ANALYSIS OF ENCRYPTED NETWORK TRAFFIC FROM SECURE INSTANT MESSAGING APPLICATION: CASE STUDY ON SYNOLOGY CHAT INSTANT MESSAGE APPLICATION

Grinaldy Yafi' Rasyad[1], Dedy Hariyadi[2], Tri Febrianto[3]

[1] Universitas Gadjah Mada
[2] Universitas Jenderal Achmad Yani Yogyakarta
[3] PT Widya Adijaya Nusantara
Email: [1] grinaldy.yafi@mail.ugm.ac.id, [2] dedy@unjaya.ac.id, [3] tri.febrianto@widyasecurity.com

Abstract

Instant messaging applications have a very important role in online interactions, especially during the COVID-19 pandemic. A safe and reliable instant messaging application for some people provides convenience and benefits. This paper examines network forensic experiments in the form of analysis of encrypted network traffic from the Synology Chat instant messaging application which identifies communication network traffic patterns using the Wireshark application. Tests in this study were carried out by direct experiments using infrastructure that is in line with the Man In the Middle test method, namely monitoring network traffic on client and server communications. Analysis is carried out by monitoring network patterns in the form of IP addresses and the size of packets sent and the protocol used. Network pattern monitoring is carried out on three channels, namely public group, private group, and personal message. Based on evidence that the packet size pattern sent by the public group has a pattern that is almost the same as personal chat and the private group has a larger packet size pattern than other channels. The dominant protocol uses TLSv1.2 as the protocol for sending encrypted data. Based on these findings, the pattern can be used as a guide if you want to carry out a forensic investigation on certain cases using the Synology Chat instant messaging application. The dominant protocol uses TLSv1.2 as the protocol for sending encrypted data. Based on these findings, the pattern can be used as a guide if you want to carry out a forensic investigation on certain cases using the Synology Chat instant messaging application. The dominant protocol uses TLSv1.2 as the protocol for sending encrypted data. Based on these findings, the pattern can be used as a guide if you want to carry out a forensic investigation on certain cases using the Synology Chat instant messaging application.

***Keywords**: synology chat, wireshark, network forensics, instant messaging, MITM*

1. INTRODUCTION

The problem that is of concern in the community is the privacy security of users of an application. People are worried if the application they use is not safe because a third party is trying to monitor user activity. One of the applications used in society is an online instant messaging application. The choice of this online instant messaging application because it provides many advantages over the features offered such as convenience in use, speed, and complete features according to user needs. In 2020, during the COVID-19 pandemic, instant messages were widely used by 4.3 trillion, with an increase of 9% supported by work that was predominantly done at home or work from home.(Afzal et al., 2021). As you know, instant messengers that are often used, namely WhatsApp, Facebook Messenger, Telegram, LINE and many more, try to make users comfortable using their applications, such as maintaining data privacy by using encryption techniques in sending data. The quality of this application also helps companies to find opportunities, marketing and advertising offered by the platform. Security and user convenience, of course, takes time to develop, and developers are certainly not immune from flaws in developing applications that allow irresponsible people to take advantage of vulnerabilities in these applications. This study aims to practice sending messages and analyzing network traffic patterns on encrypted Synology Chat instant messages. Synology Chat is a feature of the Synology brand Network Attach Storage (NAS) which functions as a chat server. Apart from being a file sharing server, Synology's NAS has many features, including as a chat server (Sidik & Putra, 2018). This research can provide benefits and contributions, namely helping to identify encrypted network traffic patterns on Synology Chat instant messages and ensure that Synology Chat instant messages are safe to use based on the findings obtained. Apart from being a file sharing server, Synology's NAS has many features, including as a chat server (Sidik & Putra, 2018). This research can provide benefits and contributions, namely helping to identify encrypted network traffic patterns on Synology Chat instant messages and ensure that Synology Chat instant messages are safe to use based on the findings obtained. Apart from being a file sharing server, Synology's NAS has many features, including as a chat server (Sidik & Putra, 2018). This research can provide benefits and contributions, namely helping to identify encrypted network traffic patterns on Synology Chat instant messages and ensure that Synology Chat instant messages are safe to use based on the findings obtained.

