Task 5: Network Packet Capture and Analysis Using Wireshark

1. Objective

To capture live network traffic using Wireshark, identify and analyse the packets for three main protocols (DNS, TCP, ICMP), and understand the role each plays in network communications.

2. What is Wireshark?

Wireshark is a free, open-source tool that captures and inspects network traffic at the packet level. It's widely used in cybersecurity for:

- Network troubleshooting
- Protocol analysis
- Security investigations

It allows you to **see exactly what data is travelling over your network**.

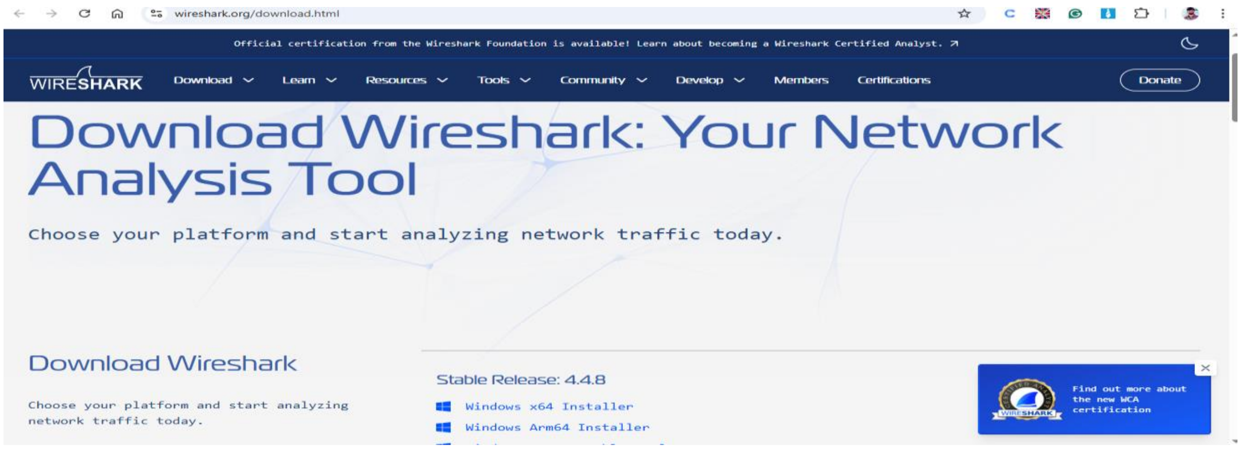
3. Tools Used

- **Wireshark** (latest version)
- Windows 10 laptop (test system and traffic source)
- Chrome browser (for website visits)
- Snipping Tool (for screenshots)

4. Step-by-Step Process

Step 1: Install Wireshark

- Downloaded from https://www.wireshark.org/download.html
- Completed installation with default settings.



Official certification from the Wireshark Foundation is available! Learn about becoming a Wireshark Certified Analyst. ↗

Download Wireshark: Your Network Analysis Tool

Choose your platform and start analyzing network traffic today.

Download Wireshark

Choose your platform and start analyzing network traffic today.

