

# NETWORK TRAFFIC ANALYSIS – SOC PERSPECTIVE

## Objective of the Analysis

To perform real-time network traffic monitoring and analysis using live packet capture in order to identify, validate, and interpret encrypted communication behavior and potential security events from a Security Operations Center (SOC) perspective.

## Analysis Aims To :

- Monitor live network traffic to observe real-time communication patterns
- Analyze encrypted traffic including HTTPS (TCP/443) and QUIC (UDP/443)
- Detect abnormal behaviors such as connection resets, timing anomalies, and high-frequency access attempts
- Validate the presence or absence of SSH-based attack activity on port 22
- Convert live packet observations into SOC-ready findings and risk assessments

## Tools Used:

Wireshark

## Dataset:

Live Wi-Fi Network Capture

## Filter: tcp

### Observation:

TCP traffic dominates the capture, mainly over destination port 443.

### Reason:

Most web applications use TCP as the transport layer for HTTPS.

### Conclusion:

The host is actively communicating with external web services using standard TCP-based HTTPS.

Capturing from Wi-Fi						
No.	Time	Source	Destination	Protocol	Length	Info
5	0.065905	192.168.1.3	100.30.98.72	TCP	66	58318 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9	0.357283	100.30.98.72	192.168.1.3	TCP	66	443 → 58318 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1250 SACK_PERM WS=256
10	0.357473	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
11	0.358342	192.168.1.3	100.30.98.72	TLSv1.2	398	Client Hello (SNI=capi.grammarrly.com)
18	0.658265	100.30.98.72	192.168.1.3	TCP	54	443 → 58318 [ACK] Seq=1 Ack=345 Win=28160 Len=0
19	0.658265	100.30.98.72	192.168.1.3	TLSv1.2	1304	Server Hello
20	0.658265	100.30.98.72	192.168.1.3	TCP	1304	443 → 58318 [ACK] Seq=1251 Ack=345 Win=28160 Len=1250 [TCP PDU reassembled in 23]
21	0.658265	100.30.98.72	192.168.1.3	TCP	1304	443 → 58318 [ACK] Seq=2501 Ack=345 Win=28160 Len=1250 [TCP PDU reassembled in 23]
22	0.658443	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=3751 Win=65280 Len=0
23	0.659369	100.30.98.72	192.168.1.3	TLSv1.2	574	Certificate, Server Key Exchange, Server Hello Done
24	0.659434	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=4271 Win=64768 Len=0
25	0.662018	192.168.1.3	100.30.98.72	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
26	0.866139	192.168.1.3	192.168.1.4	TCP	164	49712 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=250 Len=110 [TCP PDU reassembled in 2912]
27	0.869312	192.168.1.4	192.168.1.3	TCP	164	8009 → 49712 [PSH, ACK] Seq=1 Ack=111 Win=1170 Len=110 [TCP PDU reassembled in 2913]
28	0.914233	192.168.1.3	192.168.1.4	TCP	54	49712 → 8009 [ACK] Seq=111 Ack=111 Win=255 Len=0
29	0.957197	100.30.98.72	192.168.1.3	TCP	54	443 → 58318 [ACK] Seq=4271 Ack=438 Win=28160 Len=0
30	0.957197	100.30.98.72	192.168.1.3	TLSv1.2	258	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
31	0.959644	192.168.1.3	100.30.98.72	TCP	1304	58318 → 443 [ACK] Seq=438 Ack=4475 Win=64768 Len=1250 [TCP PDU reassembled in 321]
> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{917DF297-C000-4A0D-BE8C-000000000000						
> Ethernet II, Src: Intel_77:be:dd (b0:47:e9:77:be:dd), Dst: ZyxelCommuni_df:da:e8 (30:bd:13:df:da:e8)						
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 100.30.98.72						
> Transmission Control Protocol, Src Port: 58318, Dst Port: 443, Seq: 0, Len: 0						
0000 30 bd 13 df da e8 b0 47 e9 77 be dd 08 00 45 00 0-----G -w----E-						
0010 00 34 89 0b 40 00 80 06 00 00 c0 a8 01 03 64 1e -4- @-----d-						
0020 62 48 e3 ce 01 bb 0e 17 08 72 00 00 00 00 80 02 bH-----r-----						
0030 ff ff 88 38 00 00 02 04 05 b4 01 03 03 08 01 01 ---8-----						
0040 04 02 .....						

