Cyber Security Internship

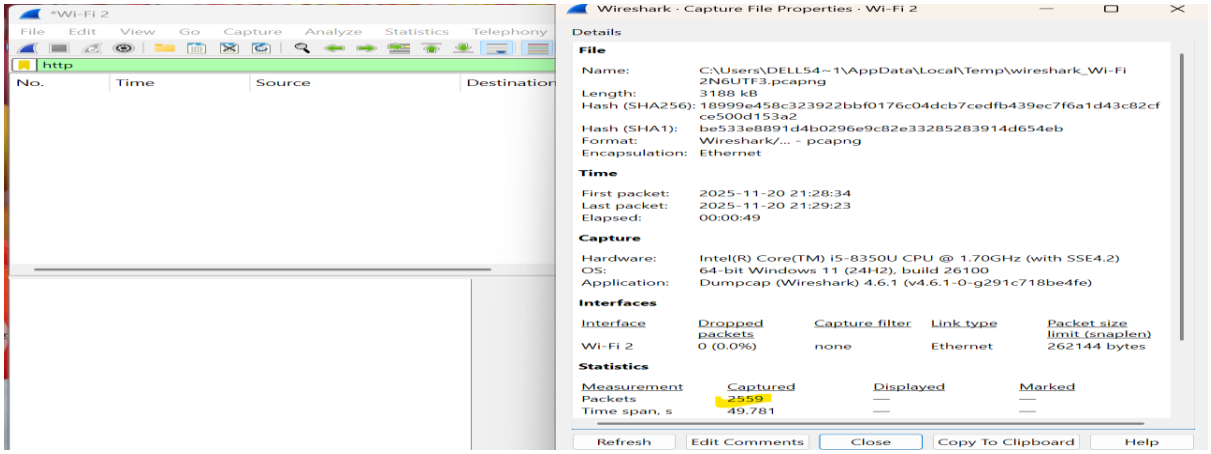
Task 5 – Capture and Analyze Network Traffic using Wireshark

Captured live network traffic for 1 minute on Wi-Fi interface, generated traffic by browsing websites and using ping.

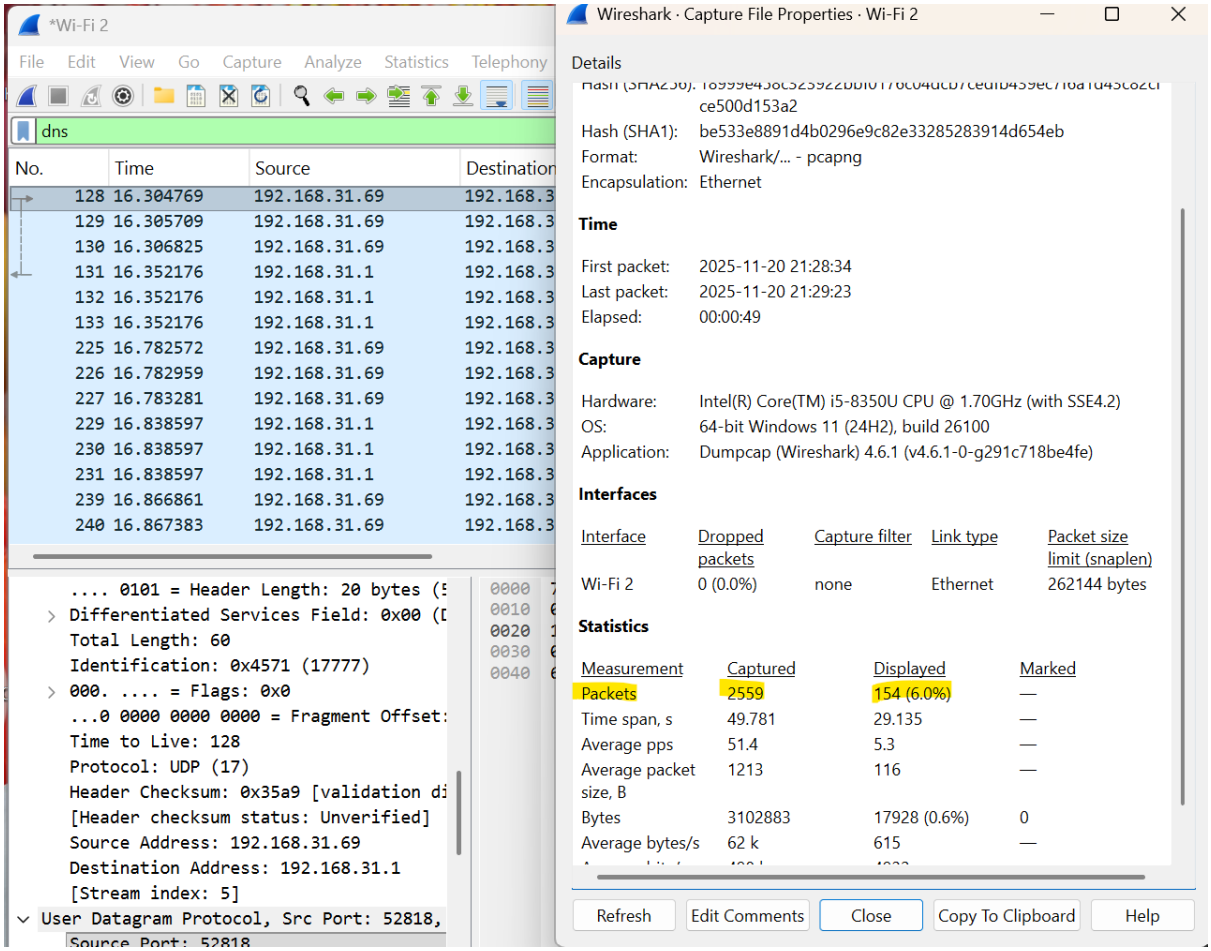
1. **Install Wireshark:**
    - Downloaded Wireshark from the official site
    - Installed Wireshark + Npcap (required for traffic capture)
    - Open Wireshark and confirm it shows network interfaces (Wi-Fi, Ethernet, etc.)
2. **Start capturing on Active network interface:**
    - Selecting active **interface**
    - Click the **Shark Fin (start capture)** icon
3. **Generating traffic (Browse/ Ping):**
    - To generate visible traffic – open a browser and visit **google.com**
    - With ping - open CMD and run: **ping 8.8.8.8**
4. **Stop Capture after 1 minute:**
    - Click the **Red square** icon to stop the capturing
    - Save the capture temporarily if needed
5. **Filter Captured packets by Protocol:**

