

Configuration Manual

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 : ...MSc Cyber Security..... **Year :** 2019.....

Module:Academic Internship.....

Lecturer:12-December-2019.....

Submission Due Date:
 ...

Project Title: Network Traffic Based Analysis of Secured Communication Application (LINE)

Word Count:585..... **Page Count:**9.....

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)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
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.	<input type="checkbox"/>

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):

Configuration Manual

Forename Surname
Student ID:

CONFIGURATION MANUAL:

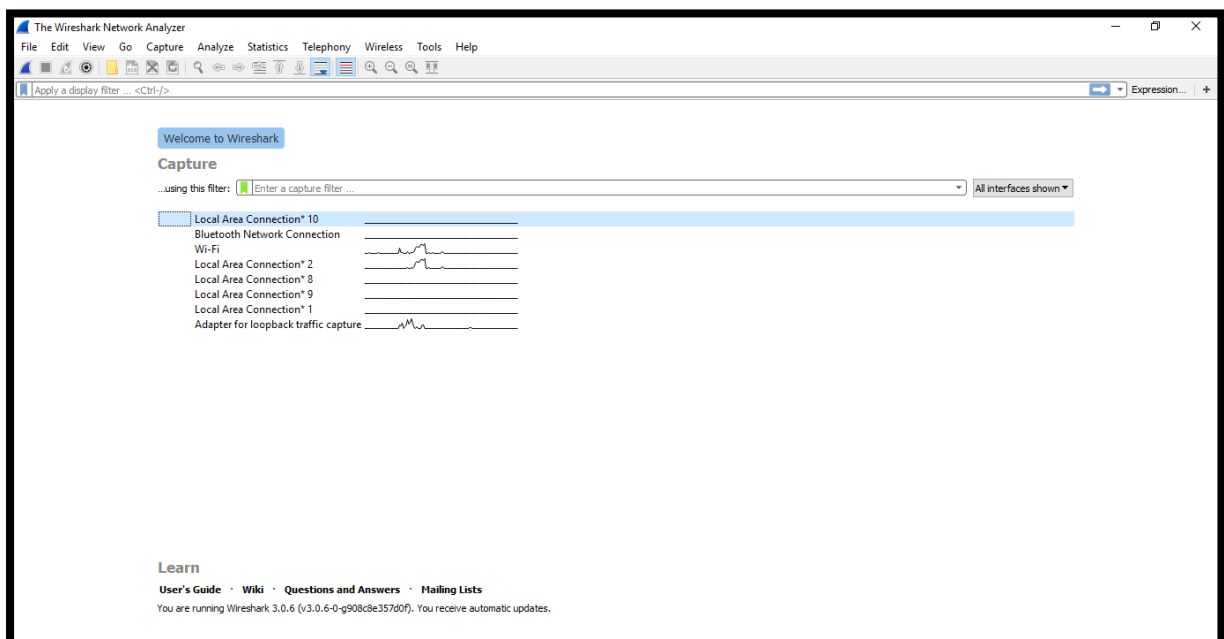
NETWORK TRAFFIC BASED ANALYSIS OF SECURE COMMUNICATION
APPLICATION (LINE)

Step 1: Connect the monitoring devices (wireshark in laptop lenovo ideapad 330S) with the WiFi.

Step 2: Connect the target devices (android, iOS, windows) to the hotspot of the monitoring device.

Step 3: Open Wireshark. To analyse the network traffic.

Step 4:



This picture explains the network traffic analysed in the network. Local area connection 2 . The target devices are connected and the network traffic of the target devices are analysed.

Step 5: By clicking the local area connection 2. It starts analysing the network traffic of the target devices connected to the monitoring devices.

Step 6: Download LINE application in the target devices.

https://play.google.com/store/apps/details?id=jp.naver.line.android&hl=en_IE

Step 7: LINE is an instant messaging application which includes the features like voice call , video call, text messages, location accuracy, and sharing information.

Step 8: By analysing the network traffic the unique signatures are found for the voice call , video call, attachments, and emoji in the target devices.

Step 9: The target devices are connected and the network traffic is analysed using Wireshark while sending the attachments between the devices.

