

TASK – 5 ELEVATE LABS : Capture and Analyze Network Traffic Using Wireshark.

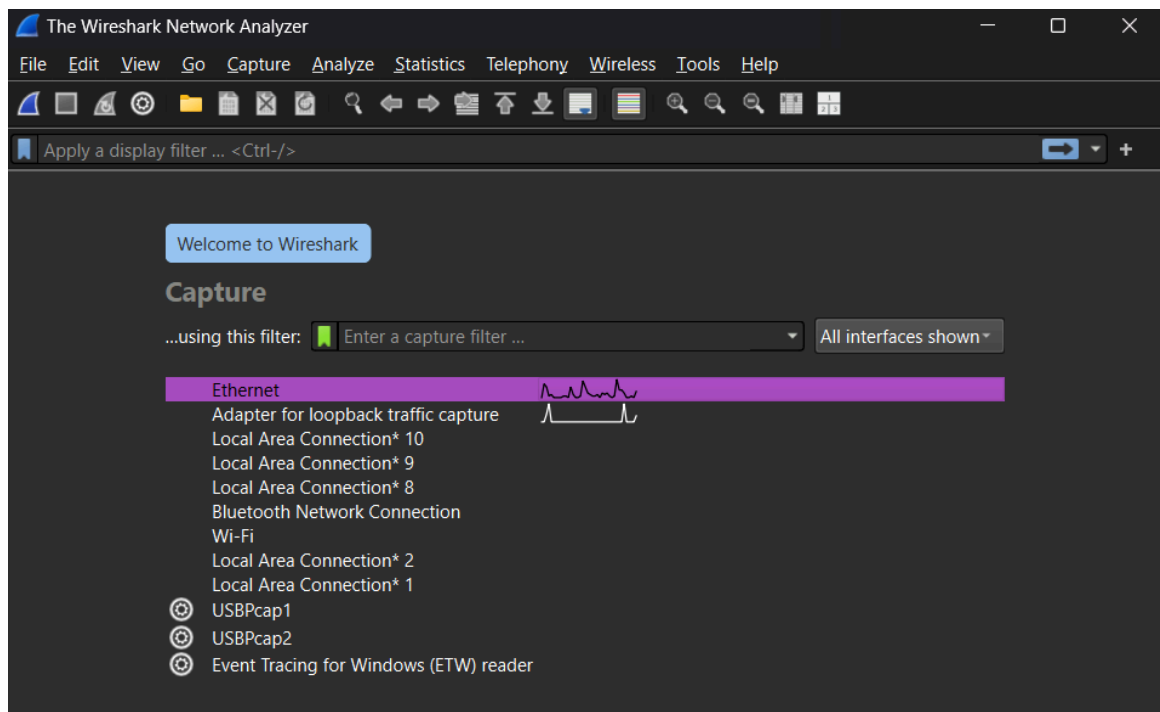
OBJECTIVE : Capture live network packets and identify basic protocols and traffic types