2. RESEARCH METHODS

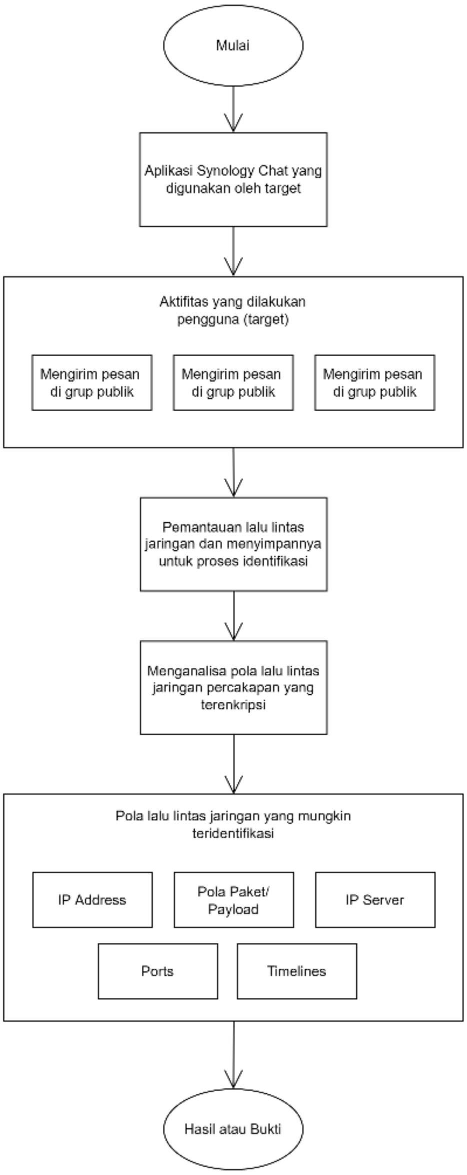
The large number of users and the popularity of social media, especially online instant messaging, is an interesting research material from a network forensic perspective. For example, several studies related to network traffic conducted by Walnycky et al analyzed devices and network traffic in 20 applications by collecting evidence in the form of passwords, images and others. The same thing was also done by Yusoff, et al, namely in the form of network forensic analysis on well-known social media such as Facebook, Twitter and Telegram on the Firefox Mobile Simulator while the simulator monitored its communication network using Wireshark and then managed to get IP addresses, ports, domains and subdomains but could not identify distinct patterns in certain activities.(Sudozai et al., 2018). In another study conducted by Conti et al. applications such as Facebook, Gmail, and Twitter are decoded on user actions using machine learning based on domain filtering, packet filtering, packet intervals, and timeouts. The results of such research can assist in studying the activities of one or more users, thereby in assisting decision making by cybersecurity experts. Research from Università del Piemonte Orientale conducted research on the AnForA automation application that android applications installed on virtual android devices can monitor a series of activities on the device's storage(Anglano et al., 2020). Another study conducted by Rathi et al. that the results of the analysis of the WeChat, Viber, WhatsApp and Telegram applications indicate that it is possible to retrieve encrypted database files in applications installed on rooted devices. Another study related to network analysis focuses on the WhatsApp application when making calls by decrypting itnetwork traffic(Karpisek et al., 2015). In other studies, there is a forensic analysis on social media such as Facebook, Twitter and LinkedIn on different platforms such as iOS, Android, Windows and Blackberry with the result that the Blackberry platform cannot recover device memory such as location, database with information about visited profiles, names. , tweets, contacts, profile ID (Cloud., 2015).

This research was carried out by direct practice in the form of experiments on infrastructure that had been arranged according to the Man In the Middle method, namely placing a third party to monitor conversational network traffic between client and server.(Mallik, 2018).The research begins by activating monitoring tools using Wireshark which then users send messages on public group, private group and personal chat channels. Then the results of the monitoring are analyzed for patterns which can be server and client IP, ports, timeline and payload patterns or packets sent, such as in figure 1

OnTable1provides information that the tools used for this experiment have their respective functions, especially to analyze a pattern in the messages sent, how clients and servers communicate and use any protocols and ports, it will be difficult if the tools used are not correct.