    Checking how packet counts changes based on filter selection – using **Display filter**

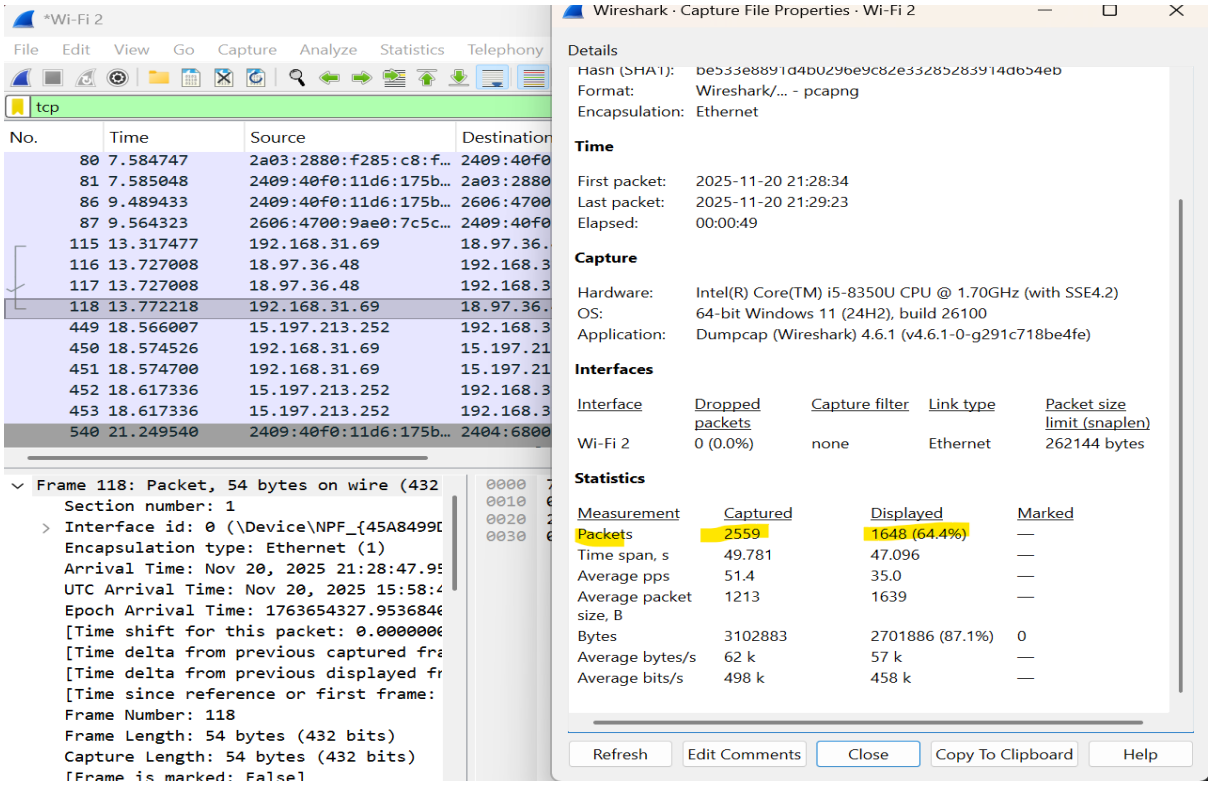
    - **HTTP**



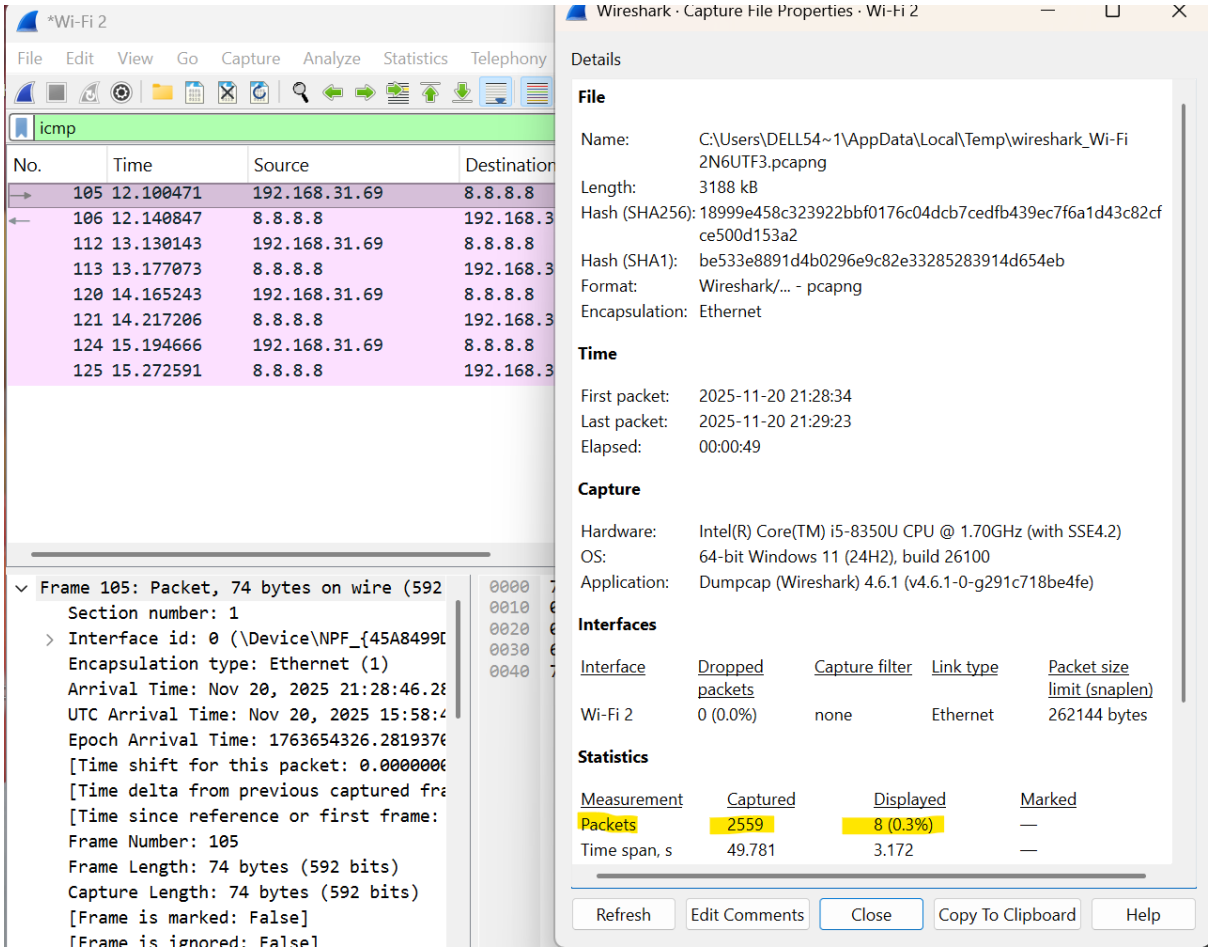
    - **DNS**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony
dns
No. Time Source Destination
128 16.304769 192.168.31.69 192.168.3
129 16.305709 192.168.31.69 192.168.3
130 16.306825 192.168.31.69 192.168.3
131 16.352176 192.168.31.1 192.168.3
132 16.352176 192.168.31.1 192.168.3
133 16.352176 192.168.31.1 192.168.3
225 16.782572 192.168.31.69 192.168.3
226 16.782959 192.168.31.69 192.168.3
227 16.783281 192.168.31.69 192.168.3
229 16.838597 192.168.31.1 192.168.3
230 16.838597 192.168.31.1 192.168.3
231 16.838597 192.168.31.1 192.168.3
239 16.866861 192.168.31.69 192.168.3
240 16.867383 192.168.31.69 192.168.3
.... 0101 = Header Length: 20 bytes (5
Differentiated Services Field: 0x00 (D
Total Length: 60
Identification: 0x4571 (17777)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset:
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x35a9 [validation di
[Header checksum status: Unverified]
Source Address: 192.168.31.69
Destination Address: 192.168.31.1
[Stream index: 5]
User Datagram Protocol, Src Port: 52818,
Source Port: 52818
Wireshark · Capture File Properties · Wi-Fi 2
Details
ce500d153a2
Hash (SHA1): be533e8891d4b0296e9c82e33285283914d654eb
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2025-11-20 21:28:34
Last packet: 2025-11-20 21:29:23
Elapsed: 00:00:49
Capture
Hardware: Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (with SSE4.2)
OS: 64-bit Windows 11 (24H2), build 26100
Application: Dumpcap (Wireshark) 4.6.1 (v4.6.1-0-g291c718be4fe)
Interfaces
Interface Dropped packets Capture filter Link type Packet size limit (snaplen)
Wi-Fi 2 0 (0.0%) none Ethernet 262144 bytes
Statistics
Measurement Captured Displayed Marked
Packets 2559 154 (6.0%) —
Time span, s 49.781 29.135 —
Average pps 51.4 5.3 —
Average packet size, B 1213 116 —
Bytes 3102883 17928 (0.6%) 0
Average bytes/s 62 k 615 —
Refresh Edit Comments Close Copy To Clipboard Help