## Filter: udp.port == 443

### Observation:

Significant UDP traffic observed on port 443 using the QUIC protocol.

### Reason:

Modern applications use QUIC (HTTP/3) for faster encrypted communication.

### Conclusion:

The host is communicating with services that support QUIC-based HTTPS.

The screenshot shows the Wireshark interface with the following details:

- File menu:** Capturing from Wi-Fi, File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help.
- Toolbar:** Standard capture and analysis tools.
- Search bar:** udp.port == 443.
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info.
- Table Data:** A list of captured frames. For example, frame 1007 is a QUIC Protected Payload (KPO) from source 2404:6800:4009:802:: to destination 2401:4900:8f57:3ef5::, with a length of 182 bytes. Frame 1008 is a QUIC Initial frame (DCID=d77187232489398c) with a length of 1292 bytes.
- Frame Details:** Shows the raw hex and ASCII data for frame 1007 and 1008.
- Frame List:** A detailed list of captured frames, including their number, time, source, destination, protocol, length, and a summary of the frame content.
- Bottom Status Bar:** wireshark\_Wi-FiQQ3MH3.pcapng, Packets: 101264 · Displayed: 11568 (11.4%), Profile: Default.

## Filter: ip.addr == 192.168.1.3

### Observation:

All displayed packets involve the internal host 192.168.1.3.

### Reason:

This filter isolates traffic generated or received by the target endpoint.

### Conclusion:

The analysis is focused on a single internal system's network behavior.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.3

No.	Time	Source	Destination	Protocol	Length	Info
5	0.065905	192.168.1.3	100.30.98.72	TCP	66	58318 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9	0.357283	100.30.98.72	192.168.1.3	TCP	66	443 → 58318 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1250 SACK_PERM WS=256
10	0.357473	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
11	0.358342	192.168.1.3	100.30.98.72	TLSv1.2	398	Client Hello (SNI=capi.grammarly.com)
18	0.658265	100.30.98.72	192.168.1.3	TCP	54	443 → 58318 [ACK] Seq=1 Ack=345 Win=28160 Len=0
19	0.658265	100.30.98.72	192.168.1.3	TLSv1.2	1304	Server Hello
20	0.658265	100.30.98.72	192.168.1.3	TCP	1304	443 → 58318 [ACK] Seq=1251 Ack=345 Win=28160 Len=1250 [TCP PDU reassembled in 23]
21	0.658265	100.30.98.72	192.168.1.3	TCP	1304	443 → 58318 [ACK] Seq=2501 Ack=345 Win=28160 Len=1250 [TCP PDU reassembled in 23]
22	0.658443	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=3751 Win=65280 Len=0
23	0.659369	100.30.98.72	192.168.1.3	TLSv1.2	574	Certificate, Server Key Exchange, Server Hello Done
24	0.659434	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=4271 Win=64768 Len=0
25	0.662018	192.168.1.3	100.30.98.72	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
26	0.866139	192.168.1.3	192.168.1.4	TCP	164	49712 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=250 Len=110 [TCP PDU reassembled in 2912]
27	0.869312	192.168.1.4	192.168.1.3	TCP	164	8009 → 49712 [PSH, ACK] Seq=1 Ack=111 Win=1170 Len=110 [TCP PDU reassembled in 2913]
28	0.914233	192.168.1.3	192.168.1.4	TCP	54	49712 → 8009 [ACK] Seq=111 Ack=111 Win=255 Len=0
29	0.957197	100.30.98.72	192.168.1.3	TCP	54	443 → 58318 [ACK] Seq=4271 Ack=438 Win=28160 Len=0
30	0.957197	100.30.98.72	192.168.1.3	TLSv1.2	258	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
31	0.959644	192.168.1.3	100.30.98.72	TCP	1304	58318 → 443 [ACK] Seq=438 Ack=4475 Win=64768 Len=1250 [TCP PDU reassembled in 321]

> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{917DF297-C0  
> Ethernet II, Src: Intel\_77:be:dd (b0:47:e9:77:be:dd), Dst: ZyxelCommuni\_df:da:e8 (30:bd:13:df:da:e8)  
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 100.30.98.72  
> Transmission Control Protocol, Src Port: 58318, Dst Port: 443, Seq: 0, Len: 0

0000	30	bd	13	df	da	e8	b0	47	e9	77	be	dd	08	00	45	00	0.....G -w----E-
0010	00	34	89	0b	40	00	80	06	00	00	c0	a8	01	03	64	1e	:4--@.....d-
0020	62	48	e3	ce	01	bb	0e	17	08	72	00	00	00	80	02	bH-----r-----	
0030	ff	ff	88	38	00	00	02	04	05	b4	01	03	03	08	01	...8-----	
0040	04	02														..	