Step 10: The network traffic is analysed when sending the text messages using Wireshark.

texting.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	74.125.193.119	192.168.137.97	TLSv1.2	122	Application Data
2	0.036259	192.168.137.97	74.125.193.119	ICMP	150	Destination unreachable (Port unreachable)
3	1.502060	192.168.137.97	125.209.252.17	TLSv1.2	234	Application Data
4	1.545147	125.209.252.17	192.168.137.97	TCP	66	443 → 39078 [ACK] Seq=1 Ack=169 Win=8312 Len=0 TSval=120842379 TSecr=16929795
5	1.545461	125.209.252.17	192.168.137.97	TLSv1.2	143	Application Data
6	1.586573	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=78 Win=347 Len=0 TSval=16929806 TSecr=120842380
7	1.803221	125.209.252.17	192.168.137.97	TLSv1.2	137	Application Data
8	1.880409	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=149 Win=347 Len=0 TSval=16929835 TSecr=120842637
9	2.059574	125.209.252.17	192.168.137.97	TLSv1.2	291	Application Data
10	2.062424	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=374 Win=351 Len=0 TSval=16929853 TSecr=120842893
11	2.064062	125.209.252.18	192.168.137.228	TLSv1.2	319	Application Data
12	2.120973	192.168.137.97	125.209.252.17	TLSv1.2	137	Application Data
13	2.176003	192.168.137.228	125.209.252.18	TCP	66	52102 → 443 [ACK] Seq=1 Ack=254 Win=2044 Len=0 TSval=1195445138 TSecr=4239298515
14	2.197584	125.209.252.17	192.168.137.97	TCP	66	443 → 39078 [ACK] Seq=374 Ack=240 Win=8312 Len=0 TSval=120843033 TSecr=16929859
15	2.213062	192.168.137.228	125.209.252.18	TLSv1.2	222	Application Data
16	2.219174	192.168.137.228	125.209.252.18	TLSv1.2	155	Application Data
17	2.251805	125.209.252.18	192.168.137.228	TCP	66	443 → 52102 [ACK] Seq=254 Ack=157 Win=8553 Len=0 TSval=4239298703 TSecr=1195445174
18	2.262639	125.209.252.18	192.168.137.228	TCP	66	443 → 52102 [ACK] Seq=254 Ack=246 Win=8553 Len=0 TSval=4239298715 TSecr=1195445180
19	2.392678	209.85.202.157	192.168.137.97	TLSv1.2	122	Application Data
20	2.395817	192.168.137.97	209.85.202.157	ICMP	150	Destination unreachable (Port unreachable)
21	2.498135	125.209.252.18	192.168.137.228	TLSv1.2	152	Application Data
22	2.517564	125.209.252.18	192.168.137.228	TLSv1.2	188	Application Data
23	2.585425	192.168.137.228	125.209.252.18	TCP	66	52102 → 443 [ACK] Seq=246 Ack=340 Win=2046 Len=0 TSval=1195445543 TSecr=4239298951

> Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0

> Ethernet II, Src: 4e:91:80:37:1f:83 (4e:91:80:37:1f:83), Dst: da:35:c7:3d:65:63 (da:35:c7:3d:65:63)

> Internet Protocol Version 4, Src: 74.125.193.119, Dst: 192.168.137.97

> Transmission Control Protocol, Src Port: 443, Dst Port: 44499, Seq: 1, Ack: 1, Len: 56

> Transport Layer Security

Step 11: By using Wireshark, The network traffic is analysed while sending emoji.