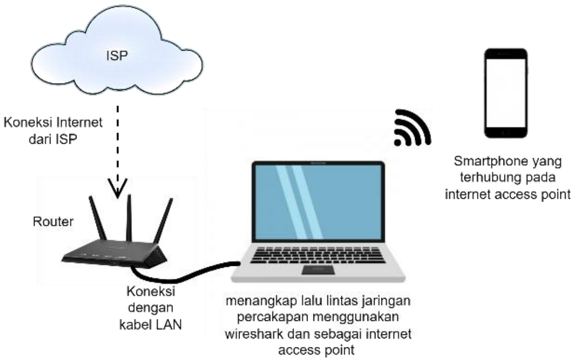
Table1Research Equipment

Device	**Purpose**	**Brand**	***Software/OS***
ZTE Routers	LAN Connection	ZTE	V7.0.10P1N14
LAN cable	Wired Connection	-	-
Desktop Computers	Deploy Wireshark	Lenovo	Windows 10, 64-bit with x64-based processor, 8 GB RAM, Intel (R) Core (TM) i7-5500U CPU @2.40 GHz.
Wireshark	Read network traffic	-	3.6.0
Synology Chat application	Carry out messaging activities	Synology Inc	2.7.1
Smartphones	Doing activities on the Synology Chat application	Xiaomi POCO X3	Android 12


Mulai
Aplikasi Synology Chat yang digunakan oleh target
Aktifitas yang dilakukan pengguna (target)
Mengirim pesan di grup publik
Mengirim pesan di grup publik
Mengirim pesan di grup publik
Pemantauan lalu lintas jaringan dan menyimpannya untuk proses identifikasi
Menganalisa pola lalu lintas jaringan percakapan yang terenkripsi
Pola lalu lintas jaringan yang mungkin teridentifikasi
IP Address
Pola Paket/ Payload
IP Server
Ports
Timelines
Hasil atau Bukti

Picture1. Analysis and Monitoring Flow

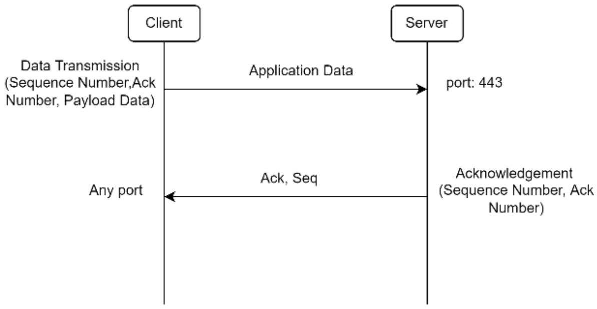
So that the monitoring machine can record communication network traffic, the infrastructure must be set in the form of an internet network provided by an ISP (internet service provider) using a router which is then connected using a LAN cable, then the laptop as the monitoring machine is set up as a wireless access point, as shown in figure 2. Mobile phones running the Synology Chat application will be connected to a laptop that has been configured as a wireless access point. The scenario starts when the user sends a message and then the network traffic is monitored by the laptop using the Wireshark application. This method is commonly called Man In The Middle which functions to monitor the activity of the target when communicating, in this study communicating with the Synology Chat server.


ISP
Koneksi Internet dari ISP
Router
Koneksi dengan kabel LAN
menangkap lalu lintas jaringan percakapan menggunakan wireshark dan sebagai internet access point
Smartphone yang terhubung pada internet access point

Picture2. Synology Chat Communication Network Traffic Monitoring Scenario

The scenario is carried out by monitoring the traffic that occurs between the user (target) and the server. From this scenario, we get communication network traffic captured using the Wireshark application which is then analyzed for network traffic patterns sending messages on the Synology Chat application. The process of sending messages to the Synology Chat application via the TCP Data Transfer process shown in Figure 3 begins when the user sends a message (client) which then the application data or messages to be sent are transferred to the server on port 443 with the TLSv1.2 security protocol. Then the server replies to what has been sent by the client in the form of an acknowledgment containing a sequence number, an ack number which is then sent to the intended port (client).