\_packets: 99785 · Displayed: 54697 (54.8%) | Profile: Default

## Filter: ip.addr == 192.168.1.3 and tcp.port == 443

### Observation:

TLS 1.2 handshake packets (Client Hello, Server Hello, Certificate) are visible.

### Reason:

TLS negotiation occurs before encrypted data transfer begins.

### Conclusion:

Secure HTTPS sessions are being properly established by the internal host.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.3 and tcp.port == 443

No.	Time	Source	Destination	Protocol	Length	Info
5	0.065905	192.168.1.3	100.30.98.72	TCP	66	58318 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9	0.357283	100.30.98.72	192.168.1.3	TCP	66	443 → 58318 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1250 SACK_PERM WS=256
10	0.357473	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
11	0.358342	192.168.1.3	100.30.98.72	TLSv1.2	398	Client Hello (SNI=capi.grammarly.com)
18	0.658265	100.30.98.72	192.168.1.3	TCP	54	443 → 58318 [ACK] Seq=1 Ack=345 Win=28160 Len=0
19	0.658265	100.30.98.72	192.168.1.3	TLSv1.2	1304	Server Hello
20	0.658265	100.30.98.72	192.168.1.3	TCP	1304	443 → 58318 [ACK] Seq=1251 Ack=345 Win=28160 Len=1250 [TCP PDU reassembled in 23]
21	0.658265	100.30.98.72	192.168.1.3	TCP	1304	443 → 58318 [ACK] Seq=2501 Ack=345 Win=28160 Len=1250 [TCP PDU reassembled in 23]
22	0.658443	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=3751 Win=65280 Len=0
23	0.659369	100.30.98.72	192.168.1.3	TLSv1.2	574	Certificate, Server Key Exchange, Server Hello Done
24	0.659434	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=4271 Win=64768 Len=0
25	0.662018	192.168.1.3	100.30.98.72	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
29	0.957197	100.30.98.72	192.168.1.3	TCP	54	443 → 58318 [ACK] Seq=4271 Ack=438 Win=28160 Len=0
30	0.957197	100.30.98.72	192.168.1.3	TLSv1.2	258	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
31	0.959644	192.168.1.3	100.30.98.72	TCP	1304	58318 → 443 [ACK] Seq=438 Ack=4475 Win=64768 Len=1250 [TCP PDU reassembled in 32]
32	0.959644	192.168.1.3	100.30.98.72	TLSv1.2	199	Application Data
33	1.262796	100.30.98.72	192.168.1.3	TCP	54	443 → 58318 [ACK] Seq=4475 Ack=1833 Win=33024 Len=0
34	1.277897	100.30.98.72	192.168.1.3	TLSv1.2	718	Application Data

> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{917DF297-C0  
> Ethernet II, Src: Intel\_77:be:dd (b0:47:e9:77:be:dd), Dst: ZyxelCommuni\_df:da:e8 (30:bd:13:df:da:e8)  
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 100.30.98.72  
> Transmission Control Protocol, Src Port: 58318, Dst Port: 443, Seq: 0, Len: 0

0000	30	bd	13	df	da	e8	b0	47	e9	77	be	dd	08	00	45	00	0.....G-w....E-
0010	00	34	89	0b	40	00	80	06	00	00	c0	a8	01	03	64	1e	-4...@...d
0020	62	48	e3	ce	01	bb	0e	17	08	72	00	00	00	80	02	bH.....r....	
0030	ff	ff	88	38	00	00	02	04	05	b4	01	03	03	08	01	01	...8.....
0040	04	02														..	

\_packets: 101860 · Displayed: 32553 (32.0%)

Profile: Default

## Filter: ip.dst != 192.168.0.0/16 and ip.dst != 10.0.0.0/8

### **Observation:**

Traffic is directed to public IP addresses outside private network ranges.

### **Reason:**

The host is communicating with external internet-based services.