emoji.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	74.125.193.188	192.168.137.97	TCP	66	5228 → 39545 [ACK] Seq=1 Ack=1 Win=253 Len=0 TSval=1180786202 TSecr=16979947
2	2.132186	192.168.137.97	125.209.252.17	TLSv1.2	278	Application Data, Application Data, Application Data, Application Data
3	2.175242	125.209.252.17	192.168.137.97	TCP	66	443 → 39206 [ACK] Seq=201 Ack=213 Win=9489 Len=0 TSval=4257446115 TSecr=16980160
4	2.177545	192.168.137.97	125.209.252.17	TLSv1.2	137	Application Data
5	2.227741	125.209.252.17	192.168.137.97	TCP	66	443 → 39206 [ACK] Seq=201 Ack=284 Win=9489 Len=0 TSval=4257446168 TSecr=16980166
6	2.230309	192.168.137.97	125.209.252.17	TLSv1.2	110	Application Data
7	2.267614	125.209.252.17	192.168.137.97	TCP	66	443 → 39206 [ACK] Seq=201 Ack=328 Win=9489 Len=0 TSval=4257446206 TSecr=16980172
8	2.777061	192.168.137.97	224.0.0.251	MDNS	119	Standard query 0x0001 PTR _C1E868AE._sub._googlecast._tcp.local, "QU" question PTR _CASE8412._sub._googlecast._tcp.local
9	3.884614	192.168.137.97	224.0.0.251	MDNS	119	Standard query 0x0002 PTR _C1E868AE._sub._googlecast._tcp.local, "QM" question PTR _CASE8412._sub._googlecast._tcp.local
10	4.881420	192.168.137.97	224.0.0.251	MDNS	119	Standard query 0x0003 PTR _C1E868AE._sub._googlecast._tcp.local, "QM" question PTR _CASE8412._sub._googlecast._tcp.local
11	7.881819	203.104.142.91	192.168.137.228	TLSv1.2	97	Encrypted Alert
12	7.881386	203.104.142.91	192.168.137.228	TCP	66	443 → 63454 [FIN, ACK] Seq=32 Ack=1 Win=269 Len=0 TSval=31471802 TSecr=1196582728
13	7.124092	192.168.137.228	203.104.142.91	TCP	66	63454 → 443 [ACK] Seq=1 Ack=32 Win=1025 Len=0 TSval=1196604129 TSecr=31471802
14	7.124094	192.168.137.228	203.104.142.91	TCP	66	63454 → 443 [ACK] Seq=1 Ack=33 Win=1025 Len=0 TSval=1196604129 TSecr=31471802
15	7.125311	192.168.137.228	203.104.142.91	TLSv1.2	97	Encrypted Alert
16	7.126356	192.168.137.228	203.104.142.91	TCP	66	63454 → 443 [FIN, ACK] Seq=32 Ack=33 Win=1025 Len=0 TSval=1196604131 TSecr=31471802
17	7.378730	203.104.142.91	192.168.137.228	TCP	54	443 → 63454 [RST] Seq=33 Win=0 Len=0
18	7.379028	203.104.142.91	192.168.137.228	TCP	54	443 → 63454 [RST] Seq=33 Win=0 Len=0
19	7.841316	192.168.137.97	74.125.193.103	TLSv1.2	627	Application Data
20	7.859499	74.125.193.103	192.168.137.97	TCP	66	443 → 43426 [ACK] Seq=1 Ack=562 Win=337 Len=0 TSval=2765424226 TSecr=16980731
21	7.862101	192.168.137.97	74.125.193.103	TLSv1.2	100	Application Data
22	7.876565	74.125.193.103	192.168.137.97	TCP	66	443 → 43426 [ACK] Seq=1 Ack=596 Win=337 Len=0 TSval=2765424244 TSecr=16980735
23	7.881330	74.125.193.103	192.168.137.97	TLSv1.2	265	Application Data

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

> Ethernet II, Src: 4e:91:80:37:1f:83 (4e:91:80:37:1f:83), Dst: da:35:c7:3d:65:63 (da:35:c7:3d:65:63)

> Internet Protocol Version 4, Src: 74.125.193.188, Dst: 192.168.137.97

> Transmission Control Protocol, Src Port: 5228, Dst Port: 39545, Seq: 1, Ack: 1, Len: 0

Step 12: When the target device is doing voice or video calling .The packet size is used to determine the type of calling.