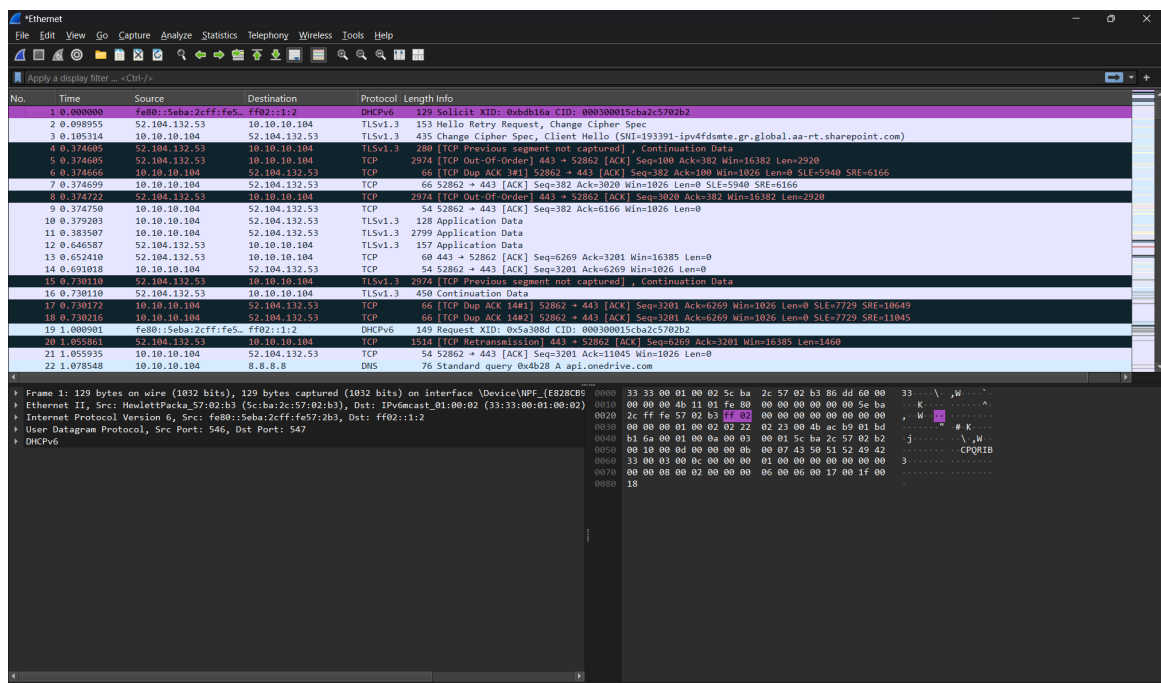
NAME : Sharma Yashika Arunkumar

DATE : 11-08-2025

1) Start Wireshark and choose an interface

1. Open Wireshark.
2. In the start page you'll see a list of interfaces (Ethernet, Wi-Fi, Npcap Loopback).
3. Pick the active interface (the one with the moving packet graph).
4. Double-click it to start capturing immediately, or click the interface once and press the blue shark-fin icon to start.





2) Generate traffic (do this while capture runs)

- Open a web page in your browser (HTTP or HTTPS).
- From Command Prompt run: `ping 8.8.8.8`.
- Optionally: `nslookup example.com` or `curl http://example.com` (if installed). These produce ICMP, DNS, TCP and HTTP/TLS packets.

```

C:\WINDOWS\system32\cmd. x + v

Microsoft Windows [Version 10.0.22631.5699]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sharm>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=5ms TTL=118
Reply from 8.8.8.8: bytes=32 time=12ms TTL=118
Reply from 8.8.8.8: bytes=32 time=3ms TTL=118
Reply from 8.8.8.8: bytes=32 time=4ms TTL=118

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 12ms, Average = 6ms

C:\Users\sharm>

```

3) Stop capture

- After ~60 seconds click the red square (stop) in Wireshark's toolbar.

4) Inspect captured packets (basic)

- Look at the Packet List pane (top): columns Time, Source, Destination, Protocol, Length, Info.

- Click a packet to see Packet Details (middle pane) and Packet Bytes (bottom pane).
- Expand layers (Ethernet → IP → TCP/UDP → application protocol) to view fields.

5) Find these protocols

Use these display filters (type into the display-filter bar and press Enter):