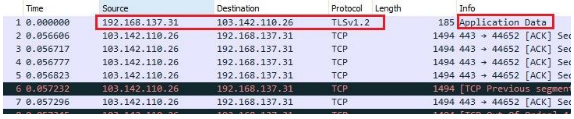
Messages are sent on three different channels, namely public groups, private groups and personal messages. The three channels send the same message, namely "TESTING CHAT".


Client
Server
Data Transmission (Sequence Number,Ack Number, Payload Data)
Application Data
port: 443
Any port
Ack, Seq
Acknowledgement (Sequence Number, Ack Number)

Picture3. TCP Data Transfer on Message Delivery Process

1. *PublicGroup*

*public groups*is an all-view group and all can join without invitation (Inc., 2022). The first experiment is by sending a "TESTING CHAT" message to the public group to find out the pattern of each message if it is sent via the public group channel then each message is recorded for its network traffic pattern using Wireshark. Figure 4 shows network traffic sending messages logged using Wireshark. The message sent for the first time in the public group recorded at time 0 provides information that the data sent from the IP client (192.168.137.31) sends Application Data with a packet of 185 which is sent via the TLSv1.2 protocol to the destination IP server (103.142.110.26) .



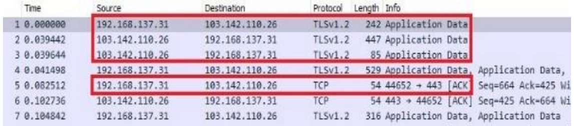
```
  Time        Source            Destination       Protocol  Length    Info
1 0.000000    192.168.137.31    103.142.110.26    TLSv1.2            185 Application Data
2 0.056606    103.142.110.26    192.168.137.31    TCP               1494 443 → 44652 [ACK] Se
3 0.056717    103.142.110.26    192.168.137.31    TCP               1494 443 → 44652 [ACK] Se
4 0.056777    103.142.110.26    192.168.137.31    TCP               1494 443 → 44652 [ACK] Se
5 0.056823    103.142.110.26    192.168.137.31    TCP               1494 443 → 44652 [ACK] Se
6 0.057232    103.142.110.26    192.168.137.31    TCP               1494 [TCP Previous segmen
7 0.057296    103.142.110.26    192.168.137.31    TCP               1494 443 → 44652 [ACK] Se
```

Picture4. Public Group Network Traffic Patterns

2. *Private*Group

*Private groups*is a group visible only to people who have been invited and can only join by invitation (Inc., 2022). The experiment on this private group is the same as the previous channel by sending a "TESTING CHAT" message to the private group to find out the message pattern if it is sent via the private group channel then each message is recorded for its network traffic pattern using Wireshark.

The recorded network traffic shown in Figure 5 provides information that the IP client (192.168.137.31) sends Application Data with packets of 242 to the IP server (103.142.110.26) at the 0th time when the target sends the message the first time, then it continues sending from the server to client twice and also still using the TLSv1.2 protocol. The next pattern that can be seen is at the fifth time where the client sends to the server with the TCP protocol with a packet of 54 with an ACK process to port 443 server.

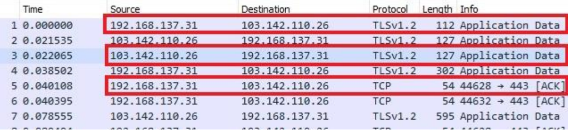


```
  Time        Source            Destination       Protocol  Length Info
1 0.000000    192.168.137.31    103.142.110.26    TLSv1.2   242 Application Data
2 0.039442    103.142.110.26    192.168.137.31    TLSv1.2   447 Application Data
3 0.039644    103.142.110.26    192.168.137.31    TLSv1.2    85 Application Data
4 0.041498    192.168.137.31    103.142.110.26    TLSv1.2   529 Application Data, Application Data,
5 0.082512    192.168.137.31    103.142.110.26    TCP        54 44652 → 443 [ACK] Seq=664 Ack=425 Wi
6 0.102736    103.142.110.26    192.168.137.31    TCP        54 443 → 44652 [ACK] Seq=425 Ack=664 Wi
7 0.104842    192.168.137.31    103.142.110.26    TLSv1.2   316 Application Data, Application Data
```