calling.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.137.228	224.0.0.251	MDNS	181	Standard query 0x0000 PTR_companion-link_tcp.local, "QM" question PTR_homekit_tcp.local, "QM" question P...
2	0.000277	fe80::63:22fc:feaa::ff02::fb	ff02::fb	MDNS	201	Standard query 0x0000 PTR_companion-link_tcp.local, "QM" question PTR_homekit_tcp.local, "QM" question P...
3	1.218292	1.0.0.1	192.168.137.97	TCP	54	853 → 43130 [FIN, ACK] Seq=1 Ack=1 Win=31 Len=0
4	1.218434	1.0.0.1	192.168.137.97	TCP	54	[TCP Out-Of-Order] 853 → 43130 [FIN, ACK] Seq=1 Ack=1 Win=31 Len=0
5	1.255579	192.168.137.97	1.0.0.1	TCP	66	43130 → 853 [ACK] Seq=1 Ack=4294967266 Win=388 Len=0 SLE=1 SRE=2
6	1.255915	192.168.137.97	1.0.0.1	TCP	74	[TCP Dup ACK 5#1] 43130 → 853 [ACK] Seq=1 Ack=4294967266 Win=388 Len=0 SLE=1 SRE=2 SLE=2 SRE=2
7	1.262143	1.0.0.1	192.168.137.97	TCP	85	[TCP Retransmission] 853 → 43130 [FIN, PSH, ACK] Seq=4294967266 Ack=1 Win=31 Len=31
8	1.265111	192.168.137.97	1.0.0.1	TLSv1.2	85	Encrypted Alert
9	1.265436	192.168.137.97	1.0.0.1	TCP	54	43130 → 853 [FIN, ACK] Seq=32 Ack=2 Win=388 Len=0
10	1.282256	1.0.0.1	192.168.137.97	TCP	54	853 → 43130 [RST] Seq=2 Win=0 Len=0
11	1.283206	1.0.0.1	192.168.137.97	TCP	54	853 → 43130 [RST] Seq=2 Win=0 Len=0
12	1.906536	192.168.137.228	192.168.137.1	DNS	84	Standard query 0xc556 A_9-courier-push.apple.com
13	1.930130	192.168.137.1	192.168.137.228	DNS	203	Standard query response 0xc556 A_9-courier-push.apple.com CNAME 9.courier-push.apple.com.akadns.net CNAME gb...
14	1.935408	192.168.137.228	17.57.146.84	TCP	78	52073 → 5223 [SYN, ECN, CHR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1194560021 TSecr=0 SACK_PERM=1
15	1.949168	17.57.146.84	192.168.137.228	TCP	74	5223 → 52073 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=4230862455 TSecr=1194560...
16	1.953226	192.168.137.228	17.57.146.84	TCP	66	5223 → 52073 [ACK] Seq=1 Ack=223 Win=30080 Len=0 TSval=4230862475 TSecr=1194560038
17	1.953553	192.168.137.228	17.57.146.84	TLSv1.2	288	Client Hello
18	1.970638	17.57.146.84	192.168.137.228	TCP	66	5223 → 52073 [ACK] Seq=1 Ack=223 Win=30080 Len=0 TSval=4230862475 TSecr=1194560038
19	1.972116	17.57.146.84	192.168.137.228	TLSv1.2	1514	Server Hello
20	1.973086	17.57.146.84	192.168.137.228	TCP	1514	5223 → 52073 [ACK] Seq=1449 Ack=223 Win=30080 Len=1448 TSval=4230862476 TSecr=1194560038 [TCP segment of a r...
21	1.973297	17.57.146.84	192.168.137.228	TLSv1.2	594	Certificate, Server Key Exchange, Server Hello Done
22	1.975822	192.168.137.228	17.57.146.84	TCP	66	52073 → 5223 [ACK] Seq=223 Ack=2897 Win=128832 Len=0 TSval=1194560061 TSecr=4230862476
23	1.975823	192.168.137.228	17.57.146.84	TCP	66	52073 → 5223 [ACK] Seq=223 Ack=3475 Win=128320 Len=0 TSval=1194560061 TSecr=4230862476

> Frame 1: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits) on interface 0

> Ethernet II, Src: Apple_66:d7:c0 (74:b5:87:66:d7:c0), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)

> Internet Protocol Version 4, Src: 192.168.137.228, Dst: 224.0.0.251

> User Datagram Protocol, Src Port: 5353, Dst Port: 5353

> Multicast Domain Name System (query)

Step 13: Two target devices are Android and iOS . Signature found for the attachments sent between two devices.