- **DNS Traffic (Domain Resolution)**

Goal: Capture DNS queries to domains

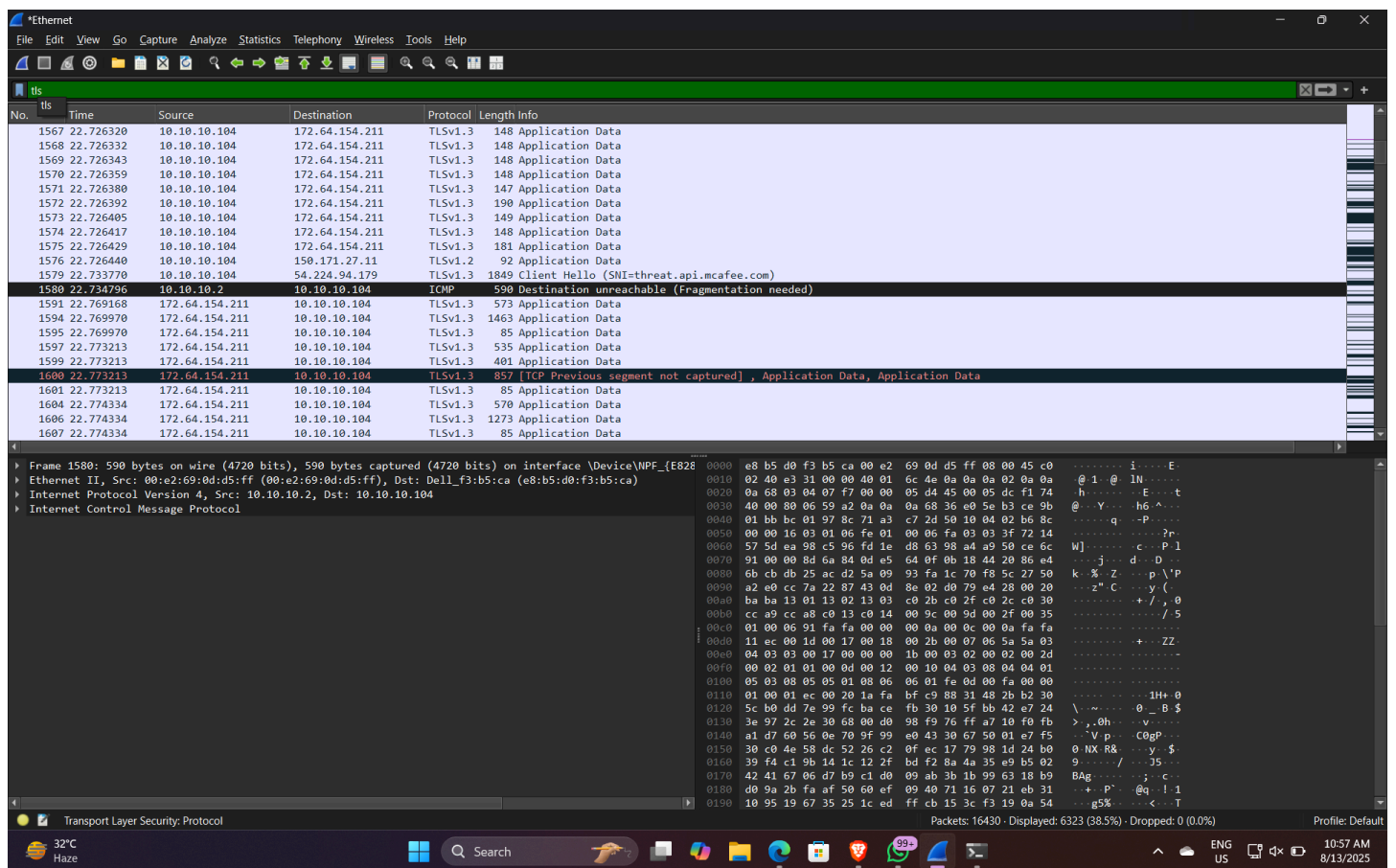
No.	Time	Source	Destination	Protocol	Length	Info
22	1.078548	10.10.10.104	8.8.8.8	DNS	76	Standard query 0x4b28 A api.onedrive.com
24	1.121065	10.10.10.104	4.2.2.2	DNS	76	Standard query 0x4b28 A api.onedrive.com
25	1.226721	4.2.2.2	10.10.10.104	DNS	298	Standard query response 0x4b28 A api.onedrive.com CNAME common-afdrk-fe.1drv.com CNAME odc-commonafdrk-geo.onedrive.akadns.net CN
41	1.305138	8.8.8.8	10.10.10.104	DNS	298	Standard query response 0x4b28 A api.onedrive.com CNAME common-afdrk-fe.1drv.com CNAME odc-commonafdrk-geo.onedrive.akadns.net CN
328	19.900209	10.10.10.104	8.8.8.8	DNS	87	Standard query 0x60cd A browser.events.data.msn.com
329	19.900956	10.10.10.104	8.8.8.8	DNS	69	Standard query 0x9ed9 A c.msn.com
330	19.901400	10.10.10.104	8.8.8.8	DNS	84	Standard query 0x0842 A sb.scorecardresearch.com
331	19.902034	10.10.10.104	8.8.8.8	DNS	74	Standard query 0x70d1 A assets.msn.com
332	19.902895	10.10.10.104	8.8.8.8	DNS	72	Standard query 0xe9be A www.bing.com
333	19.924134	8.8.8.8	10.10.10.104	DNS	226	Standard query response 0x60cd A browser.events.data.msn.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedscolprd
335	19.924864	8.8.8.8	10.10.10.104	DNS	246	Standard query response 0x70d1 A assets.msn.com CNAME assets-msn-com-world-atm-default.trafficmanager.net CNAME assets.msn-com-io
337	19.930146	10.10.10.104	4.2.2.2	DNS	84	Standard query 0x0842 A sb.scorecardresearch.com
338	19.930291	10.10.10.104	4.2.2.2	DNS	69	Standard query 0x9ed9 A c.msn.com
339	19.946716	10.10.10.104	4.2.2.2	DNS	72	Standard query 0xe9be A www.bing.com
343	19.952144	8.8.8.8	10.10.10.104	DNS	148	Standard query response 0x0842 A sb.scorecardresearch.com A 13.224.163.47 A 13.224.163.86 A 13.224.163.31 A 13.224.163.75
345	19.953530	8.8.8.8	10.10.10.104	DNS	251	Standard query response 0x9ed9 A c.msn.com CNAME c-msn-afd.trafficmanager.net CNAME idsyneprod-cehbcscqdhhgcj.b01.azurefd.net C
383	20.027437	4.2.2.2	10.10.10.104	DNS	127	Standard query response 0x9ed9 A c.msn.com CNAME c-msn-afd.trafficmanager.net A 52.231.230.148
385	20.030252	4.2.2.2	10.10.10.104	DNS	148	Standard query response 0x0842 A sb.scorecardresearch.com A 3.168.86.20 A 3.168.86.68 A 3.168.86.44 A 3.168.86.42
386	20.035674	10.10.10.104	8.8.8.8	DNS	76	Standard query 0x8ad6 A r.msftstatic.com
387	20.035743	10.10.10.104	8.8.8.8	DNS	70	Standard query 0x08e2 A r.bing.com
388	20.038450	4.2.2.2	10.10.10.104	DNS	337	Standard query response 0xe9be A www.bing.com CNAME www-www.bing.com.trafficmanager.net CNAME www.bing.com.edgekey.net CNAME e863
393	20.056102	8.8.8.8	10.10.10.104	DNS	156	Standard query response 0x8ad6 A r.msftstatic.com CNAME r-msftstatic-com-a-0016.a-msedge.net CNAME a-0016.a-msedge.net A 204.79.1