Stable Release: 4.4.8

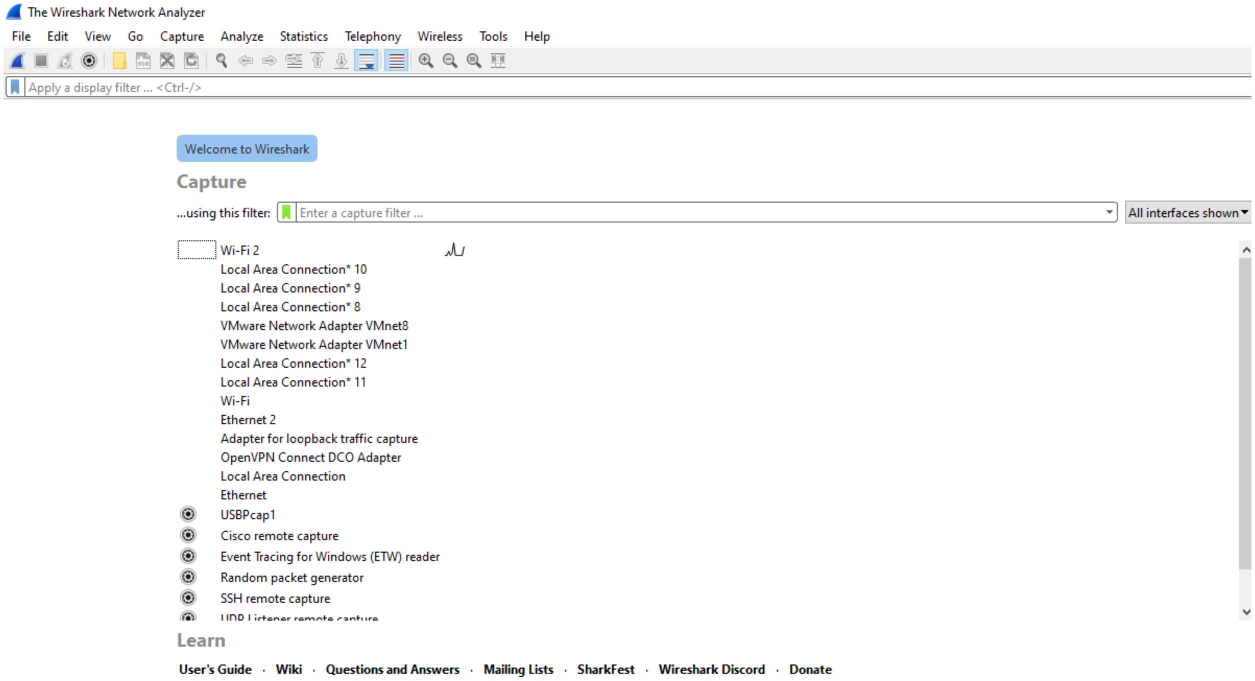
Windows x64 Installer

Windows Arm64 Installer

Find out more about the new WCA certification

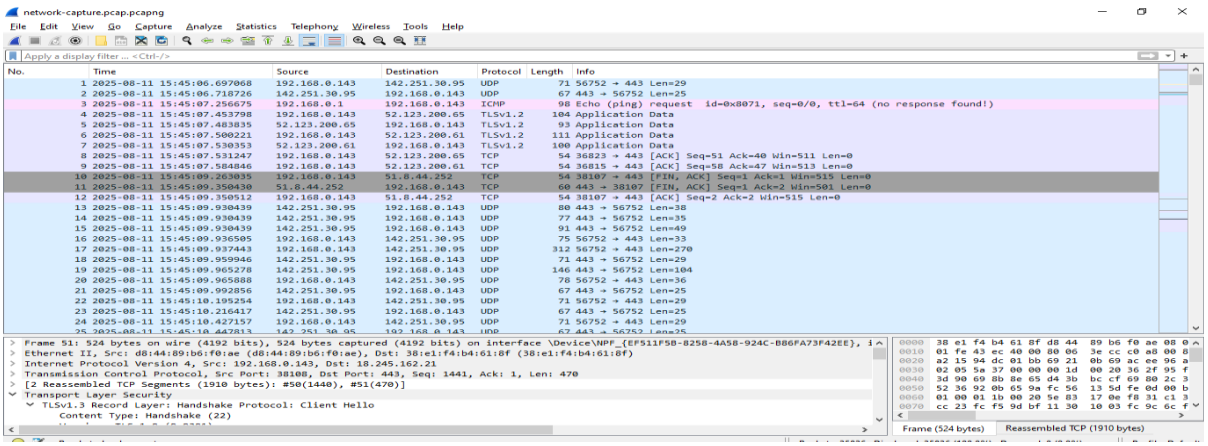
Step 2: Start Live Capture

- Launched Wireshark.
- Selected my active network interface (**Wi-Fi 2**).
- Clicked the blue shark fin icon to start capture.



Step 3: Generate Network Traffic

- Opened browser and visited a few websites (e.g., roadmap.sh).
- This generated DNS queries, TCP traffic, and ICMP echo requests/replies.


network-capture.pcap.pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Frame (524 bytes)
Reassembled TCP (1910 bytes)

```
No.   Time                        Source          Destination     Protocol Length Info
    1 2025-08-11 15:45:06.697068  192.168.0.143   142.251.30.95   UDP         71 56752 → 443 Len=29
    2 2025-08-11 15:45:06.718726  142.251.30.95   192.168.0.143   UDP         67 443 → 56752 Len=25
    3 2025-08-11 15:45:07.256675  192.168.0.1     192.168.0.143   ICMP        98 Echo (ping) request  id=0x8071, seq=0/0, ttl=64 (no response found!)
    4 2025-08-11 15:45:07.453798  192.168.0.143   52.123.200.65   TLSv1.2    104 Application Data
    5 2025-08-11 15:45:07.483835  52.123.200.65   192.168.0.143   TLSv1.2     93 Application Data
    6 2025-08-11 15:45:07.500221  192.168.0.143   52.123.200.61   TLSv1.2    111 Application Data
    7 2025-08-11 15:45:07.530353  52.123.200.61   192.168.0.143   TLSv1.2    100 Application Data
    8 2025-08-11 15:45:07.531247  192.168.0.143   52.123.200.65   TCP         54 36823 → 443 [ACK] Seq=51 Ack=40 Win=511 Len=0
    9 2025-08-11 15:45:07.584846  192.168.0.143   52.123.200.61   TCP         54 36815 → 443 [ACK] Seq=58 Ack=47 Win=513 Len=0
   10 2025-08-11 15:45:09.263035  192.168.0.143   51.8.44.252     TCP         54 38107 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
   11 2025-08-11 15:45:09.350430  51.8.44.252     192.168.0.143   TCP         60 443 → 38107 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
   12 2025-08-11 15:45:09.350512  192.168.0.143   51.8.44.252     TCP         54 38107 → 443 [ACK] Seq=2 Ack=2 Win=515 Len=0
   13 2025-08-11 15:45:09.930439  142.251.30.95   192.168.0.143   UDP         80 443 → 56752 Len=38
   14 2025-08-11 15:45:09.930439  142.251.30.95   192.168.0.143   UDP         77 443 → 56752 Len=35
   15 2025-08-11 15:45:09.930439  142.251.30.95   192.168.0.143   UDP         91 443 → 56752 Len=49
   16 2025-08-11 15:45:09.936505  192.168.0.143   142.251.30.95   UDP         75 56752 → 443 Len=33
   17 2025-08-11 15:45:09.937443  192.168.0.143   142.251.30.95   UDP        312 56752 → 443 Len=270
   18 2025-08-11 15:45:09.959946  142.251.30.95   192.168.0.143   UDP         71 443 → 56752 Len=29
   19 2025-08-11 15:45:09.965278  142.251.30.95   192.168.0.143   UDP        146 443 → 56752 Len=104
   20 2025-08-11 15:45:09.965888  192.168.0.143   142.251.30.95   UDP         78 56752 → 443 Len=36
   21 2025-08-11 15:45:09.992856  142.251.30.95   192.168.0.143   UDP         67 443 → 56752 Len=25
   22 2025-08-11 15:45:10.195254  192.168.0.143   142.251.30.95   UDP         71 56752 → 443 Len=29
   23 2025-08-11 15:45:10.216417  142.251.30.95   192.168.0.143   UDP         67 443 → 56752 Len=25
   24 2025-08-11 15:45:10.427157  192.168.0.143   142.251.30.95   UDP         71 56752 → 443 Len=29
   25 2025-08-11 15:45:10.447813  142.251.30.95   192.168.0.143   UDP         67 443 → 56752 Len=25
```

```
> Frame 51: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface \Device\NPF_{EF511F5B-8258-4A58-924C-B86FA73F42EE}, i
> Ethernet II, Src: d8:44:89:b6:f0:ae (d8:44:89:b6:f0:ae), Dst: 38:e1:f4:b4:61:8f (38:e1:f4:b4:61:8f)
> Internet Protocol Version 4, Src: 192.168.0.143, Dst: 18.245.162.21
> Transmission Control Protocol, Src Port: 38108, Dst Port: 443, Seq: 1441, Ack: 1, Len: 470
> [2 Reassembled TCP Segments (1910 bytes): #50(1440), #51(470)]
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
```