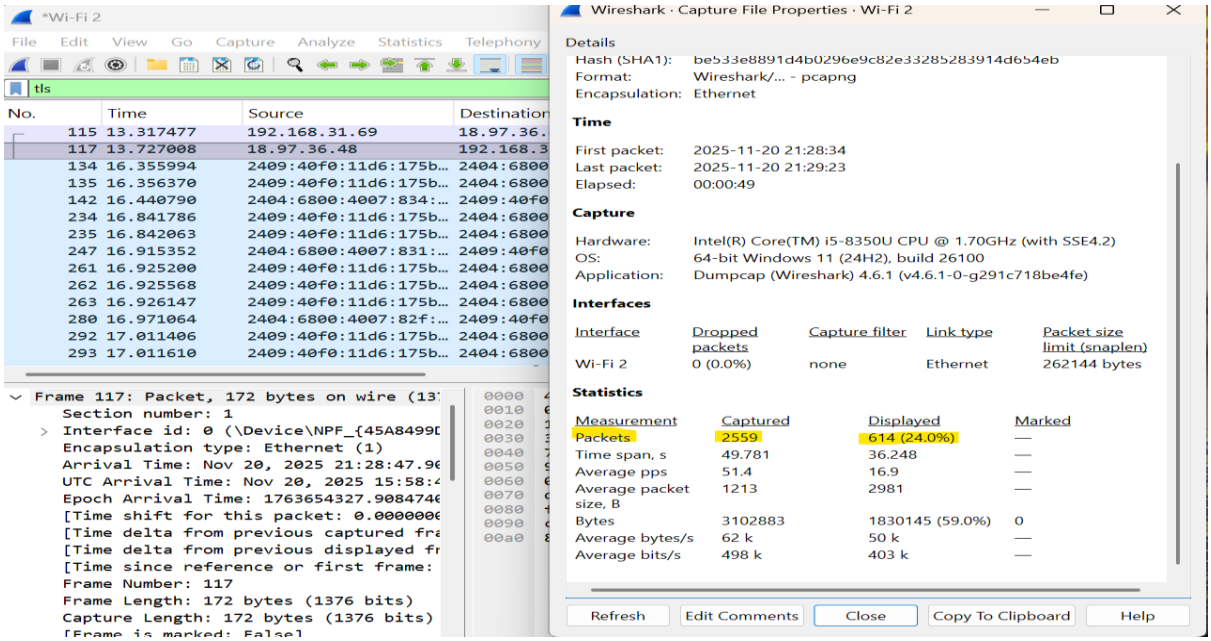
- **TCP**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony
tcp
No. Time Source Destination
80 7.584747 2a03:2880:f285:c8:f... 2409:40f0
81 7.585048 2409:40f0:11d6:175b... 2a03:2880
86 9.489433 2409:40f0:11d6:175b... 2606:4700
87 9.564323 2606:4700:9ae0:7c5c... 2409:40f0
115 13.317477 192.168.31.69 18.97.36.
116 13.727008 18.97.36.48 192.168.3
117 13.727008 18.97.36.48 192.168.3
118 13.772218 192.168.31.69 18.97.36.
449 18.566007 15.197.213.252 192.168.3
450 18.574526 192.168.31.69 15.197.21
451 18.574700 192.168.31.69 15.197.21
452 18.617336 15.197.213.252 192.168.3
453 18.617336 15.197.213.252 192.168.3
540 21.249540 2409:40f0:11d6:175b... 2404:6800
Frame 118: Packet, 54 bytes on wire (432
Section number: 1
Interface id: 0 (\Device\NPF_{45A8499D
Encapsulation type: Ethernet (1)
Arrival Time: Nov 20, 2025 21:28:47.95
UTC Arrival Time: Nov 20, 2025 15:58:4
Epoch Arrival Time: 1763654327.9536846
[Time shift for this packet: 0.000000
[Time delta from previous captured fra
[Time delta from previous displayed fr
[Time since reference or first frame:
Frame Number: 118
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
Wireshark · Capture File Properties · Wi-Fi 2
Details
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2025-11-20 21:28:34
Last packet: 2025-11-20 21:29:23
Elapsed: 00:00:49
Capture
Hardware: Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (with SSE4.2)
OS: 64-bit Windows 11 (24H2), build 26100
Application: Dumpcap (Wireshark) 4.6.1 (v4.6.1-0-g291c718be4fe)
Interfaces
Interface Dropped packets Capture filter Link type Packet size limit (snaplen)
Wi-Fi 2 0 (0.0%) none Ethernet 262144 bytes
Statistics
Measurement Captured Displayed Marked
Packets 2559 1648 (64.4%) —
Time span, s 49.781 47.096 —
Average pps 51.4 35.0 —
Average packet size, B 1213 1639 —
Bytes 3102883 2701886 (87.1%) 0
Average bytes/s 62 k 57 k —
Average bits/s 498 k 458 k —
Refresh Edit Comments Close Copy To Clipboard Help