What to Check:

- **Source:** Your host IP
- **Destination:** Local DNS server .
- **Query Name & Response:** Contains the resolved IP addresses.

- **tls (or ssl)**

Goal: TLS (HTTPS) handshakes & records

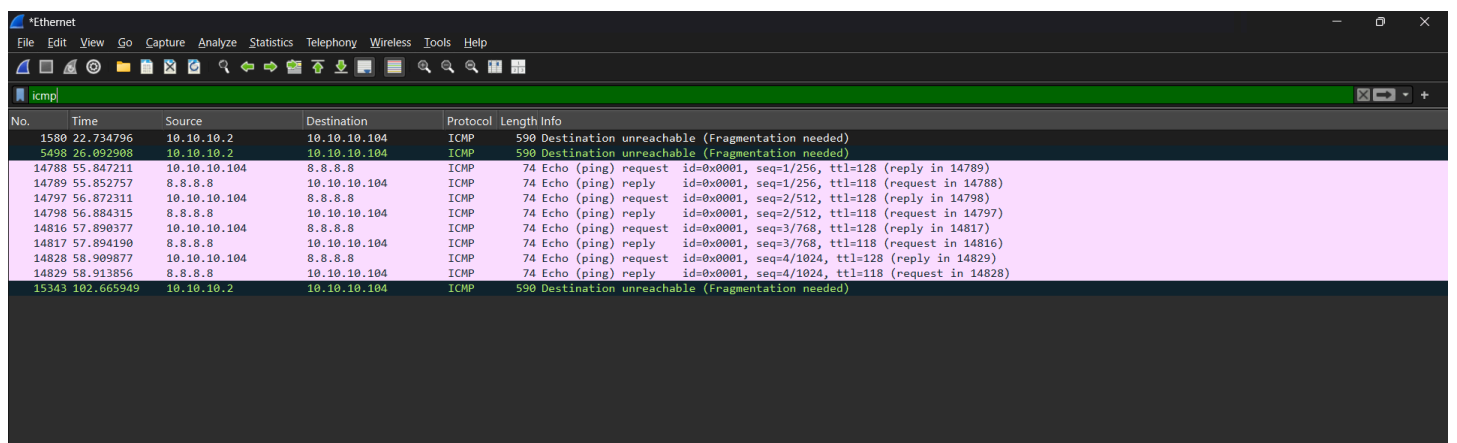


What to Check:

- **Client Hello** packet: Contains *Server Name Indication (SNI)* → shows the domain name before encryption.
- **Server Hello** packet: Contains server's chosen TLS parameters.
- **Encrypted Application Data** afterwards → proves payload is encrypted.

icmp

Goal: ping/Echo request & reply



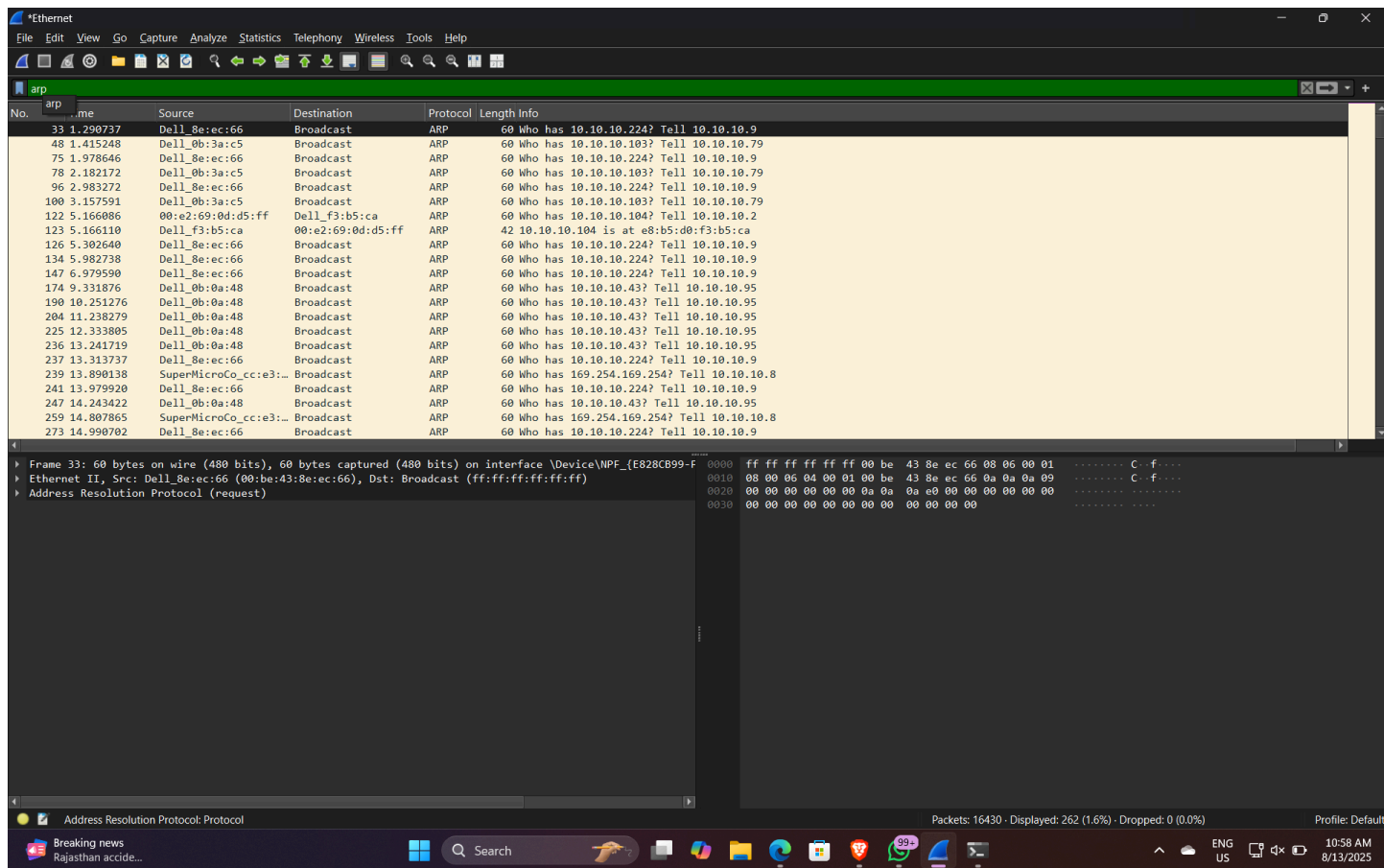
What to Check:

- **Echo (request)** packets from your IP to 8.8.8.8.

- **Echo reply** packets from 8.8.8.8 back to your IP.

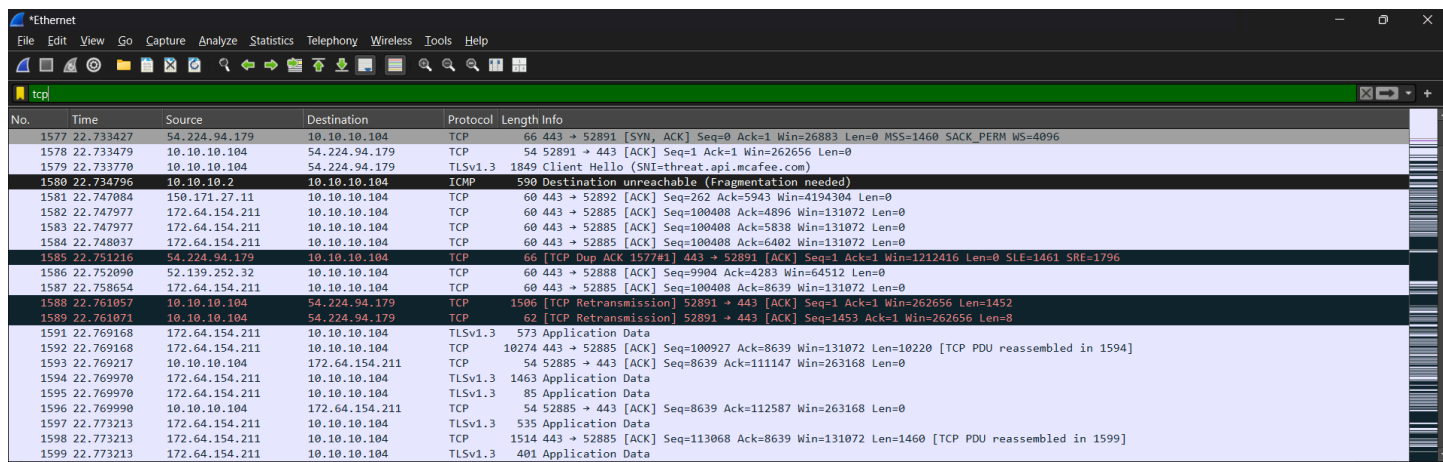
arp

Goal: ARP requests/replies



TCP Traffic (Transport Layer)

Goal: See TCP connections for browsing and app traffic.