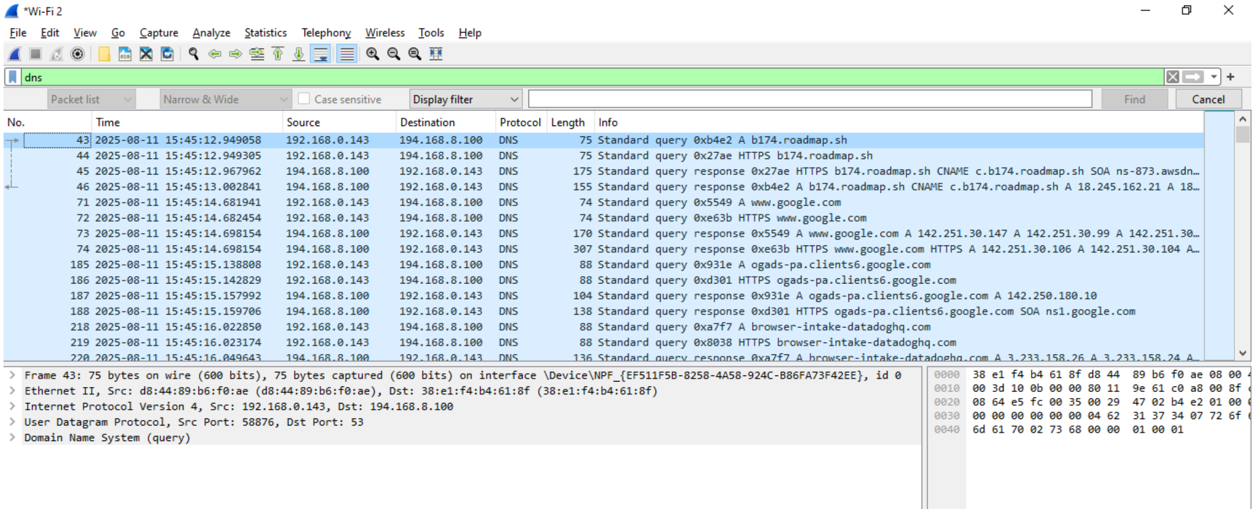
```
0000  38 e1 f4 b4 61 8f d8 44  89 b6 f0 ae 08 0
0010  01 fe 43 ec 40 00 80 06  3e cc c0 a8 00 8
0020  a2 15 94 dc 01 bb 69 21  0b 69 ac ee 96 a
0030  02 05 5a 37 00 00 00 1d  00 20 36 2f 95 f
0040  3d 90 69 8b 8e 65 d4 3b  bc cf 69 80 2c 3
0050  52 36 92 0b 65 9a fc 56  13 5d fe 0d 00 b
0060  01 00 01 1b 00 20 5e 83  17 0e f8 31 c1 3
0070  cc 23 fc f5 9d bf 11 30  10 03 fc 9c 6c f
```

Step 4: Stop Capture

- Let capture run for about 2 minutes.
- Stopped capture by clicking the red square icon.

Step 5: Filter by Protocol

- In the filter bar:
- For **DNS**: dns


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
□ Case sensitive
Find
Cancel