- **ICMP**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony
icmp
No. Time Source Destination
105 12.100471 192.168.31.69 8.8.8.8
106 12.140847 8.8.8.8 192.168.3
112 13.130143 192.168.31.69 8.8.8.8
113 13.177073 8.8.8.8 192.168.3
120 14.165243 192.168.31.69 8.8.8.8
121 14.217206 8.8.8.8 192.168.3
124 15.194666 192.168.31.69 8.8.8.8
125 15.272591 8.8.8.8 192.168.3
Frame 105: Packet, 74 bytes on wire (592
Section number: 1
Interface id: 0 (\Device\NPF_{45A8499
Encapsulation type: Ethernet (1)
Arrival Time: Nov 20, 2025 21:28:46.28
UTC Arrival Time: Nov 20, 2025 15:58:4
Epoch Arrival Time: 1763654326.281937
[Time shift for this packet: 0.000000
[Time delta from previous captured fra
[Time since reference or first frame:
Frame Number: 105
Frame Length: 74 bytes (592 bits)
Capture Length: 74 bytes (592 bits)
[Frame is marked: False]
[Frame is ignored: False]
Wireshark · Capture File Properties · Wi-Fi 2
Details
File
Name: C:\Users\DELL54~1\AppData\Local\Temp\wireshark_Wi-Fi 2N6UTF3.pcapng
Length: 3188 kB
Hash (SHA256): 18999e458c323922bbf0176c04dcb7cedfb439ec7f6a1d43c82cf ce500d153a2
Hash (SHA1): be533e8891d4b0296e9c82e33285283914d654eb
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2025-11-20 21:28:34
Last packet: 2025-11-20 21:29:23
Elapsed: 00:00:49
Capture
Hardware: Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (with SSE4.2)
OS: 64-bit Windows 11 (24H2), build 26100
Application: Dumpcap (Wireshark) 4.6.1 (v4.6.1-0-g291c718be4fe)
Interfaces
Interface Dropped packets Capture filter Link type Packet size limit (snaplen)
Wi-Fi 2 0 (0.0%) none Ethernet 262144 bytes
Statistics
Measurement Captured Displayed Marked
Packets 2559 8 (0.3%) —
Time span, s 49.781 3.172 —
Refresh Edit Comments Close Copy To Clipboard Help