Picture5. Private Group Network Traffic Patterns

3. *Personal Chat*

*Personal chat*This can be done by directly sending a message to the person concerned. The pattern identified in sending messages using personal chat can be seen in Figure 6 which shows that the pattern for sending application data from the IP client (192.168.137.31) to the IP server (103.142.110.26) with the TLSv1.2 protocol with 112 packets at a time 0. Then for sending from the IP server (103.142.110.26) to the IP client (192.168.137.31) at number 3 uses the TLSv1.2 protocol to send application data by sending a packet of 127. At number 5 it sends data from the IP client (192.168.137.31) to the IP server (103.142.110.26) using the TCP protocol with a packet size of 54.



```
  Time        Source            Destination       Protocol  Length Info
1 0.000000    192.168.137.31    103.142.110.26    TLSv1.2   112 Application Data
2 0.021535    103.142.110.26    192.168.137.31    TLSv1.2   127 Application Data
3 0.022065    103.142.110.26    192.168.137.31    TLSv1.2   127 Application Data
4 0.038502    192.168.137.31    103.142.110.26    TLSv1.2   302 Application Data
5 0.040108    192.168.137.31    103.142.110.26    TCP        54 44628 → 443 [ACK]
6 0.040395    192.168.137.31    103.142.110.26    TCP        54 44632 → 443 [ACK]
7 0.078555    103.142.110.26    192.168.137.31    TLSv1.2   595 Application Data
```

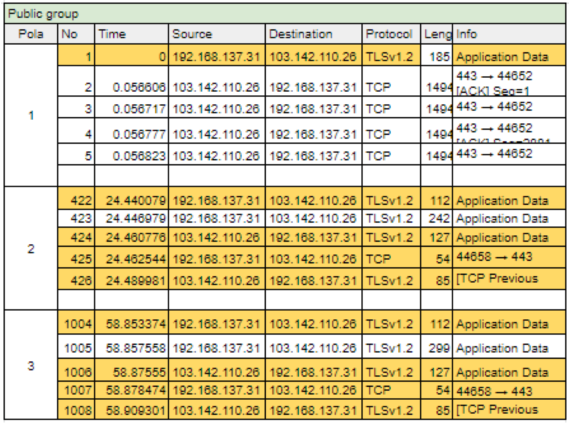
Picture6. Personal Message Network Traffic Patterns

3. RESULTS AND DISCUSSION

This Synology Chat application uses the TLSv1.2 protocol (Transport Layer Security), which is an encryption protocol used to send data on the internet.(Ali, 2021). This protocol encrypts the payload, so only the packet size is visible and the pattern can be analyzed from this information. The pattern that looks different between public group channels, private group and private chat. Each channel has a different pattern which is shown in the amount of Lenght, which is a value of the data packet including the header with the size of the byte.

1. Patterns on public groups

In the public group, it can be seen that patterns 2 and 3 have similarities in the delivery IP address of the client to the server and vice versa with the protocol used and the size of the packet sent is the same, while the difference in packet size after sending a packet is 112 in pattern 2 and 3, as shown in figure 7.