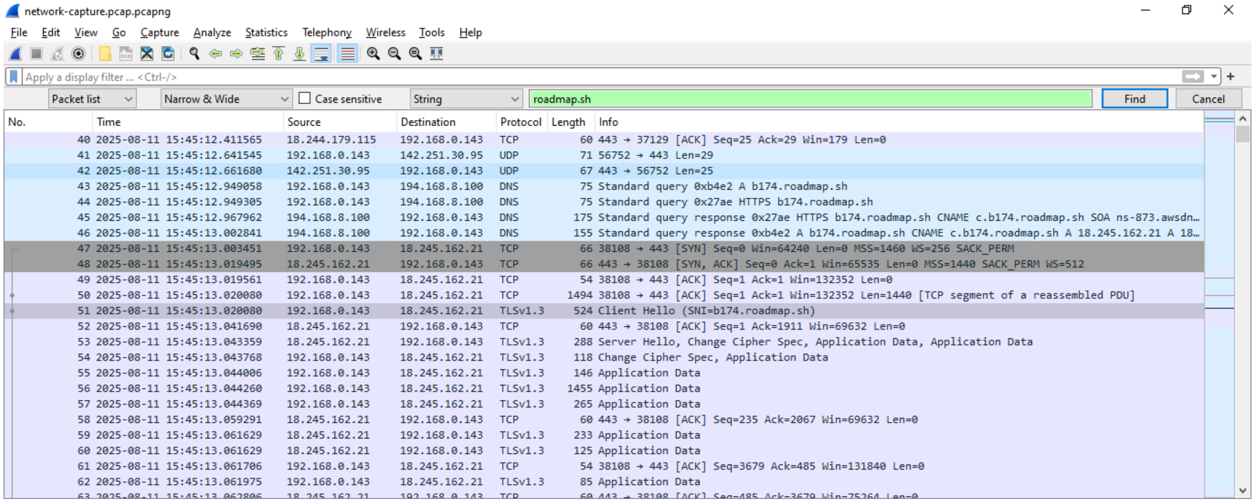
dns

Display filter

```
No.  Time                           Source          Destination     Protocol Length Info
  43 2025-08-11 15:45:12.949058     192.168.0.143   194.168.8.100   DNS        75 Standard query 0xb4e2 A b174.roadmap.sh
  44 2025-08-11 15:45:12.949305     192.168.0.143   194.168.8.100   DNS        75 Standard query 0x27ae HTTPS b174.roadmap.sh
  45 2025-08-11 15:45:12.967962     194.168.8.100   192.168.0.143   DNS       175 Standard query response 0x27ae HTTPS b174.roadmap.sh CNAME c.b174.roadmap.sh SOA ns-873.awsdn…
  46 2025-08-11 15:45:13.002841     194.168.8.100   192.168.0.143   DNS       155 Standard query response 0xb4e2 A b174.roadmap.sh CNAME c.b174.roadmap.sh A 18.245.162.21 A 18…
  71 2025-08-11 15:45:14.681941     192.168.0.143   194.168.8.100   DNS        74 Standard query 0x5549 A www.google.com
  72 2025-08-11 15:45:14.682454     192.168.0.143   194.168.8.100   DNS        74 Standard query 0xe63b HTTPS www.google.com
  73 2025-08-11 15:45:14.698154     194.168.8.100   192.168.0.143   DNS       170 Standard query response 0x5549 A www.google.com A 142.251.30.147 A 142.251.30.99 A 142.251.30…
  74 2025-08-11 15:45:14.698154     194.168.8.100   192.168.0.143   DNS       307 Standard query response 0xe63b HTTPS www.google.com HTTPS A 142.251.30.106 A 142.251.30.104 A…
 185 2025-08-11 15:45:15.138808     192.168.0.143   194.168.8.100   DNS        88 Standard query 0x931e A ogads-pa.clients6.google.com
 186 2025-08-11 15:45:15.142829     192.168.0.143   194.168.8.100   DNS        88 Standard query 0xd301 HTTPS ogads-pa.clients6.google.com
 187 2025-08-11 15:45:15.157992     194.168.8.100   192.168.0.143   DNS       104 Standard query response 0x931e A ogads-pa.clients6.google.com A 142.250.180.10
 188 2025-08-11 15:45:15.159706     194.168.8.100   192.168.0.143   DNS       138 Standard query response 0xd301 HTTPS ogads-pa.clients6.google.com SOA ns1.google.com
 218 2025-08-11 15:45:16.022850     192.168.0.143   194.168.8.100   DNS        88 Standard query 0xa7f7 A browser-intake-datadoghq.com
 219 2025-08-11 15:45:16.023174     192.168.0.143   194.168.8.100   DNS        88 Standard query 0x8038 HTTPS browser-intake-datadoghq.com
 220 2025-08-11 15:45:16.049643     194.168.8.100   192.168.0.143   DNS       136 Standard query response 0xa7f7 A browser-intake-datadoghq.com A 3.233.158.26 A 3.233.158.24 A…
```

```
> Frame 43: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{EF511F5B-8258-4A58-924C-B86FA73F42EE}, id 0
> Ethernet II, Src: d8:44:89:b6:f0:ae (d8:44:89:b6:f0:ae), Dst: 38:e1:f4:b4:61:8f (38:e1:f4:b4:61:8f)
> Internet Protocol Version 4, Src: 192.168.0.143, Dst: 194.168.8.100
> User Datagram Protocol, Src Port: 58876, Dst Port: 53
> Domain Name System (query)
```

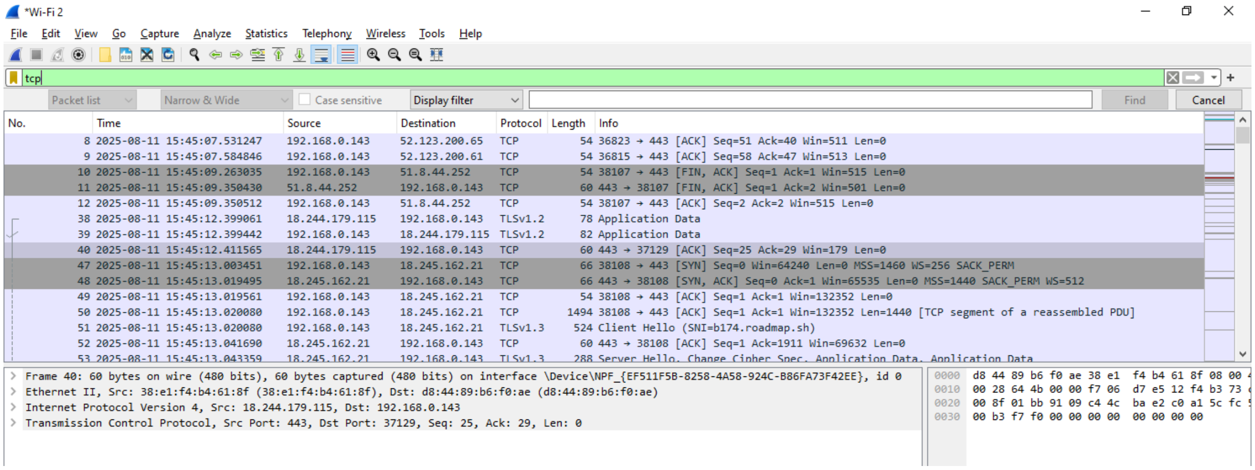
```
0000  38 e1 f4 b4 61 8f d8 44  89 b6 f0 ae 08 00
0010  00 3d 10 0b 00 00 80 11  9e 61 c0 a8 00 8f
0020  08 64 e5 fc 00 35 00 29  47 02 b4 e2 01 00
0030  00 00 00 00 00 00 04 62  31 37 34 07 72 6f
0040  6d 61 70 02 73 68 00 00  01 00 01
```


network-capture.pcap.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Find
Cancel

Packet list | Narrow & Wide | □ Case sensitive | String | roadmap.sh

```
No.  Time                           Source          Destination     Protocol Length Info
  40 2025-08-11 15:45:12.411565     18.244.179.115  192.168.0.143   TCP        60 443 → 37129 [ACK] Seq=25 Ack=29 Win=179 Len=0
  41 2025-08-11 15:45:12.641545     192.168.0.143   142.251.30.95   UDP        71 56752 → 443 Len=29
  42 2025-08-11 15:45:12.661680     142.251.30.95   192.168.0.143   UDP        67 443 → 56752 Len=25
  43 2025-08-11 15:45:12.949058     192.168.0.143   194.168.8.100   DNS        75 Standard query 0xb4e2 A b174.roadmap.sh
  44 2025-08-11 15:45:12.949305     192.168.0.143   194.168.8.100   DNS        75 Standard query 0x27ae HTTPS b174.roadmap.sh
  45 2025-08-11 15:45:12.967962     194.168.8.100   192.168.0.143   DNS       175 Standard query response 0x27ae HTTPS b174.roadmap.sh CNAME c.b174.roadmap.sh SOA ns-873.awsdn…
  46 2025-08-11 15:45:13.002841     194.168.8.100   192.168.0.143   DNS       155 Standard query response 0xb4e2 A b174.roadmap.sh CNAME c.b174.roadmap.sh A 18.245.162.21 A 18…
  47 2025-08-11 15:45:13.003451     192.168.0.143   18.245.162.21   TCP        66 38108 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  48 2025-08-11 15:45:13.019495     18.245.162.21   192.168.0.143   TCP        66 443 → 38108 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=512
  49 2025-08-11 15:45:13.019561     192.168.0.143   18.245.162.21   TCP        54 38108 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  50 2025-08-11 15:45:13.020080     192.168.0.143   18.245.162.21   TCP      1494 38108 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=1440 [TCP segment of a reassembled PDU]
  51 2025-08-11 15:45:13.020080     192.168.0.143   18.245.162.21   TLSv1.3   524 Client Hello (SNI=b174.roadmap.sh)
  52 2025-08-11 15:45:13.041690     18.245.162.21   192.168.0.143   TCP        60 443 → 38108 [ACK] Seq=1 Ack=1911 Win=69632 Len=0
  53 2025-08-11 15:45:13.043359     18.245.162.21   192.168.0.143   TLSv1.3   288 Server Hello, Change Cipher Spec, Application Data, Application Data
  54 2025-08-11 15:45:13.043768     192.168.0.143   18.245.162.21   TLSv1.3   118 Change Cipher Spec, Application Data
  55 2025-08-11 15:45:13.044006     192.168.0.143   18.245.162.21   TLSv1.3   146 Application Data
  56 2025-08-11 15:45:13.044260     192.168.0.143   18.245.162.21   TLSv1.3  1455 Application Data
  57 2025-08-11 15:45:13.044369     192.168.0.143   18.245.162.21   TLSv1.3   265 Application Data
  58 2025-08-11 15:45:13.059291     18.245.162.21   192.168.0.143   TCP        60 443 → 38108 [ACK] Seq=235 Ack=2067 Win=69632 Len=0
  59 2025-08-11 15:45:13.061629     18.245.162.21   192.168.0.143   TLSv1.3   233 Application Data
  60 2025-08-11 15:45:13.061629     18.245.162.21   192.168.0.143   TLSv1.3   125 Application Data
  61 2025-08-11 15:45:13.061706     192.168.0.143   18.245.162.21   TCP        54 38108 → 443 [ACK] Seq=3679 Ack=485 Win=131840 Len=0
  62 2025-08-11 15:45:13.061975     192.168.0.143   18.245.162.21   TLSv1.3    85 Application Data
  63 2025-08-11 15:45:13.062806     18.245.162.21   192.168.0.143   TCP        60 443 → 38108 [ACK] Seq=485 Ack=3679 Win=75264 Len=0
```

