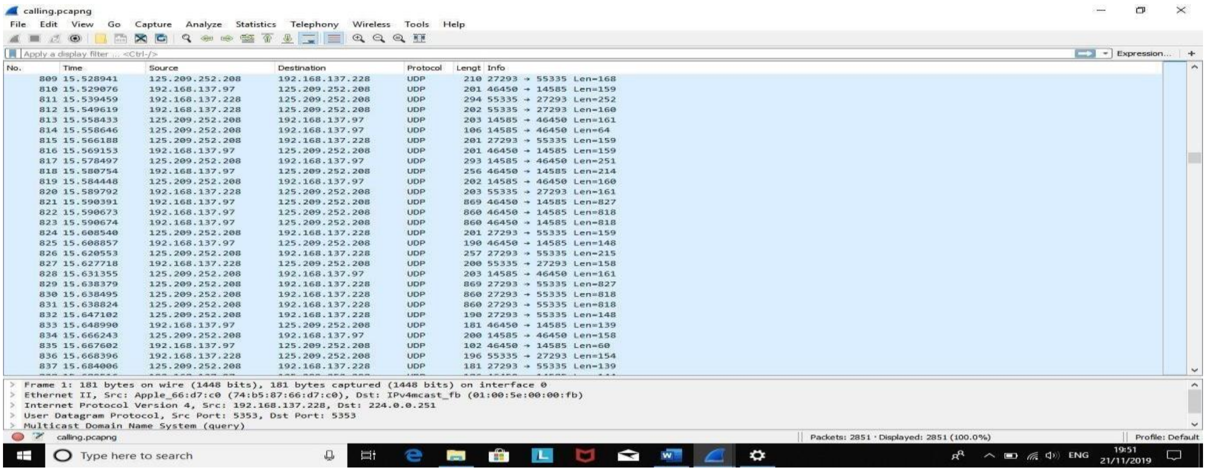

Figure 15 signature for calling in IOS

In **Figure 15 ,** Signature of video and voice call is determined by the packet size.

For filtering the voice and video call traffic, the packets size can be used. Filter(Voice call)- frame.len <= 250 && frame.len >= 50
Filter(Video call)- frame.len <= 1200 && frame.len >= 800

7 Conclusion and Future Work

The above analysis implies the profiling the user activities even on the encrypted network traffic. The analysis explains detail about the various signature profiling the user activities like voice/ video calling, sending text messages, attachments,file sharing and location accuracy so on. The findings of the signatures are based on the payload sizes and the frequency of the packets sent and receive. The network traffic analysis can be done in different platforms such as an Android, iOS, windows and macOS. The mobile devices such as android and iOS have a numerous sensitive information regarding the user activities. These analyses will help the investigators or any security professionals in their research. The analysis is done with single user communications, there is an enhanced feature such as group chat messaging which needs a clear study for the future works. Further research can be done with group messaging and group calling features of the LINE applications can be performed on various platforms. To conclude from the above analysis,it is clear analysis of profiling the user activities based on the signatures that found in the traces of analyzing the network traffic. This information gathered are sensitive and can be useful for the person in the Law Enforcement Agency or Corporate investigation cases. The suspect user activities can be found without spooking the user. If a decryption key for the encrypted LINE traffic is analyses in the future, these signatures are useful for decrypting the data .

References

1. F. A. Awan, Forensic examination of social networking applications on smartphones,, Vol. 2015.

2. F. N. Dezfouli, A. Dehghantanha, Brett, Eterovic- Soric & Kim-Kwang Raymond Choo (2015)Inves- tigating Social Networking applications on smart- phones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms, Australian Journal of Forensic Sciences 48 (4) 469– 488.

3. K. A. A. Zaabi, Android Forensics: Investigating Social Networking Cybercrimes against Man-in-the- Middle Attacks, 2016.

4. D. Walnycky, I. Baggili, A. Marrington, J. Moore, F. Breitinger, Network and device forensic analysis of Android social-messaging applications, Digital In- vestigation, Volume 14 (1), S77-S84, ISSN 1742- 2876.

5. M. A. K. Sudozai, N. Habib, S. Saleem, A. A. Khan, Signatures of Viber Security Traffic, Journal of Dig- ital Forensics, Security and Law 12 (2).

6. F. Karpisek, I. Baggili, F. Breitinger, WhatsApp net- work forensics: Decrypting and understanding the WhatsApp call signaling messages.

7. F. C. Tsai, E. C. C. D. Y. Kao, WhatsApp network forensics: Discovering the communication payloads behind cybercriminals, Korea (South, 2018.

8. Z. Yuan, C. Du, X. Chen, D. W. Y. Xue, SkyTracer: Towards fine- grained identification for Skype traffic via sequence signatures, Honolulu, HI, 2014.

9. S. E. K. P. Dyer, Traffic Analysis of Encrypted Mes- saging Services: Apple iMessage and Beyond, SIG- COMM Comput. Commun. Rev 44 (2014) 5–11.

10. N. Malik, J. Chandramouli, P. Suresh, K. Fairbanks, L. W. W. H. Robinson, Using network traffic to verify mobile device forensic artifacts, NV, 2017.

11. M. A. K. S. S. Saleem, Profiling of secure chat and calling apps from encrypted traffic,2018.

12. ‘LINE Transparency Report’ (LINE Corporation)

13. N. &. B. I. &. M. A. (. F. a. o. s. n. a. o. m. d. D. I. 9. S. 1. Al Mutawa, Forensic analysis of social networking applications on mobile devices, 2012.

14. T. V. a. R. L. Artur Kane, The data privacy-preserving way, 2018.

15. F. &. B. I. &. B. F. (. W. n. f. D. a. u. t. W. c. s. m. D. I. 1. 1. Karpisek, WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages.

16. F.Karpisek, WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages, 2015.

17. F. A. Awan, Forensic examination of social networking applications on smartphones, 2018.

18. J. Fran¸cois, Network traffic analysis (for encrypted traffic and security monitoring), 2017.

19. P. &. C. M. &. C. P. &. D. M. (. A. s. o. m. f. e. t. c. a. a. I. J. o. N. M. 2. 1. Velan, A survey of methods for encrypted traffic classification and analysis, 2019.

20. C. K. Ambreen F.A.H1, Forensic Analysis of Social Applications, 2012.