### **Conclusion:**

Outbound internet access is active and functioning as expected.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst != 192.168.0.0/16 and ip.dst != 10.0.0.0/8

No.	Time	Source	Destination	Protocol	Length	Info
5	0.065905	192.168.1.3	100.30.98.72	TCP	66	58318 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
10	0.357473	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
11	0.358342	192.168.1.3	100.30.98.72	TLSv1.2	398	Client Hello (SNI=capi.grammarly.com)
22	0.658443	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=3751 Win=65280 Len=0
24	0.659434	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=345 Ack=4271 Win=64768 Len=0
25	0.662018	192.168.1.3	100.30.98.72	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
31	0.959644	192.168.1.3	100.30.98.72	TCP	1304	58318 → 443 [ACK] Seq=438 Ack=4475 Win=64768 Len=1250 [TCP PDU reassembled in 32]
32	0.959644	192.168.1.3	100.30.98.72	TLSv1.2	199	Application Data
35	1.293136	192.168.1.3	100.30.98.72	TLSv1.2	1017	Application Data
38	1.705968	192.168.1.3	100.30.98.72	TCP	54	58318 → 443 [ACK] Seq=2796 Ack=5793 Win=64768 Len=0
72	5.858322	192.168.1.3	172.188.155.25	TLSv1.2	120	Application Data
740	14.390785	192.168.1.3	108.159.61.96	TCP	54	53514 → 443 [ACK] Seq=1 Ack=41 Win=255 Len=0
741	14.391389	192.168.1.3	108.159.61.96	TCP	54	53514 → 443 [FIN, ACK] Seq=1 Ack=41 Win=255 Len=0
745	14.408117	192.168.1.3	142.250.207.226	QUIC	1292	Initial, DCID=814d3e3c371c707e, PKN: 1, CRYPTO, CRYPTO, PING, PING, CRYPTO
746	14.408313	192.168.1.3	142.250.207.226	QUIC	1292	Initial, DCID=814d3e3c371c707e, PKN: 2, PING, PING, PING, PING, CRYPTO
747	14.410636	192.168.1.3	142.250.207.226	QUIC	124	0-RTT, DCID=814d3e3c371c707e
748	14.411014	192.168.1.3	142.250.207.226	QUIC	928	0-RTT, DCID=814d3e3c371c707e
776	14.467352	192.168.1.3	142.250.207.226	QUIC	120	Handshake. DCID=e14d3e3c371c707e

> Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{917DF297-C0  
> Ethernet II, Src: Intel\_77:be:dd (b0:47:e9:77:be:dd), Dst: ZyxelCommuni\_df:da:e8 (30:bd:13:df:da:e8)  
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 100.30.98.72  
> Transmission Control Protocol, Src Port: 58318, Dst Port: 443, Seq: 0, Len: 0

0000	30	bd	13	df	da	e8	b0	47	e9	77	be	dd	08	00	45	00	0.....G-w-E-
0010	00	34	89	0b	40	00	80	06	00	00	c0	a8	01	03	64	1e	-4-@-----d-
0020	62	48	e3	ce	01	bb	0e	17	08	72	00	00	00	80	02	bH-----r-----	
0030	ff	ff	88	38	00	00	02	04	05	b4	01	03	03	08	01	01	...8-----
0040	04	02														..	

\_packets: 102281 · Displayed: 11855 (11.6%)

Profile: Default

## Filter: tcp.flags.reset == 1

### Observation:

Multiple TCP RST packets observed, primarily on port 443 connections.

### Reason:

Connections were abruptly terminated by either client or server.

### Conclusion:

Session termination behavior is present and appears non-malicious.