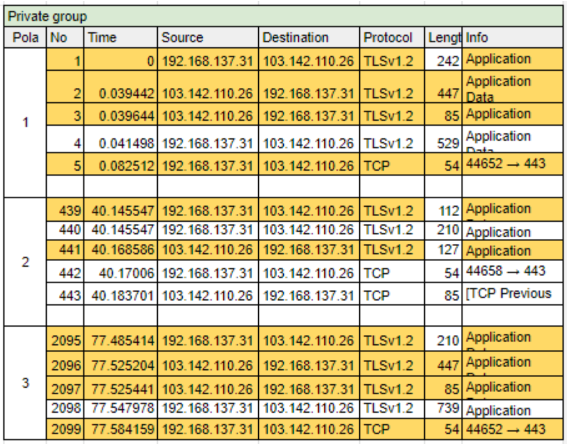


Public group							
Pola	No	Time	Source	Destination	Protocol	Leng	Info
1	1	0	192.168.137.31	103.142.110.26	TLSv1.2	185	Application Data
	2	0.056606	103.142.110.26	192.168.137.31	TCP	1494	443 → 44652 [ACK] Seq=1
	3	0.056717	103.142.110.26	192.168.137.31	TCP	1494	443 → 44652
	4	0.056777	103.142.110.26	192.168.137.31	TCP	1494	443 → 44652
	5	0.056823	103.142.110.26	192.168.137.31	TCP	1494	443 → 44652
2	422	24.440079	192.168.137.31	103.142.110.26	TLSv1.2	112	Application Data
	423	24.446979	192.168.137.31	103.142.110.26	TLSv1.2	242	Application Data
	424	24.460776	103.142.110.26	192.168.137.31	TLSv1.2	127	Application Data
	425	24.462544	192.168.137.31	103.142.110.26	TCP	54	44658 → 443
	426	24.489981	103.142.110.26	192.168.137.31	TLSv1.2	85	[TCP Previous
3	1004	58.853374	192.168.137.31	103.142.110.26	TLSv1.2	112	Application Data
	1005	58.857558	192.168.137.31	103.142.110.26	TLSv1.2	299	Application Data
	1006	58.87555	103.142.110.26	192.168.137.31	TLSv1.2	127	Application Data
	1007	58.878474	192.168.137.31	103.142.110.26	TCP	54	44658 → 443
	1008	58.909301	103.142.110.26	192.168.137.31	TLSv1.2	85	[TCP Previous

Picture7. Identified Patterns in Public Groups

2. Patterns on private groups

The pattern identified in the private group is slightly different from the other channels, namely in the size of the packets sent. Patterns 1 and 3 have the same packet size sent from the IP server to the client, namely 447 and 85, then when sending using TCP the packet size becomes 54. It can be seen that all dominant patterns use the TLSv1.2 protocol in sending application data from client to server or On the other hand, as shown in Figure 8.



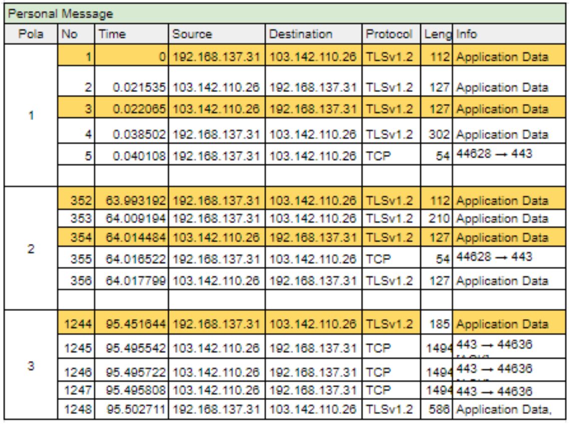
Private group

Pola	No	Time	Source	Destination	Protocol	Lengt	Info
1	1	0	192.168.137.31	103.142.110.26	TLSv1.2	242	Application
	2	0.039442	103.142.110.26	192.168.137.31	TLSv1.2	447	Application Data
	3	0.039644	103.142.110.26	192.168.137.31	TLSv1.2	85	Application
	4	0.041498	192.168.137.31	103.142.110.26	TLSv1.2	529	Application Data
	5	0.082512	192.168.137.31	103.142.110.26	TCP	54	44652 → 443
2	439	40.145547	192.168.137.31	103.142.110.26	TLSv1.2	112	Application
	440	40.145547	192.168.137.31	103.142.110.26	TLSv1.2	210	Application
	441	40.168586	103.142.110.26	192.168.137.31	TLSv1.2	127	Application
	442	40.17006	192.168.137.31	103.142.110.26	TCP	54	44658 → 443
	443	40.183701	103.142.110.26	192.168.137.31	TCP	85	[TCP Previous
3	2095	77.485414	192.168.137.31	103.142.110.26	TLSv1.2	210	Application
	2096	77.525204	103.142.110.26	192.168.137.31	TLSv1.2	447	Application
	2097	77.525441	103.142.110.26	192.168.137.31	TLSv1.2	85	Application
	2098	77.547978	192.168.137.31	103.142.110.26	TLSv1.2	739	Application
	2099	77.584159	192.168.137.31	103.142.110.26	TCP	54	44652 → 443