- For **TCP**: tcp



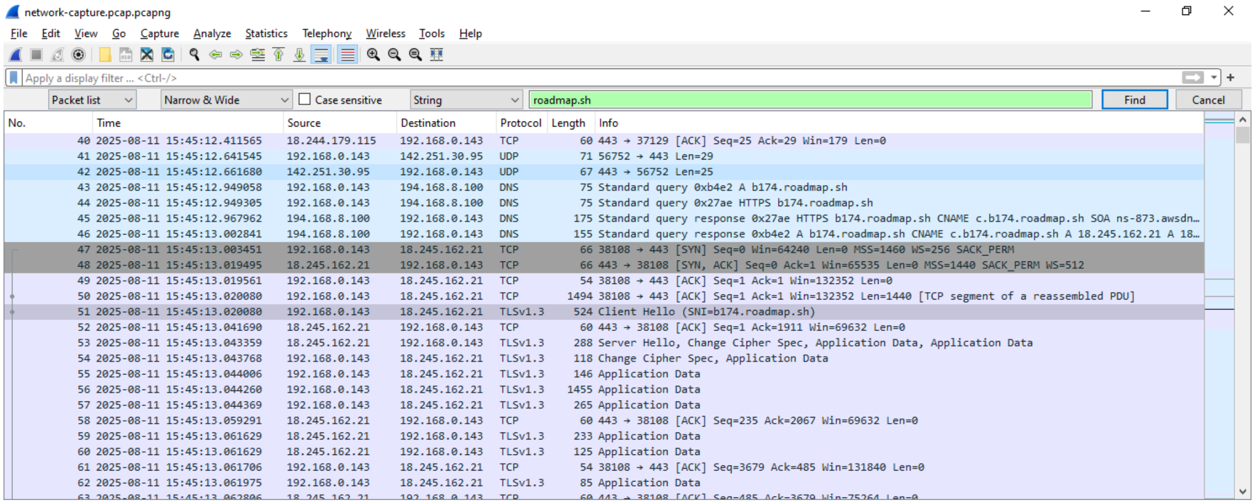
tcp

Display filter

```
No.   Time                         Source           Destination      Protocol Length Info
    8 2025-08-11 15:45:07.531247   192.168.0.143    52.123.200.65    TCP        54 36823 → 443 [ACK] Seq=51 Ack=40 Win=511 Len=0
    9 2025-08-11 15:45:07.584846   192.168.0.143    52.123.200.61    TCP        54 36815 → 443 [ACK] Seq=58 Ack=47 Win=513 Len=0
   10 2025-08-11 15:45:09.263035   192.168.0.143    51.8.44.252      TCP        54 38107 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
   11 2025-08-11 15:45:09.350430   51.8.44.252      192.168.0.143    TCP        60 443 → 38107 [FIN, ACK] Seq=1 Ack=2 Win=501 Len=0
   12 2025-08-11 15:45:09.350512   192.168.0.143    51.8.44.252      TCP        54 38107 → 443 [ACK] Seq=2 Ack=2 Win=515 Len=0
   38 2025-08-11 15:45:12.399061   18.244.179.115   192.168.0.143    TLSv1.2    78 Application Data
   39 2025-08-11 15:45:12.399442   192.168.0.143    18.244.179.115   TLSv1.2    82 Application Data
   40 2025-08-11 15:45:12.411565   18.244.179.115   192.168.0.143    TCP        60 443 → 37129 [ACK] Seq=25 Ack=29 Win=179 Len=0
   47 2025-08-11 15:45:13.003451   192.168.0.143    18.245.162.21    TCP        66 38108 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   48 2025-08-11 15:45:13.019495   18.245.162.21    192.168.0.143    TCP        66 443 → 38108 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=512
   49 2025-08-11 15:45:13.019561   192.168.0.143    18.245.162.21    TCP        54 38108 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
   50 2025-08-11 15:45:13.020080   192.168.0.143    18.245.162.21    TCP      1494 38108 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=1440 [TCP segment of a reassembled PDU]
   51 2025-08-11 15:45:13.020080   192.168.0.143    18.245.162.21    TLSv1.3   524 Client Hello (SNI=b174.roadmap.sh)
   52 2025-08-11 15:45:13.041690   18.245.162.21    192.168.0.143    TCP        60 443 → 38108 [ACK] Seq=1 Ack=1911 Win=69632 Len=0
   53 2025-08-11 15:45:13.043359   18.245.162.21    192.168.0.143    TLSv1.3   288 Server Hello, Change Cipher Spec, Application Data, Application Data
```

```
> Frame 40: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{EF511F5B-8258-4A58-924C-B86FA73F42EE}, id 0
> Ethernet II, Src: 38:e1:f4:b4:61:8f (38:e1:f4:b4:61:8f), Dst: d8:44:89:b6:f0:ae (d8:44:89:b6:f0:ae)
> Internet Protocol Version 4, Src: 18.244.179.115, Dst: 192.168.0.143
> Transmission Control Protocol, Src Port: 443, Dst Port: 37129, Seq: 25, Ack: 29, Len: 0
```

```
0000  d8 44 89 b6 f0 ae 38 e1  f4 b4 61 8f 08 00
0010  00 28 64 4b 00 00 f7 06  d7 e5 12 f4 b3 73
0020  00 8f 01 bb 91 09 c4 4c  ba e2 c0 a1 5c fc
0030  00 b3 f7 f0 00 00 00 00  00 00 00 00
```