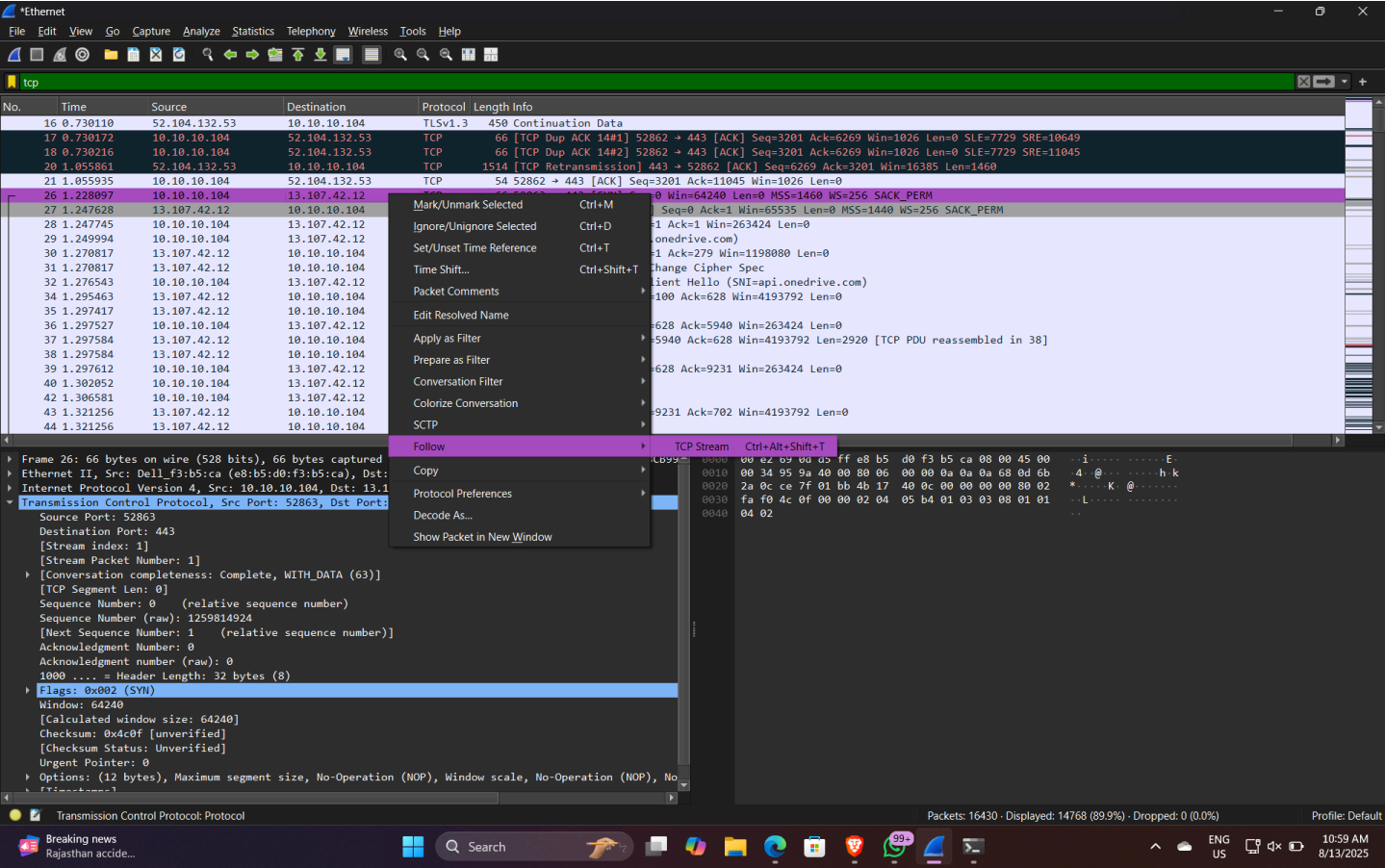


What to Check:

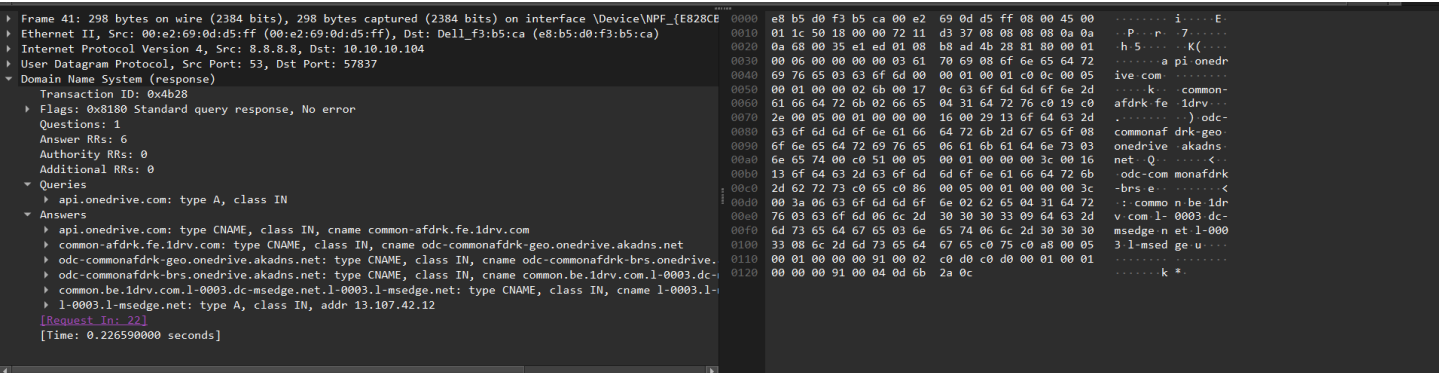
- **TCP handshakes** (SYN, SYN-ACK, ACK).
- Established sessions carrying HTTP/HTTPS.