Picture8. Identified Patterns in Private Groups

3. Pattern in personal message

In personal chat patterns 1 and 2 have the same pattern in sending application data from the IP client to the server and vice versa. Then the Length of the data packet sent is the same, namely in pattern 1 number 1 of 112 with pattern 2 number 352. Likewise with pattern 1 number 3 and pattern 2 number 354, the Length value of the same packet is 127. The protocol used is also the same i.e. TLSv1.2. The difference is only in the 3rd pattern in the length of the packet sent and the IP pattern afterwards but still using TLSv1.2 as shown in Figure 9.



Personal Message

Pola	No	Time	Source	Destination	Protocol	Leng	Info
1	1	0	192.168.137.31	103.142.110.26	TLSv1.2	112	Application Data
	2	0.021535	103.142.110.26	192.168.137.31	TLSv1.2	127	Application Data
	3	0.022065	103.142.110.26	192.168.137.31	TLSv1.2	127	Application Data
	4	0.038502	192.168.137.31	103.142.110.26	TLSv1.2	302	Application Data
	5	0.040108	192.168.137.31	103.142.110.26	TCP	54	44628 → 443
2	352	63.993192	192.168.137.31	103.142.110.26	TLSv1.2	112	Application Data
	353	64.009194	192.168.137.31	103.142.110.26	TLSv1.2	210	Application Data
	354	64.014484	103.142.110.26	192.168.137.31	TLSv1.2	127	Application Data
	355	64.016522	192.168.137.31	103.142.110.26	TCP	54	44628 → 443
	356	64.017799	103.142.110.26	192.168.137.31	TLSv1.2	127	Application Data
3	1244	95.451644	192.168.137.31	103.142.110.26	TLSv1.2	185	Application Data
	1245	95.495542	103.142.110.26	192.168.137.31	TCP	1494	443 → 44636
	1246	95.495722	103.142.110.26	192.168.137.31	TCP	1494	443 → 44636
	1247	95.495808	103.142.110.26	192.168.137.31	TCP	1494	443 → 44636
	1248	95.502711	192.168.137.31	103.142.110.26	TLSv1.2	586	Application Data,

Picture9. Identified Patterns in Personal Messages

4. CONCLUSIONS AND RECOMMENDATIONS

Synology Chat instant messaging has utilized communication on an encrypted network based on monitoring using Wireshark with the MITM method. Therefore, monitoring is carried out by identifying the IP client, server, the length of the packet sent, the port and timeline that the protocol used is TLSv1.2, that is, the data sent is encrypted. Likewise, the port used is also 443 or HTTPS for web-based communication. The patterns found in the large packets sent to the server or to the client can identify some of the patterns. The length on the public group and private chat packet sizes are almost the same but in the private group the length pattern on the data packets sent is larger than the other channels and the dominant delivery uses the TLSv1.2 protocol.

Suggestions that can be given for future research are to identify other patterns such as when sending pictures, calling, video calls, typing, exchanging messages or when opening applications. This process can be called network forensic analysis which is useful when investigating crimes. This research is also limited to the version of the application used so that in the future the results obtained may be different and also smartphones that still have background processes that affect observations.