calling.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.137.97	192.168.137.1	DNS	90	Standard query 0xc123 A_android.prod.cloud.netflix.com
2	0.014200	192.168.137.1	192.168.137.97	DNS	209	Standard query response 0xc123 A_android.prod.cloud.netflix.com CNAME prod.cloud.geo.netflix.com CNAME prod...
3	1.531706	192.168.137.97	74.125.193.95	TCP	74	37508 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=17086093 TSecr=0 WS=256
4	1.549488	74.125.193.95	192.168.137.97	TCP	74	443 → 37508 [SYN, ACK] Seq=0 Ack=1 Win=62392 Len=0 MSS=1430 SACK_PERM=1 TSval=130405403 TSecr=17086093 WS=256
5	1.551602	192.168.137.97	74.125.193.95	ICMP	102	Destination unreachable (Port unreachable)
6	1.849068	74.125.193.95	192.168.137.97	TCP	74	[TCP Retransmission] 443 → 37508 [SYN, ACK] Seq=0 Ack=1 Win=62392 Len=0 MSS=1430 SACK_PERM=1 TSval=130405703...
7	1.920961	192.168.137.97	74.125.193.95	ICMP	102	Destination unreachable (Port unreachable)
8	3.119289	192.168.137.97	224.0.0.251	MDNS	103	Standard query 0x0004 PTR_C1EB68AE_sub_googlecast_tcp.local, "QM" question PTR_googlecast_tcp.local, "
9	3.915764	74.125.193.95	192.168.137.97	TCP	74	[TCP Retransmission] 443 → 37508 [SYN, ACK] Seq=0 Ack=1 Win=62392 Len=0 MSS=1430 SACK_PERM=1 TSval=130407703...
10	3.971167	192.168.137.97	74.125.193.95	ICMP	102	Destination unreachable (Port unreachable)
11	4.573618	192.168.137.97	125.209.252.17	TLSv1.2	650	Application Data, Application Data, Application Data, Application Data
12	4.614759	125.209.252.17	192.168.137.97	TCP	66	443 → 40052 [ACK] Seq=1 Ack=585 Win=8068 Len=0 TSval=4258874100 TSecr=17086396
13	4.863335	125.209.252.17	192.168.137.97	TLSv1.2	159	Application Data
14	4.865933	125.209.252.17	192.168.137.97	TLSv1.2	207	Application Data
15	4.869023	125.209.252.17	192.168.137.97	TLSv1.2	147	Application Data
16	4.890831	192.168.137.97	125.209.252.17	TCP	66	40052 → 443 [ACK] Seq=585 Ack=94 Win=347 Len=0 TSval=17086430 TSecr=4258874349
17	4.891186	192.168.137.97	125.209.252.17	TCP	66	40052 → 443 [ACK] Seq=585 Ack=235 Win=351 Len=0 TSval=17086430 TSecr=4258874352
18	4.891187	192.168.137.97	125.209.252.17	TCP	66	40052 → 443 [ACK] Seq=585 Ack=316 Win=351 Len=0 TSval=17086430 TSecr=4258874355
19	4.899570	192.168.137.97	125.209.252.14	TLSv1.2	577	Application Data
20	4.899904	192.168.137.97	125.209.252.14	TLSv1.2	97	Encrypted Alert
21	4.900851	192.168.137.97	125.209.252.14	TCP	74	38648 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1 TSval=17086431 TSecr=0 WS=256
22	4.941489	125.209.252.14	192.168.137.97	TCP	54	443 → 38522 [RST] Seq=1 Win=0 Len=0
23	4.941708	125.209.252.14	192.168.137.97	TCP	54	443 → 38522 [RST] Seq=1 Win=0 Len=0

> Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0

> Ethernet II, Src: da:35:c7:3d:65:63 (da:35:c7:3d:65:63), Dst: 4e:91:80:37:1f:83 (4e:91:80:37:1f:83)

> Internet Protocol Version 4, Src: 192.168.137.97, Dst: 192.168.137.1

> User Datagram Protocol, Src Port: 34972, Dst Port: 53

> Domain Name System (query)

Step 14: Signature analysed for the emoji

The screenshot shows a Wireshark interface with a list of network packets. The following table represents the data visible in the packet list pane:

No.	Time	Source	Destination	Protocol	Length	Info
572	88.297888	125.209.252.17	192.168.137.97	TLSv1.2	162	Application Data
573	88.304180	125.209.252.17	192.168.137.228	TCP	66	443 → 52116 [ACK] Seq=3051 Ack=2299 Win=14398 Len=0 TSval=4257508994 TSecr=1196146482
574	88.357165	192.168.137.97	125.209.252.17	TLSv1.2	137	Application Data
575	88.402417	125.209.252.17	192.168.137.97	TCP	66	443 → 39320 [ACK] Seq=3527 Ack=3166 Win=32976 Len=0 TSval=4257498012 TSecr=16987985
576	83.405797	192.168.137.228	192.168.137.1	DHCP	342	DHCP Request - Transaction ID 0xee2dd0db
577	83.417552	192.168.137.1	192.168.137.228	DHCP	344	DHCP ACK - Transaction ID 0xee2dd0db
578	88.023307	192.168.137.97	224.0.0.251	MDNS	110	Standard query 0x0010 PTR_C1E688AE_sub_googlecast_tcp.local "Q" question PTR_CASE8412_sub_googlecas...
579	88.432818	192.168.137.97	125.209.252.17	TLSv1.2	162	Application Data
580	88.471621	125.209.252.17	192.168.137.97	TCP	66	443 → 39320 [ACK] Seq=3527 Ack=3262 Win=32976 Len=0 TSval=4257498080 TSecr=16988789
581	88.471924	125.209.252.17	192.168.137.97	TLSv1.2	143	Application Data
582	88.511483	192.168.137.97	125.209.252.17	TCP	66	39320 → 443 [ACK] Seq=3262 Ack=3604 Win=95232 Len=0 TSval=16988800 TSecr=4257498080
583	88.721572	125.209.252.17	192.168.137.97	TLSv1.2	137	Application Data
584	88.737314	192.168.137.97	125.209.252.17	TCP	66	39320 → 443 [ACK] Seq=3262 Ack=3675 Win=95232 Len=0 TSval=16988822 TSecr=4257498332
585	88.977615	125.209.252.17	192.168.137.97	TLSv1.2	267	Application Data
586	88.982116	125.209.252.17	192.168.137.228	TLSv1.2	288	Application Data
587	89.027921	192.168.137.97	224.0.0.251	MDNS	119	Standard query 0x0011 PTR_C1E688AE_sub_googlecast_tcp.local, "Q" question PTR_CASE8412_sub_googlecas...
588	89.027725	192.168.137.97	125.209.252.17	TCP	66	39320 → 443 [ACK] Seq=3262 Ack=3876 Win=96256 Len=0 TSval=16988851 TSecr=4257498588
589	89.036984	192.168.137.97	125.209.252.17	TLSv1.2	137	Application Data
590	89.044818	192.168.137.228	125.209.252.17	TCP	66	52116 → 443 [ACK] Seq=2299 Ack=3273 Win=2044 Len=0 TSval=1196155259 TSecr=4257517671
591	89.076941	192.168.137.228	125.209.252.17	TLSv1.2	208	Application Data
592	89.081994	192.168.137.228	125.209.252.17	TLSv1.2	155	Application Data
593	89.116728	125.209.252.17	192.168.137.228	TCP	66	443 → 52116 [ACK] Seq=3273 Ack=2441 Win=14787 Len=0 TSval=4257517806 TSecr=1196155290
594	89.120027	125.209.252.17	192.168.137.97	TCP	66	443 → 39320 [ACK] Seq=3876 Ack=3333 Win=32976 Len=0 TSval=4257498731 TSecr=16988852

Annotations in the image include red boxes around packets 573, 579, and 580, and a text label 'signature for start typing emoji' pointing to packet 574. The packet details pane shows the structure of the first packet (Frame 1):

- Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: 4e:91:80:37:1f:83 (4e:91:80:37:1f:83), Dst: da:35:c7:3d:65:63 (da:35:c7:3d:65:63)
- Internet Protocol Version 4, Src: 74.125.193.188, Dst: 192.168.137.97
- Transmission Control Protocol, Src Port: 5228, Dst Port: 39545, Seq: 1, Ack: 1, Len: 0

The packet bytes pane shows the raw hex and ASCII data for the first two packets:

```

0000 da 35 c7 3d 65 63 4e 91 80 37 1f 83 08 00 45 00 5-ecN-7...E-
0018 00 34 3f e9 00 00 77 06 ad 97 4a 7d c1 bc c0 a8 -4?..w..:}....
  
```

Step 15: Signature found for the text messages.