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.reset == 1

No.	Time	Source	Destination	Protocol	Length	Info
1412	24.056384	192.168.1.3	35.168.28.131	TCP	54	53926 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1468	25.849812	20.189.173.4	192.168.1.3	TCP	54	443 → 58315 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
2977	36.449671	2401:4900:8f57:3ef5...	2001:4860:4802:34::...	TCP	74	53489 → 443 [RST, ACK] Seq=2193 Ack=6962 Win=0 Len=0
4709	52.082871	192.168.1.3	45.133.44.23	TCP	54	63915 → 443 [RST, ACK] Seq=1828 Ack=2501 Win=0 Len=0
4728	52.112409	192.168.1.3	45.133.44.23	TCP	54	49554 → 443 [RST, ACK] Seq=1876 Ack=3457 Win=0 Len=0
4759	52.124966	192.168.1.3	45.133.44.23	TCP	54	52033 → 443 [RST, ACK] Seq=1732 Ack=3154 Win=0 Len=0
6947	53.232791	192.168.1.3	136.243.90.144	TCP	54	57025 → 443 [RST, ACK] Seq=1726 Ack=1251 Win=0 Len=0
7027	53.271587	192.168.1.3	45.133.44.23	TCP	54	58478 → 443 [RST, ACK] Seq=1732 Ack=2501 Win=0 Len=0
8345	55.367299	2401:4900:8f57:3ef5...	2a02:6ea0:d100::29	TCP	74	60071 → 443 [RST, ACK] Seq=1730 Ack=2461 Win=0 Len=0
8688	55.990223	2401:4900:8f57:3ef5...	2404:6800:4009:807::	TCP	74	62137 → 443 [RST, ACK] Seq=1833 Ack=9761 Win=0 Len=0
9592	59.483659	45.144.148.181	192.168.1.3	TCP	54	443 → 56768 [RST] Seq=3182 Win=0 Len=0
18039	75.765332	79.127.170.197	192.168.1.3	TCP	54	443 → 62279 [RST, ACK] Seq=3211 Ack=1941 Win=64512 Len=0
18040	75.767138	79.127.170.197	192.168.1.3	TCP	54	443 → 62279 [RST] Seq=3211 Win=0 Len=0
18042	75.767138	79.127.170.197	192.168.1.3	TCP	54	443 → 62279 [RST] Seq=3211 Win=0 Len=0
25758	86.469477	192.168.1.3	98.89.159.84	TCP	54	53929 → 443 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
25901	86.556430	192.168.1.3	98.87.105.159	TCP	54	61857 → 443 [RST, ACK] Seq=1 Ack=33 Win=0 Len=0
29704	97.479467	192.168.1.3	142.250.192.78	TCP	54	52111 → 443 [RST, ACK] Seq=1908 Ack=8893 Win=0 Len=0
29707	97.479698	192.168.1.3	142.250.192.78	TCP	54	49570 → 443 [RST, ACK] Seq=1812 Ack=8893 Win=0 Len=0

> Frame 1412: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPFE\_{917DF297-0000-0000-0000-000000000000  
> Ethernet II, Src: Intel\_77:be:dd (b0:47:e9:77:be:dd), Dst: ZyxelCommuni\_df:da:e8 (30:bd:13:df:da:e8)  
> Internet Protocol Version 4, Src: 192.168.1.3, Dst: 35.168.28.131  
> Transmission Control Protocol, Src Port: 53926, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000	30	bd	13	df	da	e8	b0	47	e9	77	be	dd	08	00	45	00	0-----G-w----E-
0010	00	28	56	43	40	00	80	06	00	00	c0	a8	01	03	23	a8	-(VC@-----#-
0020	1c	83	d2	a6	01	bb	50	10	05	89	dc	6c	63	34	50	14	-----P-----lc4P-
0030	00	00	01	f1	00	00											-----

wireshark\_Wi-FiQQ3MH3.pcapng

Packets: 102613 · Displayed: 127 (0.1%)