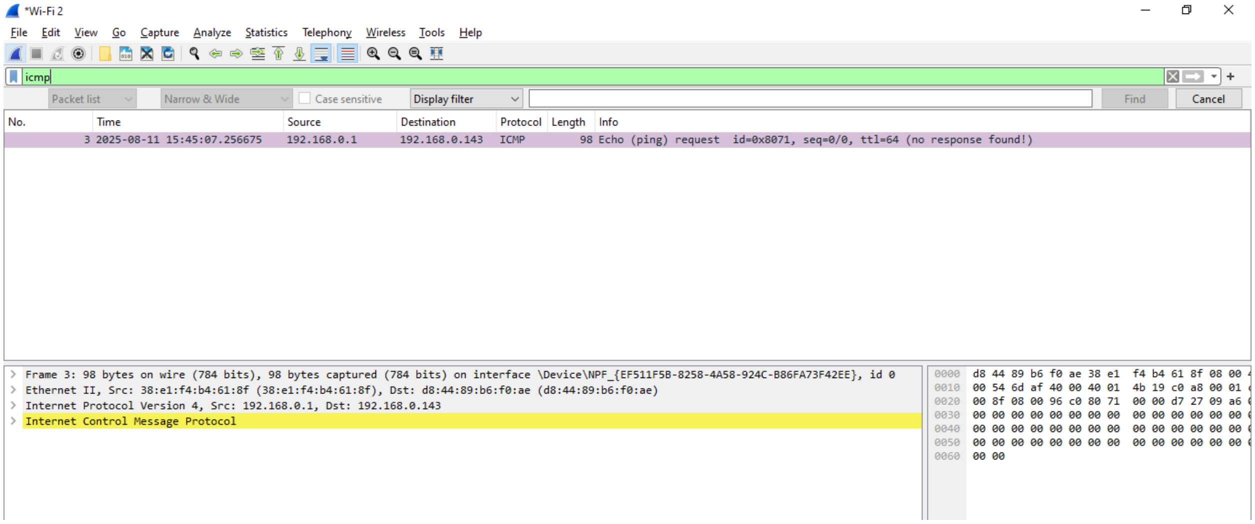


String

roadmap.sh

```
No.   Time                         Source           Destination      Protocol Length Info
   40 2025-08-11 15:45:12.411565   18.244.179.115   192.168.0.143    TCP        60 443 → 37129 [ACK] Seq=25 Ack=29 Win=179 Len=0
   41 2025-08-11 15:45:12.641545   192.168.0.143    142.251.30.95    UDP        71 56752 → 443 Len=29
   42 2025-08-11 15:45:12.661680   142.251.30.95    192.168.0.143    UDP        67 443 → 56752 Len=25
   43 2025-08-11 15:45:12.949058   192.168.0.143    194.168.8.100    DNS        75 Standard query 0xb4e2 A b174.roadmap.sh
   44 2025-08-11 15:45:12.949305   192.168.0.143    194.168.8.100    DNS        75 Standard query 0x27ae HTTPS b174.roadmap.sh
   45 2025-08-11 15:45:12.967962   194.168.8.100    192.168.0.143    DNS       175 Standard query response 0x27ae HTTPS b174.roadmap.sh CNAME c.b174.roadmap.sh SOA ns-873.awsdn…
   46 2025-08-11 15:45:13.002841   194.168.8.100    192.168.0.143    DNS       155 Standard query response 0xb4e2 A b174.roadmap.sh CNAME c.b174.roadmap.sh A 18.245.162.21 A 18…
   47 2025-08-11 15:45:13.003451   192.168.0.143    18.245.162.21    TCP        66 38108 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   48 2025-08-11 15:45:13.019495   18.245.162.21    192.168.0.143    TCP        66 443 → 38108 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=512
   49 2025-08-11 15:45:13.019561   192.168.0.143    18.245.162.21    TCP        54 38108 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
   50 2025-08-11 15:45:13.020080   192.168.0.143    18.245.162.21    TCP      1494 38108 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=1440 [TCP segment of a reassembled PDU]
   51 2025-08-11 15:45:13.020080   192.168.0.143    18.245.162.21    TLSv1.3   524 Client Hello (SNI=b174.roadmap.sh)
   52 2025-08-11 15:45:13.041690   18.245.162.21    192.168.0.143    TCP        60 443 → 38108 [ACK] Seq=1 Ack=1911 Win=69632 Len=0
   53 2025-08-11 15:45:13.043359   18.245.162.21    192.168.0.143    TLSv1.3   288 Server Hello, Change Cipher Spec, Application Data, Application Data
   54 2025-08-11 15:45:13.043768   192.168.0.143    18.245.162.21    TLSv1.3   118 Change Cipher Spec, Application Data
   55 2025-08-11 15:45:13.044006   192.168.0.143    18.245.162.21    TLSv1.3   146 Application Data
   56 2025-08-11 15:45:13.044260   192.168.0.143    18.245.162.21    TLSv1.3  1455 Application Data
   57 2025-08-11 15:45:13.044369   192.168.0.143    18.245.162.21    TLSv1.3   265 Application Data
   58 2025-08-11 15:45:13.059291   18.245.162.21    192.168.0.143    TCP        60 443 → 38108 [ACK] Seq=235 Ack=2067 Win=69632 Len=0
   59 2025-08-11 15:45:13.061629   18.245.162.21    192.168.0.143    TLSv1.3   233 Application Data
   60 2025-08-11 15:45:13.061629   18.245.162.21    192.168.0.143    TLSv1.3   125 Application Data
   61 2025-08-11 15:45:13.061706   192.168.0.143    18.245.162.21    TCP        54 38108 → 443 [ACK] Seq=3679 Ack=485 Win=131840 Len=0
   62 2025-08-11 15:45:13.061975   192.168.0.143    18.245.162.21    TLSv1.3    85 Application Data
   63 2025-08-11 15:45:13.062806   18.245.162.21    192.168.0.143    TCP        60 443 → 38108 [ACK] Seq=485 Ack=3679 Win=75264 Len=0
```