BIBLIOGRAPHY

SIDIK, & PUTRA, M. (2018). Implementasi Network Attached Storage (NAS) Menggunakan Synology Disk Station Manager (DSM 5.2) Untuk Optimalisasi Data Sharing Center. Jurnal Teknik Komputer, IV(2), 39-47. doi:10.31294/jtk.v4i2.3508

POLWALNYCKY, D., BAGGILI, I., MARRINGTON, A., MOORE, J., & BREITINGER, F. (2015). Network and device forensic analysis of Android social-messaging applications. *Digital Investigation*, *14*, S77–S84. https://doi.org/10.1016/j.diin.2015.05.009

INC., S. (2022). *Creating Channels and Conversations | Synology Chat - Synology Knowledge Center*. Kb.synology.com. Retrieved 30 August 2022, fromhttps://kb.synology.com/enaf/DSM/help/Chat/chat_creating_channels_conversations?version=7.

ALI, I. (2021). *Examining cyber security implementation through TLS/SSL on academic institutional repository in Indonesia Irhamni Ali*. *17*(2), 238–249.

ANGLANO, C., CANONICO, M., & GUAZZONE, M. (2020). *Computers & Security The Android Forensics Automator (AnForA): A tool for the Automated Forensic Analysis of Android Applications*. *88*. https://doi.org/10.1016/j.cose.2019.101650

KARPISEK, F., BAGGILI, I., & BREITINGER, F. (2015). WhatsApp network forensics : Decrypting and understanding the WhatsApp call signaling messages. *Digital Investigation*, *15*, 110–118. https://doi.org/10.1016/j.diin.2015.09.002

SUDOZAI, M. A. K., SALEEM, S., BUCHANAN, W. J., HABIB, N., & ZIA, H. (2018). Forensics study of IMO call and chat app. *Digital Investigation*, *25*, 5–23. https://doi.org/10.1016/j.diin.2018.04.006

YUSOFF, M.N YUSOFF, M.N.; DEHGHANTANHA, A.; MAHMOD, R. Network Traffic Forensics on Firefox Mobile

OS: Facebook, Twitter, and Telegram as Case Studies. In Contemporary Digital Forensic Investigations of Cloudand Mobile Applications; Elsevier Inc.: Amsterdam, The Netherlands, 2017; pp. 63–78.

AFZAL, A., HUSSAIN, M., SALEEM, S., SHAHZAD, M. K., HO, A. T. S., & JUNG, K. (2021). *applied sciences Encrypted Network Traffic Analysis of Secure Instant Messaging Application : A Case Study of Signal Messenger App*.

CONTI, M., MANCINI, L., SPOLAOR, R., & VERDE, N. (2015). Can't You Hear Me Knocking. *Proceedings Of The 5Th ACM Conference On Data And Application Security And Privacy*. https://doi.org/10.1145/2699026.2699119

RATHI, K.; KARABIYIK, U.; ADERIBIGBE, T.; CHI, H. (2018). Forensic analysis of encrypted instant messaging applications on Android. International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25March 2018.

MALLIK, A. (2018). *MAN-IN-THE-MIDDLE-ATTACK : UNDERSTANDING IN SIMPLE*., Jurnal Pendidikan Teknologi Informasi 2, 2,109–134.

HE, G.; XU, B.; ZHU, H (2017). Identifying Mobile Applications for Encrypted Network Traffic. In Proceedings of the 2017 Fifth International Conference on Advanced Cloud and Big Data (CBD), Shanghai, China, 13–16 August 2017; pp. 279–284.

OMOLARA, A.E.; JANTAN, A.; ABIODUN, O.I.; DADA, K.V.; ARSHAD, H.; EMMANUEL, E. A Deception Model Robust to Eavesdropping Over Communication for Social Network Systems 2019.IEEE. Retrieved 5 September 2022, from https://ieeexplore.ieee.org/document/8760227.

AWAN, F.A. Forensic examination of social networking applications on smartphones (2015). In Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 18 December 2015; pp. 36–43.

GREGORIO, J., GARDEL, A., & ALARCOS, B. (2017). Forensic analysis of Telegram Messenger for Windows Phone. *Digital Investigation*, *22*, 88–106. https://doi.org/10.1016/j.diin.2017.07.004