Profile: Default

Filter: `tcp.port == 22 and frame.time_delta < 1`

**Observation:**

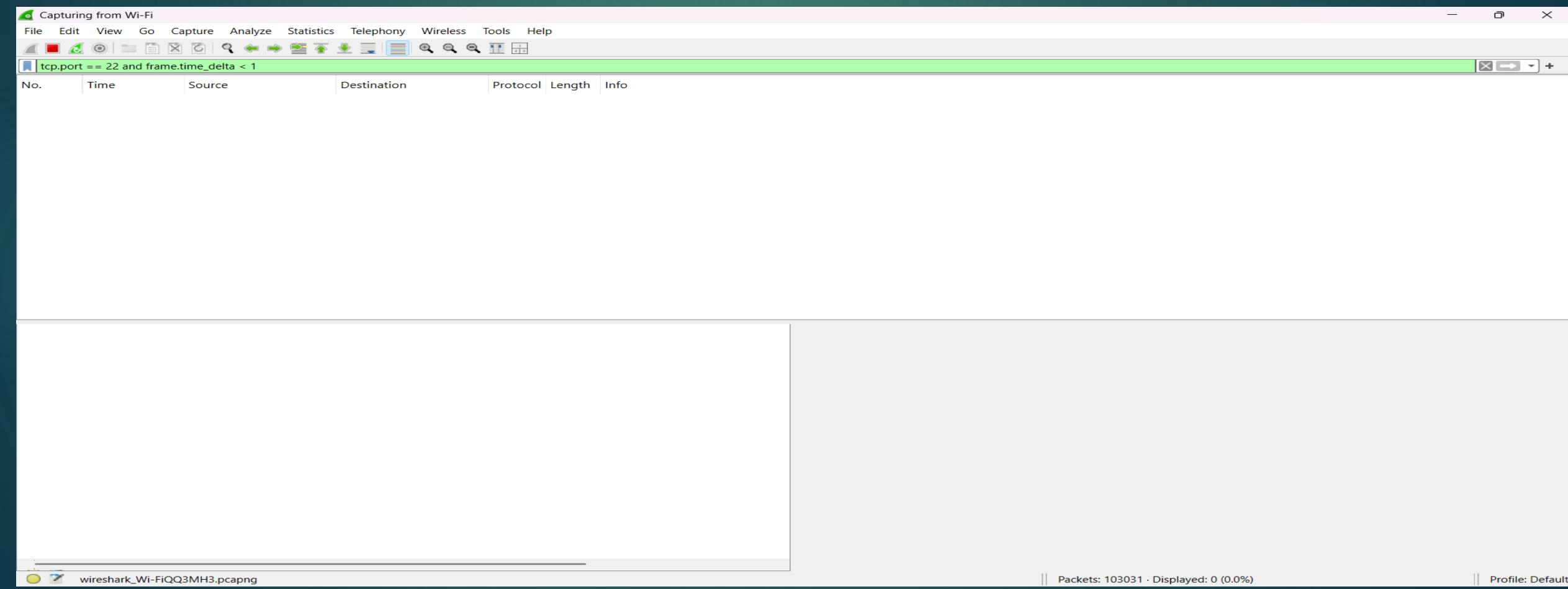
No packets were displayed for TCP port 22 within a time delta of less than 1 second.

**Reason:**

There is no evidence of rapid or repeated SSH connection attempts during the capture period.

**Conclusion:**

No SSH brute-force activity or automated attack behavior was detected.



## Filter: quic

### Observation:

QUIC Initial, Handshake, and Protected Payload packets detected.

### Reason:

QUIC is used by modern browsers and cloud services for performance improvements.

### Conclusion:

The network supports modern encrypted transport protocols.

The screenshot shows a Wireshark interface with a green title bar labeled "wireshark\_project.pcapng". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. A toolbar with various icons is above the main pane. The packet list pane is titled "quic" and displays 116 selected packets. The columns in the list are No., Time, Source, Destination, Protocol, Length, and Info. The "Info" column provides detailed descriptions of each packet, such as "Initial, DCID=673ccf87b9630754, PKN: 1, PING, PING, PING, CRYPTO, CRYPTO, PING" and "Protected Payload (KP0)". The details pane at the bottom left shows a summary of the selected frame, including its bytes on wire and captured length, source and destination MAC addresses, and protocol stack. The hex and ASCII panes on the right show the raw byte data and its corresponding ASCII representation for the selected frame.

No. Time Source Destination Protocol Length Info

55 5.688720 2401:4900:8f57:3ef5... 2404:6800:4009:810:... QUIC 1292 Initial, DCID=673ccf87b9630754, PKN: 1, PING, PING, PING, CRYPTO, CRYPTO, PING

56 5.688862 2401:4900:8f57:3ef5... 2404:6800:4009:810:... QUIC 1292 Initial, DCID=673ccf87b9630754, PKN: 2, PING, PING, PING, CRYPTO, PING

57 5.689095 2401:4900:8f57:3ef5... 2404:6800:4009:810:... QUIC 141 0-RTT, DCID=673ccf87b9630754

58 5.741461 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 102 Initial, SCID=e73ccf87b9630754, PKN: 1, ACK

59 5.745487 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 1292 Initial, SCID=e73ccf87b9630754, PKN: 2, ACK, PADDING

60 5.747764 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 1292 Initial, SCID=e73ccf87b9630754, PKN: 3, CRYPTO, PADDING

61 5.747764 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 371 Protected Payload (KP0)