- For **ICMP**: icmp


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel

icmp

```
No.   Time                        Source        Destination    Protocol Length Info
    3 2025-08-11 15:45:07.256675  192.168.0.1   192.168.0.143  ICMP         98 Echo (ping) request  id=0x8071, seq=0/0, ttl=64 (no response found!)
```

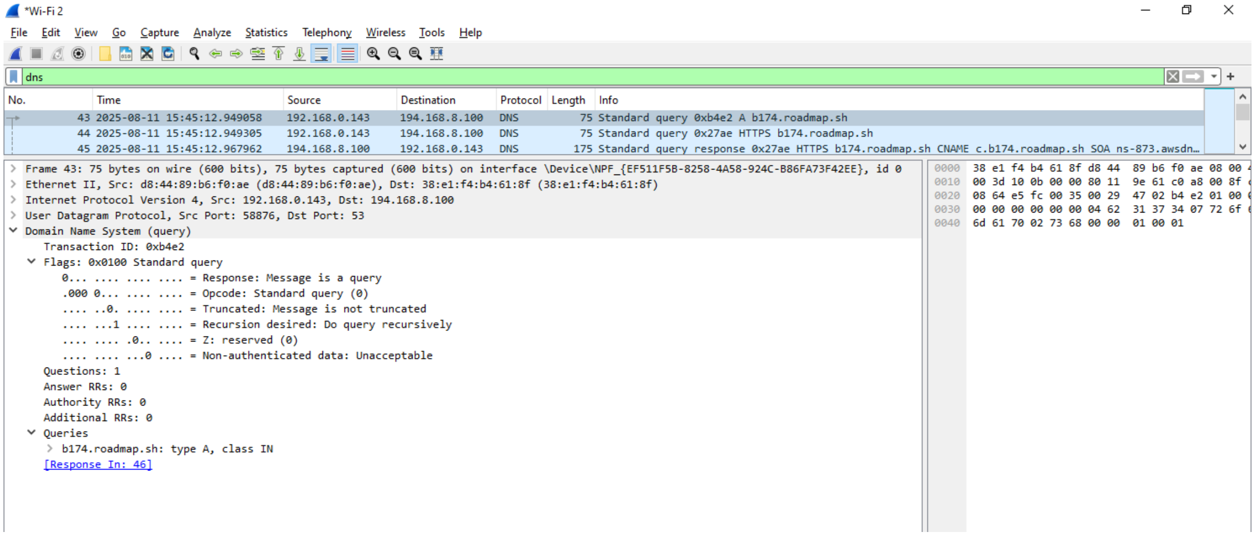
```
> Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{EF511F5B-8258-4A58-924C-B86FA73F42EE}, id 0
> Ethernet II, Src: 38:e1:f4:b4:61:8f (38:e1:f4:b4:61:8f), Dst: d8:44:89:b6:f0:ae (d8:44:89:b6:f0:ae)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.143
> Internet Control Message Protocol
```

```
0000  d8 44 89 b6 f0 ae 38 e1  f4 b4 61 8f 08 00
0010  00 54 6d af 40 00 40 01  4b 19 c0 a8 00 01
0020  00 8f 08 00 96 c0 80 71  00 00 d7 27 09 a6
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00
0060  00 00
```

- Verified packet lists changed according to each protocol.

Step 6: Inspect Packets

- Selected example packets to view details in the middle and bottom panes.
- Noted source/destination IPs, request/response types, and packet info.

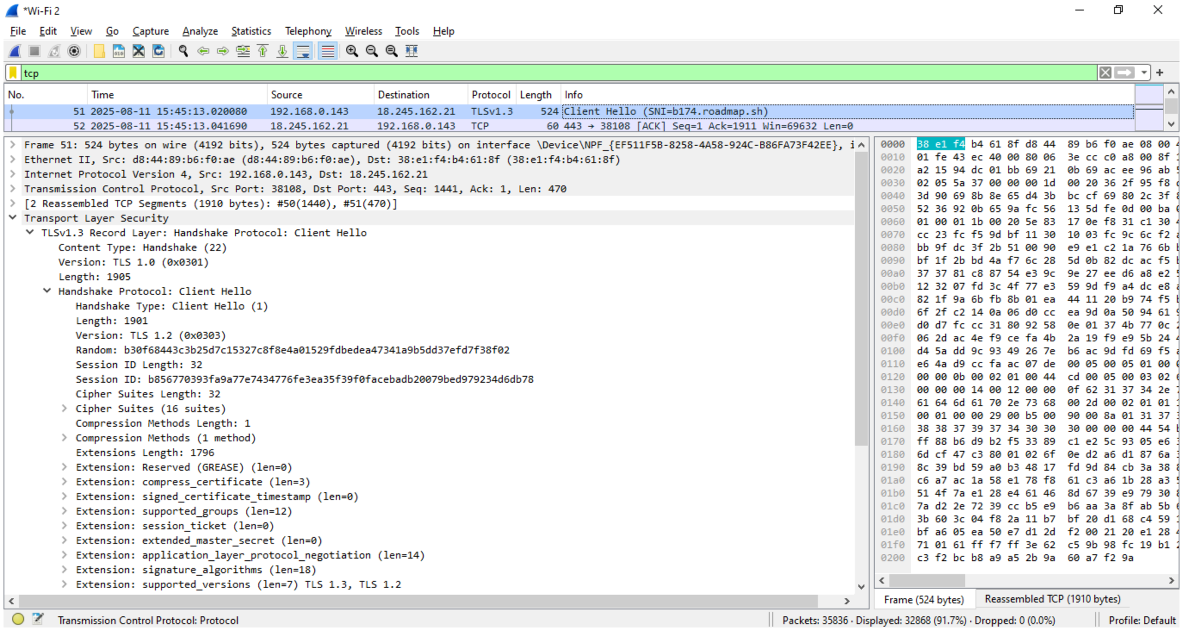

*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.   Time                        Source          Destination    Protocol Length Info
   43 2025-08-11 15:45:12.949058  192.168.0.143   194.168.8.100  DNS          75 Standard query 0xb4e2 A b174.roadmap.sh
   44 2025-08-11 15:45:12.949305  192.168.0.143   194.168.8.100  DNS          75 Standard query 0x27ae HTTPS b174.roadmap.sh
   45 2025-08-11 15:45:12.967962  194.168.8.100   192.168.0.143  DNS         175 Standard query response 0x27ae HTTPS b174.roadmap.sh CNAME c.b174.roadmap.sh SOA ns-873.awsdn…
```

