

# **Network Traffic Capture and Analysis Report**

**Task Title:** Capture and Analyze Network Traffic Using Wireshark

**Tool Used:** Wireshark v4.4.6

**Report Prepared By:** Kshitij

**Date:** 4th June 2025

**Capture File:** wireshark\_Wi-FiLBT072.pcapng

**Capture Duration:** 3 minutes 14 seconds

**Network Interface:** Wi-Fi

**Packet Count:** 2536 packets captured

---

## 1. Objective

The purpose of this exercise was to:

- Capture live network packets using Wireshark.
  - Identify and analyze at least three different network protocols.
  - Understand protocol behavior and packet flow.
  - Export the data in .pcapng format and summarize key insights.
- 

## 2. Setup and Methodology

### Environment:

- **Device:** Windows 11 (64-bit), Intel i5-1235U
- **Wireshark Version:** 4.4.6 (Dumpcap)
- **Interface:** Wireless (Wi-Fi)
- **No Capture Filters Used**

### Steps Taken:

1. Wireshark installed and launched.
  2. Packet capture started on the active Wi-Fi interface.
  3. To generate traffic:
    - Accessed a secure website (HTTPS).
    - Performed a ping to a known server.
  4. Capture stopped after ~3 minutes.
  5. Used filters to isolate and study specific protocols.
-

### 3. Capture Summary

Metric	Value
Packets Captured	2536
Duration	194.066 seconds
Avg. Packets/sec	13.1
Avg. Packet Size	484 bytes
Dropped Packets	0
Total Bytes	1.2 MB (1226920 bytes)
Displayed Packets	580 (22.9%)
Encapsulation	Ethernet

---

### 4. Protocols Identified

At least **three major protocols** were identified and analyzed in this capture:

#### a. TCP (Transmission Control Protocol)

- TCP is the most prevalent protocol in the capture.
- Port 443 was seen frequently, indicating secure HTTPS communication.
- Observed TCP flags: ACK, PSH, FIN, RST.
- Notable issues:
  - **Duplicate ACKs**
  - **Retransmissions**
  - **Out-of-order segments**
  - **D-SACK Sequences**
- These indicate typical internet latency or packet loss and recovery processes.

TCP retransmissions and duplicate ACKs help ensure reliability in data delivery. They are normal in internet communication and handled gracefully by the TCP stack.

---

### b. TLSv1.2 (Transport Layer Security)

- TLS packets were captured showing encrypted communication, primarily between clients and web servers.
- No certificate-level details were available as the capture did not include the TLS handshake start.
- TLS used TCP as the transport layer and ran over port 443.
- Shows that secure HTTPS browsing occurred during the capture.

TLS ensures data confidentiality and integrity over insecure networks, commonly used in secure websites.

---

### c. DNS (Domain Name System)

- DNS protocol was observed resolving domain names.
- Worked over UDP port 53 (not shown in screenshots but typically expected during browsing).
- It translates human-readable domain names to IP addresses, crucial before any web connection can occur.

DNS is a foundational protocol that initiates most user activities by resolving hostnames to IPs.

---

## 5. Expert Information & Observations

Based on Wireshark's **Expert Info**, several TCP-related anomalies were detected:

Type	Summary	Count
Warning	D-SACK Sequence	2
Warning	Out-of-order Segment	2
Warning	Previous segments not captured	2
Note	Suspected retransmission	2
Note	Duplicate ACK	7

These are common in wireless networks and indicate reordering, lost packets, and TCP recovery mechanisms.

## 6.Screenshots

Wireshark · Capture File Properties · Wi-Fi

Details

File

Name:

C:\Users\KSHITU\AppData\Local\Temp\wireshark\_Wi-Fi\BTO72.pcapng

Length:

1312 kB

Hash (SHA256):

dcda0063424c6562dc48e31e31c169c7d26a38cb97fa509bcf25b69603832b43

Hash (SHA1):

4b74b8710d0b8b4a8c16fe5390d0c44144326e02

Format:

Wireshark/... - pcapng

Encapsulation:

Ethernet

Time

First packet:

2025-06-04 19:11:02

Last packet:

2025-06-04 19:14:16

Elapsed:

00:03:14

Capture

Hardware:

12th Gen Intel(R) Core(TM) i5-1235U (with SSE4.2)

OS:

64-bit Windows 11 (24H2), build 26100

Application:

Dumpcap (Wireshark) 4.4.6 (v4.4.6-0-gaebb20483889)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	2536	580 (22.9%)	—
Time span, s	194.066	183.668	—
Average pps	13.1	3.2	—
Average packet size, B	484	453	—
Bytes	1226920	262783 (21.4%)	0
Average bytes/s	6322	1430	—
Average bits/s	50 k	11 k	—

Wireshark · Expert Information · Wi-Fi

Packet	Summary	Group	Protocol	Count
▼ Warning	D-SACK Sequence	Sequence	TCP	2
1717	[TCP Dup ACK 1716#1] 443 → 53969 [ACK] Seq=7228 Ack=42838 Win=1...	Sequence	TCP	
2453	53969 → 443 [ACK] Seq=150691 Ack=46195 Win=1019 Len=0 SLE=4595...	Sequence	TCP	
▼ Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	2
291	[TCP Out-Of-Order] 443 → 53969 [PSH, ACK] Seq=2660 Ack=14287 Win...	Sequence	TCP	
2221	[TCP Out-Of-Order] 443 → 53969 [PSH, ACK] Seq=30074 Ack=101541 W...	Sequence	TCP	
> Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	2
▼ Note	This frame is a (suspected) retransmission	Sequence	TCP	2
1701	[TCP Retransmission] 53969 → 443 [PSH, ACK] Seq=41538 Ack=7228 Wi...	Sequence	TCP	
2452	[TCP Retransmission] 443 → 53969 [PSH, ACK] Seq=45953 Ack=150691 ...	Sequence	TCP	
▼ Note	Duplicate ACK	Sequence	TCP	7
292	[TCP Dup ACK 114#1] 53969 → 443 [ACK] Seq=14287 Ack=2660 Win=10...	Sequence	TCP	
1244	[TCP Dup ACK 1243#1] 443 → 53969 [ACK] Seq=3762 Ack=19188 Win=1...	Sequence	TCP	
1358	[TCP Dup ACK 1351#1] 443 → 53969 [ACK] Seq=6511 Ack=32242 Win=1...	Sequence	TCP	
1717	[TCP Dup ACK 1716#1] 443 → 53969 [ACK] Seq=7228 Ack=42838 Win=1...	Sequence	TCP	
2184	[TCP Dup ACK 2183#1] 443 → 53969 [ACK] Seq=24244 Ack=90651 Win=...	Sequence	TCP	
2222	[TCP Dup ACK 2205#1] 53969 → 443 [ACK] Seq=104432 Ack=30074 Win...	Sequence	TCP	
2501	[TCP Dup ACK 2496#1] 443 → 53969 [ACK] Seq=46622 Ack=162004 Win...	Sequence	TCP	