62 5.747946 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 983 Protected Payload (KP0)

63 5.747946 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 165 Protected Payload (KP0)

64 5.749490 2401:4900:8f57:3ef5... 2404:6800:4009:810:... QUIC 1292 Protected Payload (KP0), DCID=e73ccf87b9630754

65 5.749825 2401:4900:8f57:3ef5... 2404:6800:4009:810:... QUIC 93 Protected Payload (KP0), DCID=e73ccf87b9630754

66 5.771399 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 86 Protected Payload (KP0)

67 5.776327 2401:4900:8f57:3ef5... 2404:6800:4009:810:... QUIC 94 Protected Payload (KP0), DCID=e73ccf87b9630754

68 5.800622 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 182 Protected Payload (KP0)

69 5.825909 2404:6800:4009:810:... 2401:4900:8f57:3ef5... QUIC 88 Protected Payload (KP0)

70 5.826208 2401:4900:8f57:3ef5... 2404:6800:4009:810:... QUIC 93 Protected Payload (KP0), DCID=e73ccf87b9630754

116 6.725174 2401:4900:8f57:3ef5... 2404:6800:4003:c04:... QUIC 1292 Initial, DCID=267852e6fa1a9036, PKN: 1, PING, CRYPTO, CRYPTO, CRYPTO, CRYPTO

> Frame 66: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF\_{917DF297-d...  
> Ethernet II, Src: ZyxelCommuni\_df:da:e8 (30:bd:13:df:da:e8), Dst: Intel\_77:be:dd (b0:47:e9:77:be:dd)  
> Internet Protocol Version 6, Src: 2404:6800:4009:810::2004, Dst: 2401:4900:8f57:3ef5:fd76:5559:b4e1:8d6  
> User Datagram Protocol, Src Port: 443, Dst Port: 62049  
> QUIC IETF

0000 b0 47 e9 77 be dd 30 bd 13 df da e8 86 dd 6b 80 -G-w-0- .----k.  
0010 00 00 00 20 11 3b 24 04 68 00 40 09 08 10 00 00 .--;\$- h@----  
0020 00 00 00 00 20 04 24 01 49 00 8f 57 3e f5 fd 76 .----\$- I-W>--v  
0030 55 59 b4 e1 08 d6 01 bb f2 61 00 20 59 6d 57 60 UY-----a- YmW`  
0040 a7 2b 1d f1 ee 8f 31 f5 b3 be dd 4b 2a 91 b4 bf +---1- ---K\*---  
0050 06 82 c1 f2 fc 59 .----Y

Packets: 103479 · Displayed: 11738 (11.3%) | Profile: Default

## Filter: tls (TLS 1.2)

### Observation:

TLS handshake and application data packets are present.

### Reason:

TLS encrypts application-layer data to ensure confidentiality.

### Conclusion:

Captured traffic is encrypted, limiting payload inspection but confirming secure communication.

wireshark\_project.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tls

No.	Time	Source	Destination	Protocol	Length	Info
25	0.662018	192.168.1.3	100.30.98.72	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
30	0.957197	100.30.98.72	192.168.1.3	TLSv1.2	258	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
32	0.959644	192.168.1.3	100.30.98.72	TLSv1.2	199	Application Data
34	1.277897	100.30.98.72	192.168.1.3	TLSv1.2	718	Application Data
35	1.293136	192.168.1.3	100.30.98.72	TLSv1.2	1017	Application Data
37	1.662704	100.30.98.72	192.168.1.3	TLSv1.2	708	Application Data
55	5.688720	2401:4900:8f57:3ef5...	2404:6800:4009:810...	QUIC	1292	Initial, DCID=673ccf87b9630754, PKN: 1, PING, PING, PING, CRYPTO, CRYPTO, PING
56	5.688862	2401:4900:8f57:3ef5...	2404:6800:4009:810...	QUIC	1292	Initial, DCID=673ccf87b9630754, PKN: 2, PING, PING, PING, CRYPTO, PING
60	5.747764	2404:6800:4009:810...	2401:4900:8f57:3ef5...	QUIC	1292	Initial, SCID=e73ccf87b9630754, PKN: 3, CRYPTO, PADDING
71	5.854938	172.188.155.25	192.168.1.3	TLSv1.2	113	Application Data
72	5.858322	192.168.1.3	172.188.155.25	TLSv1.2	120	Application Data
76	5.935117	2620:1ec:50::12	2401:4900:8f57:3ef5...	TLSv1.2	113	Application Data
77	5.943702	2401:4900:8f57:3ef5...	2620:1ec:50::12	TLSv1.2	109	Application Data
78	5.943789	2401:4900:8f57:3ef5...	2620:1ec:50::12	TLSv1.2	109	Application Data
82	6.007185	2401:4900:8f57:3ef5...	2606:4700:90d1:d8b7...	TLSv1.2	165	Application Data
88	6.079355	2401:4900:8f57:3ef5...	2606:4700:90d2:7cbc...	TLSv1.2	665	Application Data
89	6.079524	2401:4900:8f57:3ef5...	2606:4700:90d2:7cbc...	TLSv1.2	113	Application Data