The screenshot shows a Wireshark capture of network traffic. The packet list pane contains the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	74.125.193.119	192.168.137.97	TLSv1.2	122	Application Data
0	0.036259	192.168.137.97	74.125.193.119	ICMP	150	Destination unreachable (Port unreachable)
3	1.502060	192.168.137.97	125.209.252.17	TLSv1.2	234	Application Data
4	1.545147	125.209.252.17	192.168.137.97	TCP	66	443 → 39078 [ACK] Seq=1 Ack=169 Win=8312 Len=0 TSval=120842379 TSecr=16929795
5	1.545461	125.209.252.17	192.168.137.97	TLSv1.2	143	Application Data
6	1.586573	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=78 Win=347 Len=0 TSval=16929806 TSecr=120842380
7	1.803221	125.209.252.17	192.168.137.97	TLSv1.2	137	Application Data
8	1.808409	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=149 Win=347 Len=0 TSval=16929835 TSecr=120842637
9	2.059574	125.209.252.17	192.168.137.97	TLSv1.2	291	Application Data
10	2.062424	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=374 Win=351 Len=0 TSval=16929853 TSecr=120842893
11	2.064062	125.209.252.18	192.168.137.228	TLSv1.2	319	Application Data
12	2.120973	192.168.137.97	125.209.252.17	TLSv1.2	137	Application Data
13	2.176003	192.168.137.228	125.209.252.18	TCP	66	52102 → 443 [ACK] Seq=1 Ack=254 Win=2044 Len=0 TSval=1195445138 TSecr=4239298515
14	2.197704	125.209.252.17	192.168.137.97	TCP	66	443 → 39078 [ACK] Seq=374 Ack=246 Win=8553 Len=0 TSval=120842637 TSecr=16929795
15	2.213062	192.168.137.228	125.209.252.18	TLSv1.2	222	Application Data
16	2.219174	192.168.137.228	125.209.252.18	TLSv1.2	155	Application Data
17	2.251805	125.209.252.18	192.168.137.228	TCP	66	443 → 52102 [ACK] Seq=254 Ack=157 Win=8553 Len=0 TSval=4239298703 TSecr=1195445174
18	2.262639	125.209.252.18	192.168.137.228	TCP	66	443 → 52102 [ACK] Seq=254 Ack=246 Win=8553 Len=0 TSval=4239298715 TSecr=1195445180
19	2.392678	209.85.202.157	192.168.137.97	TLSv1.2	122	Application Data
20	2.395817	192.168.137.97	209.85.202.157	ICMP	150	Destination unreachable (Port unreachable)
21	2.498135	125.209.252.18	192.168.137.228	TLSv1.2	152	Application Data
22	2.517564	125.209.252.18	192.168.137.228	TLSv1.2	188	Application Data
23	2.585425	192.168.137.228	125.209.252.18	TCP	66	52102 → 443 [ACK] Seq=246 Ack=340 Win=2046 Len=0 TSval=1195445543 TSecr=4239298951

Red boxes highlight packets 6, 7, 8, 9, 12, and 13. A red annotation on the right says: "signature exacts when user sends the text".

The packet details pane for packet 6 shows:

- Frame 5: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface 0
- Ethernet II, Src: 4e:91:80:37:1f:83 (4e:91:80:37:1f:83), Dst: da:35:c7:3d:65:63 (da:35:c7:3d:65:63)
- Internet Protocol Version 4, Src: 125.209.252.17, Dst: 192.168.137.97
- Transmission Control Protocol, Src Port: 443, Dst Port: 39078, Seq: 1, Ack: 169, Len: 77
- Transport Layer Security

The packet bytes pane shows the raw data: 0000 da 35 c7 3d 65 63 4e 91 80 37 1f 83 08 00 45 00 0018 00 81 4e b8 40 00 31 06 36 42 7d d1 fc 11 c0 a8

Step 16: Signature extract from the calling (voice and video)

The screenshot shows a Wireshark capture of network traffic, identical to Step 15. The packet list pane contains the following entries:

No.	Time	Source	Destination	Protocol	Length	Info
0	0.000000	74.125.193.119	192.168.137.97	TLSv1.2	122	Application Data
0	0.036259	192.168.137.97	74.125.193.119	ICMP	150	Destination unreachable (Port unreachable)
3	1.502060	192.168.137.97	125.209.252.17	TLSv1.2	234	Application Data
4	1.545147	125.209.252.17	192.168.137.97	TCP	66	443 → 39078 [ACK] Seq=1 Ack=169 Win=8312 Len=0 TSval=120842379 TSecr=16929795
5	1.545461	125.209.252.17	192.168.137.97	TLSv1.2	143	Application Data
6	1.586573	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=78 Win=347 Len=0 TSval=16929806 TSecr=120842380
7	1.803221	125.209.252.17	192.168.137.97	TLSv1.2	137	Application Data
8	1.808409	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=149 Win=347 Len=0 TSval=16929835 TSecr=120842637
9	2.059574	125.209.252.17	192.168.137.97	TLSv1.2	291	Application Data
10	2.062424	192.168.137.97	125.209.252.17	TCP	66	39078 → 443 [ACK] Seq=169 Ack=374 Win=351 Len=0 TSval=16929853 TSecr=120842893
11	2.064062	125.209.252.18	192.168.137.228	TLSv1.2	319	Application Data
12	2.120973	192.168.137.97	125.209.252.17	TLSv1.2	137	Application Data
13	2.176003	192.168.137.228	125.209.252.18	TCP	66	52102 → 443 [ACK] Seq=1 Ack=254 Win=2044 Len=0 TSval=1195445138 TSecr=4239298515
14	2.197704	125.209.252.17	192.168.137.97	TCP	66	443 → 39078 [ACK] Seq=374 Ack=246 Win=8553 Len=0 TSval=120842637 TSecr=16929795
15	2.213062	192.168.137.228	125.209.252.18	TLSv1.2	222	Application Data
16	2.219174	192.168.137.228	125.209.252.18	TLSv1.2	155	Application Data
17	2.251805	125.209.252.18	192.168.137.228	TCP	66	443 → 52102 [ACK] Seq=254 Ack=157 Win=8553 Len=0 TSval=4239298703 TSecr=1195445174
18	2.262639	125.209.252.18	192.168.137.228	TCP	66	443 → 52102 [ACK] Seq=254 Ack=246 Win=8553 Len=0 TSval=4239298715 TSecr=1195445180
19	2.392678	209.85.202.157	192.168.137.97	TLSv1.2	122	Application Data
20	2.395817	192.168.137.97	209.85.202.157	ICMP	150	Destination unreachable (Port unreachable)
21	2.498135	125.209.252.18	192.168.137.228	TLSv1.2	152	Application Data
22	2.517564	125.209.252.18	192.168.137.228	TLSv1.2	188	Application Data
23	2.585425	192.168.137.228	125.209.252.18	TCP	66	52102 → 443 [ACK] Seq=246 Ack=340 Win=2046 Len=0 TSval=1195445543 TSecr=4239298951

Red boxes highlight packets 6, 7, 8, 9, 12, and 13. A red annotation on the right says: "signature exacts when user sends the text".

The packet details pane for packet 6 shows:

- Frame 5: 143 bytes on wire (1144 bits), 143 bytes captured (1144 bits) on interface 0
- Ethernet II, Src: 4e:91:80:37:1f:83 (4e:91:80:37:1f:83), Dst: da:35:c7:3d:65:63 (da:35:c7:3d:65:63)
- Internet Protocol Version 4, Src: 125.209.252.17, Dst: 192.168.137.97
- Transmission Control Protocol, Src Port: 443, Dst Port: 39078, Seq: 1, Ack: 169, Len: 77
- Transport Layer Security

The packet bytes pane shows the raw data: 0000 da 35 c7 3d 65 63 4e 91 80 37 1f 83 08 00 45 00 0018 00 81 4e b8 40 00 31 06 36 42 7d d1 fc 11 c0 a8

Step 17: Signature extract from attachment

The screenshot shows a Wireshark capture of a TLS handshake and subsequent application data. A red box highlights a specific TCP segment (No. 40) with the following details:

- Packet No.:** 40
- Time:** 5.121484
- Source:** 192.168.137.97
- Destination:** 125.209.252.14
- Protocol:** TCP
- Length:** 443
- Info:** Seq=3883 Ack=855 Win=16896 Len=0 TSval=281440812 TSecr=17086446

The packet details pane for this segment shows:

- Ethernet II, Src:** da:35:c7:3d:65:63 (da:35:c7:3d:65:63), Dst: 4e:91:80:37:1f:83 (4e:91:80:37:1f:83)
- Internet Protocol Version 4, Src:** 192.168.137.97, Dst: 125.209.252.14
- Transmission Layer Protocol, Src Port:** 38648, Dst Port: 443, Seq: 218, Ack: 3332, Len: 126
- Transport Layer Security**

The packet bytes pane shows the raw hex data of the signature:

```

0000 4e 91 80 37 1f 83 da 35 c7 3d 65 63 08 00 45 00  N...S...E.
0018 00 b2 91 d1 40 00 40 06 e4 8a c0 a8 89 61 7d d1  ...@.....a
    
```