Useful analysis actions

- Follow a TCP stream: Right-click a TCP packet → Follow → TCP Stream (shows full conversation).

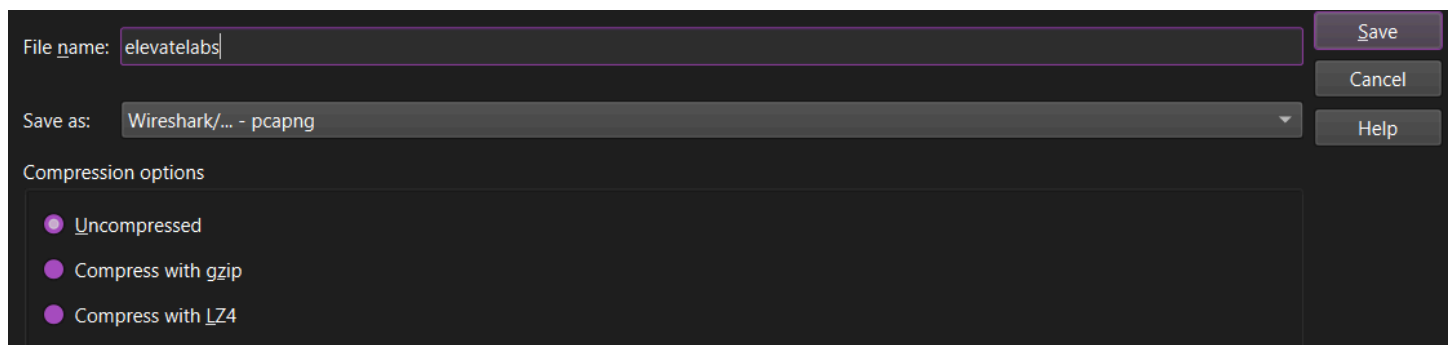


- DNS details: Click DNS packet, expand DNS section to see query name and answers.



Save and Document the Capture

- Stop Capture (red square icon).
- Go to File → Save As → Save as .pcapng.

A screenshot of the Wireshark 'Save' dialog box. The 'File name' field contains 'elevatelabs'. The 'Save as' dropdown menu is set to 'Wireshark/... - pcapng'. The 'Compression options' section shows three radio buttons: 'Uncompressed' (selected), 'Compress with gzip', and 'Compress with LZ4'. On the right side, there are three buttons: 'Save', 'Cancel', and 'Help'.

File name:

Save as:

Compression options

- ☒ Uncompressed
- ☐ Compress with gzip
- ☐ Compress with LZ4

Analysis :

The Wireshark capture contained a mix of protocols typical for normal browsing and network activity:

- **DNS (Domain Name System)** traffic was observed, resolving domain names such as openai.com and example.com into IP addresses. All queries were sent to the local DNS server (192.168.1.1), which returned valid responses.
- **ICMP (Internet Control Message Protocol)** packets showed echo requests and replies (ping) to Google's public DNS server (8.8.8.8), confirming that the host had connectivity to the internet.
- **TCP (Transmission Control Protocol)** was present as the transport layer for most application traffic.
- **TLS (Transport Layer Security)** traffic indicated secure HTTPS communication with remote web servers. The packet details showed Client Hello and Server Hello messages, with the Server Name Indication (SNI) revealing the target domains. Payload content was encrypted, as expected.
- **ARP (Address Resolution Protocol)** packets were seen for resolving MAC addresses of devices on the local network. No suspicious packets, malformed traffic, or signs of scanning/attacks were detected during the observation period. Traffic patterns and endpoint IP addresses matched the intentional actions performed during the test (web browsing, DNS lookups, pings).