- **TLS**


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony
tls
No. Time Source Destination
115 13.317477 192.168.31.69 18.97.36.
117 13.727008 18.97.36.48 192.168.3
134 16.355994 2409:40f0:11d6:175b... 2404:6800
135 16.356370 2409:40f0:11d6:175b... 2404:6800
142 16.440790 2404:6800:4007:834:... 2409:40f0
234 16.841786 2409:40f0:11d6:175b... 2404:6800
235 16.842063 2409:40f0:11d6:175b... 2404:6800
247 16.915352 2404:6800:4007:831:... 2409:40f0
261 16.925200 2409:40f0:11d6:175b... 2404:6800
262 16.925568 2409:40f0:11d6:175b... 2404:6800
263 16.926147 2409:40f0:11d6:175b... 2404:6800
280 16.971064 2404:6800:4007:82f:... 2409:40f0
292 17.011406 2409:40f0:11d6:175b... 2404:6800
293 17.011610 2409:40f0:11d6:175b... 2404:6800
Frame 117: Packet, 172 bytes on wire (13
Section number: 1
Interface id: 0 (\Device\NPF_{45A8499
Encapsulation type: Ethernet (1)
Arrival Time: Nov 20, 2025 21:28:47.96
UTC Arrival Time: Nov 20, 2025 15:58:4
Epoch Arrival Time: 1763654327.908474
[Time shift for this packet: 0.000000
[Time delta from previous captured fra
[Time delta from previous displayed fr
[Time since reference or first frame:
Frame Number: 117
Frame Length: 172 bytes (1376 bits)
Capture Length: 172 bytes (1376 bits)
[Frame is marked: False]
Wireshark · Capture File Properties · Wi-Fi 2
Details
Hash (SHA1): be533e8891d4b0296e9c82e33285283914d654eb
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2025-11-20 21:28:34
Last packet: 2025-11-20 21:29:23
Elapsed: 00:00:49
Capture
Hardware: Intel(R) Core(TM) i5-8350U CPU @ 1.70GHz (with SSE4.2)
OS: 64-bit Windows 11 (24H2), build 26100
Application: Dumpcap (Wireshark) 4.6.1 (v4.6.1-0-g291c718be4fe)
Interfaces
Interface Dropped packets Capture filter Link type Packet size limit (snaplen)
Wi-Fi 2 0 (0.0%) none Ethernet 262144 bytes
Statistics
Measurement Captured Displayed Marked
Packets 2559 614 (24.0%) —
Time span, s 49.781 36.248 —
Average pps 51.4 16.9 —
Average packet size, B 1213 2981 —
Bytes 3102883 1830145 (59.0%) 0
Average bytes/s 62 k 50 k —
Average bits/s 498 k 403 k —
Refresh Edit Comments Close Copy To Clipboard Help

6. Summarize:

By using **Wireshark,** we had started to capture live network traffic for 1 minute on Wi-Fi interface and generated data packets by browsing websites and using ping.

→ The total packets captured – **2559**

→ While capturing we had identified different protocols used in the network traffic which are **DNS, TCP, TLS and ICMP.**

→ Here we attached the screenshots of the specified protocol packet count by using **Capture File Properties**

→ We also observed the following:

- DNS queries initiated immediately when browsing new websites
- Majority of traffic is encrypted TLS due to HTTPS
- ICMP packets are visible and easy to analyze
- No suspicious or malformed packets detected

→ The file has exported in the format of **packet.pcap** – which contains filtered and unfiltered packets.

→ This is how we capture and analyze data packets in **Wireshark.**