No.	Time	Source	Destination	Protocol	Length	Info
36	23.199830	2409:40d7:a0:aaf7:4...	2404:6800:4002:817:...	TCP	74	55207 → 443 [ACK] Seq=1 Ack=113 Win=255 Len=0
37	23.199935	2603:1040:a03:9::1b6	2409:40d7:a0:aaf7:4...	TLSv1.2	113	Application Data
38	23.232537	2620:1ec:50::12	2409:40d7:a0:aaf7:4...	TCP	74	443 → 53969 [ACK] Seq=118 Ack=141 Win=16385 Len=0
39	23.241596	2620:1ec:50::12	2409:40d7:a0:aaf7:4...	TCP	74	443 → 53969 [ACK] Seq=118 Ack=176 Win=16385 Len=0
40	23.247783	2409:40d7:a0:aaf7:4...	2603:1040:a03:9::1b6	TCP	74	55204 → 443 [ACK] Seq=51 Ack=40 Win=255 Len=0
41	23.289487	2409:40d7:a0:aaf7:4...	2404:6800:4002:816:...	TLSv1.2	98	Application Data
42	23.291225	2409:40d7:a0:aaf7:4...	2404:6800:4002:816:...	TCP	74	55186 → 443 [FIN, ACK] Seq=25 Ack=1 Win=253 Len=0
43	23.354733	2404:6800:4002:816:...	2409:40d7:a0:aaf7:4...	TCP	74	443 → 55186 [RST] Seq=1 Win=0 Len=0
44	23.354733	2404:6800:4002:816:...	2409:40d7:a0:aaf7:4...	TCP	74	443 → 55186 [RST] Seq=1 Win=0 Len=0
45	23.354733	2620:1ec:50::12	2409:40d7:a0:aaf7:4...	TLSv1.2	113	Application Data
46	23.360041	2409:40d7:a0:aaf7:4...	2620:1ec:50::12	TLSv1.2	109	Application Data
47	23.412424	2620:1ec:50::12	2409:40d7:a0:aaf7:4...	TCP	74	443 → 53969 [ACK] Seq=157 Ack=211 Win=16385 Len=0
48	23.566763	2409:40d7:a0:aaf7:4...	64:ff9b::34bb:4f6d	TCP	75	53932 → 443 [ACK] Seq=1 Ack=1 Win=251 Len=1 [TCP PDU reassembled in 374]
49	23.680630	64:ff9b::34bb:4f6d	2409:40d7:a0:aaf7:4...	TCP	86	443 → 53932 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2
50	23.780380	2409:40d7:a0:aaf7:4...	2001:4860:4802:38:...	TLSv1.2	98	Application Data
51	23.781401	2409:40d7:a0:aaf7:4...	2001:4860:4802:38:...	TCP	74	55195 → 443 [FIN, ACK] Seq=25 Ack=1 Win=251 Len=0
52	23.839103	2001:4860:4802:38:...	2409:40d7:a0:aaf7:4...	TCP	74	443 → 55195 [RST] Seq=1 Win=0 Len=0
53	23.839103	2001:4860:4802:38:...	2409:40d7:a0:aaf7:4...	TCP	74	443 → 55195 [RST] Seq=1 Win=0 Len=0
54	23.991016	64:ff9b::23ae:7f1f	2409:40d7:a0:aaf7:4...	TLSv1.2	98	Application Data
55	23.991291	2409:40d7:a0:aaf7:4...	64:ff9b::23ae:7f1f	TLSv1.2	102	Application Data
56	24.430955	2409:40d7:a0:aaf7:4...	64:ff9b::23ae:7f1f	TCP	102	[TCP Retransmission] 55214 → 443 [PSH, ACK] Seq=478 Ack=551 Win=251 Len=28
57	24.464401	64:ff9b::23ae:7f1f	2409:40d7:a0:aaf7:4...	TCP	74	443 → 55214 [ACK] Seq=551 Ack=506 Win=337 Len=0
58	24.716125	64:ff9b::23ae:7f1f	2409:40d7:a0:aaf7:4...	TCP	86	[TCP Dup ACK 57#1] 443 → 55214 [ACK] Seq=551 Ack=506 Win=337 Len=0 SLE=478 SRE=506
59	27.344259	2404:6800:4002:803:...	2409:40d7:a0:aaf7:4...	TLSv1.2	156	Application Data
60	27.390803	2409:40d7:a0:aaf7:4...	2404:6800:4002:803:...	TCP	74	54013 → 443 [ACK] Seq=1 Ack=165 Win=255 Len=0

[ TCP Flags: .....R.. ]  
Window: 0  
[ Calculated window size: 0 ]  
[ Window size scaling factor: -1 (unknown) ]  
Checksum: 0xf26f [unverified]  
[ Checksum Status: Unverified ]  
Urgent Pointer: 0  
▼ [ Timestamps ]  
[ Time since first frame in this TCP stream: 0.065246000 seconds ]  
[ Time since previous frame in this TCP stream: 0.000000000 seconds ]

0000 30 03 c8 84 63 c3 8a 32 8b 8b 21 c9 86 dd 68 06 0...c...2...I...h-  
0010 44 2e 00 14 06 77 24 04 68 00 40 02 08 16 00 00 D...w\$. h.@.....  
0020 00 00 00 00 20 0a 24 09 40 d7 00 a0 aa f7 4d d9 .... \$. @.....M-  
0030 1d 22 03 4c 2c f5 01 bb d7 92 33 7c 10 cc 00 00 -".L,...:3]....  
0040 00 00 50 04 00 00 f2 6f 00 00 ..P....o ..

## 7. Notable Packet Details (from capture)

- **Packet #43 & #44:** TCP RST packets indicating abrupt termination of connections.
- **Packet #56:** TCP Retransmission observed with Seq=478 Ack=551.
- **Packet #57:** Followed by TCP Duplicate ACK, confirming the retransmission requirement.
- **TLSv1.2 Packets:** Many encrypted data packets observed with consistent lengths (e.g., 102, 109, 156 bytes).

## 8. Conclusion

This hands-on exercise with Wireshark helped develop core packet analysis skills and improved understanding of how protocols function and interact in real-time. The most active protocol was TCP, facilitating reliable communication. TLSv1.2 confirmed the usage of encrypted web connections, while DNS played its role in initial name resolution.

### Skills Gained:

- Live packet capture using Wireshark
- Protocol filtering and analysis
- Understanding retransmissions and TCP flow issues
- Exporting .pcapng files and generating reports