> Frame 60: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF\_{91...  
> Ethernet II, Src: ZyxelCommuni\_df:da:e8 (30:bd:13:df:da:e8), Dst: Intel\_77:be:dd (b0:47:e9:77:be:dd)  
> Internet Protocol Version 6, Src: 2404:6800:4009:810::2004, Dst: 2401:4900:8f57:3ef5:fd76:5559:b4e1:8d6  
> User Datagram Protocol, Src Port: 443, Dst Port: 62049  
> QUIC IETF

Frame 60 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF\_{91...  
0000 b0 47 e9 77 be dd 30 bd 13 df da e8 86 dd 6b 80 -G-w-0-----k-  
0010 00 00 04 d6 11 3b 24 04 68 00 40 09 08 10 00 00 -----;\$ h@-----  
0020 00 00 00 00 20 04 24 01 49 00 8f 57 3e f5 fd 76 -----\$ I-W>-v  
0030 55 59 b4 e1 08 d6 01 bb f2 61 04 d6 9c e7 c3 00 UY-----a-----  
0040 00 00 01 00 08 e7 3c cf 87 b9 63 07 54 00 44 bc -----<-c-T-D-  
0050 dc 21 1c 38 4a 6f 31 09 ff fe bb 9b 30 1c 82 43 -! 8Jo1-----0-C  
0060 18 8a 9e 8e 9d 6b f3 29 fa ed 20 02 09 b0 48 c0 -----k-)-----H-  
0070 23 d7 5f ba 49 f0 6c b9 4d 73 fe a8 b0 2b ee 0a #\_.I.1 Ms-+...  
0080 35 3f f3 39 71 7f 4c 05 ca 57 d4 d2 63 d0 cd bf 5? 9q-L- W-c...  
0090 9a 82 dd 5c eb a0 77 f6 db ad 9b fc f1 37 bc ef ...`-w-----7...  
00a0 e5 fb 05 4c 66 30 68 d5 e3 60 11 e9 cb 5a 2b f9 ...Lf0h-----Z+  
00b0 b2 c6 bd 3d 78 42 5e 25 17 88 60 15 a7 55 a6 b3 ...=xB^%-----U-  
00c0 5e c7 ac 3f e6 ec 53 a3 8c 43 90 be d7 a8 ee 97 ^?-S-C-----  
00d0 88 f8 97 6f 64 0d 83 50 77 e2 0e e6 56 15 01 48 ..od-P w-V-H  
00e0 64 d4 34 0d 35 94 1b db b9 08 56 8c 89 a7 a5 f0 d-4-5-----V...  
00f0 93 3b a0 65 a2 30 53 ea 0c 27 fd 32 bf 92 e9 29 ; e-0S- '2- )  
0100 59 f1 e5 8d fb 57 28 9c ca 93 1d 43 bf cf b6 4d Y-----W(-----C-M  
0110 c8 c6 9b f7 0a 79 af 92 9d ac bb a7 67 7d 76 44 .....y-----g)D  
0120 8a a6 5a 99 ec 35 98 bd f9 27 2d 51 2c b2 d5 18 ..Z-5-----'Q,...  
0130 fa 8d 9b 14 89 8a d2 ed 89 c7 e8 07 63 bc 5f 70 .....c\_p  
0140 9f 59 c9 f5 c7 14 81 dc 0a 05 b4 ea 7b 15 8e 6f .Y-----{ o

Frame (1292 bytes) Decrypted QUIC (1195 bytes)

Packets: 103479 · Displayed: 21384 (20.7%)

Profile: Default