```
> Frame 43: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{EF511F5B-8258-4A58-924C-B86FA73F42EE}, id 0
> Ethernet II, Src: d8:44:89:b6:f0:ae (d8:44:89:b6:f0:ae), Dst: 38:e1:f4:b4:61:8f (38:e1:f4:b4:61:8f)
> Internet Protocol Version 4, Src: 192.168.0.143, Dst: 194.168.8.100
> User Datagram Protocol, Src Port: 58876, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xb4e2
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > b174.roadmap.sh: type A, class IN
    [Response In: 46]
```

```
0000  38 e1 f4 b4 61 8f d8 44  89 b6 f0 ae 08 00
0010  00 3d 10 0b 00 00 80 11  9e 61 c0 a8 00 8f
0020  08 64 e5 fc 00 35 00 29  47 02 b4 e2 01 00
0030  00 00 00 00 00 00 04 62  31 37 34 07 72 6f
0040  6d 61 70 02 73 68 00 00  01 00 01
```



*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

```
No.   Time                        Source          Destination     Protocol  Length Info
   51 2025-08-11 15:45:13.020080  192.168.0.143   18.245.162.21   TLSv1.3      524 Client Hello (SNI=b174.roadmap.sh)
   52 2025-08-11 15:45:13.041690  18.245.162.21   192.168.0.143   TCP           60 443 → 38108 [ACK] Seq=1 Ack=1911 Win=69632 Len=0
```

```
> Frame 51: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface \Device\NPF_{EF511F5B-8258-4A58-924C-B86FA73F42EE}, i
> Ethernet II, Src: d8:44:89:b6:f0:ae (d8:44:89:b6:f0:ae), Dst: 38:e1:f4:b4:61:8f (38:e1:f4:b4:61:8f)
> Internet Protocol Version 4, Src: 192.168.0.143, Dst: 18.245.162.21
> Transmission Control Protocol, Src Port: 38108, Dst Port: 443, Seq: 1441, Ack: 1, Len: 470
> [2 Reassembled TCP Segments (1910 bytes): #50(1440), #51(470)]
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 1905
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 1901
        Version: TLS 1.2 (0x0303)
        Random: b30f68443c3b25d7c15327c8f8e4a01529fdbedea47341a9b5dd37efd7f38f02
        Session ID Length: 32
        Session ID: b856770393fa9a77e7434776fe3ea35f39f0facebadb20079bed979234d6db78
        Cipher Suites Length: 32
      > Cipher Suites (16 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 1796
      > Extension: Reserved (GREASE) (len=0)
      > Extension: compress_certificate (len=3)
      > Extension: signed_certificate_timestamp (len=0)
      > Extension: supported_groups (len=12)
      > Extension: session_ticket (len=0)
      > Extension: extended_master_secret (len=0)
      > Extension: application_layer_protocol_negotiation (len=14)
      > Extension: signature_algorithms (len=18)
      > Extension: supported_versions (len=7) TLS 1.3, TLS 1.2
```

```
0000  38 e1 f4 b4 61 8f d8 44  89 b6 f0 ae 08 00
0010  01 fe 43 ec 40 00 80 06  3e cc c0 a8 00 8f
0020  a2 15 94 dc 01 bb 69 21  0b 69 ac ee 96 ab
0030  02 05 5a 37 00 00 00 1d  00 20 36 2f 95 f8
0040  3d 90 69 8b 8e 65 d4 3b  bc cf 69 80 2c 3f
0050  52 36 92 0b 65 9a fc 56  13 5d fe 0d 00 ba
0060  01 00 01 1b 00 20 5e 83  17 0e f8 31 c1 30
0070  cc 23 fc f5 9d bf 11 30  10 03 fc 9c 6c f2
0080  bb 9f dc 3f 2b 51 00 90  e9 e1 c2 1a 76 6b
0090  bf 1f 2b bd 4a f7 6c 28  5d 0b 82 dc ac f5
00a0  37 37 81 c8 87 54 e3 9c  9e 27 ee d6 a8 e2
00b0  12 32 07 fd 3c 4f 77 e3  59 9d f9 a4 dc e8
00c0  82 1f 9a 6b fb 8b 01 ea  44 11 20 b9 74 f5
00d0  6f 2f c2 14 0a 06 d0 cc  ea 9d 0a 50 94 61
00e0  d0 d7 fc cc 31 80 92 58  0e 01 37 4b 77 0c
00f0  06 2d ac 4e f9 ce fa 4b  2a 19 f9 e9 5b 24
0100  d4 5a dd 9c 93 49 26 7e  b6 ac 9d fd 69 f5
0110  e6 4a d9 cc fa ac 07 de  00 05 00 05 01 00
0120  00 00 0b 00 02 01 00 44  cd 00 05 00 03 02
0130  00 00 00 14 00 12 00 00  0f 62 31 37 34 2e
0140  61 64 6d 61 70 2e 73 68  00 2d 00 02 01 01
0150  00 01 00 00 29 00 b5 00  90 00 8a 01 31 37
0160  38 38 37 39 37 34 30 30  30 00 00 00 44 54
0170  ff 88 b6 d9 b2 f5 33 89  c1 e2 5c 93 05 e6
0180  6d cf 47 c3 80 01 02 6f  0e d2 a6 d1 87 6a
0190  8c 39 bd 59 a0 b3 48 17  fd 9d 84 cb 3a 38
01a0  c6 a7 ac 1a 58 e1 78 f8  61 c3 a6 1b 28 a3
01b0  51 4f 7a e1 28 e4 61 46  8d 67 39 e9 79 30
01c0  7a d2 2e 72 39 cc b5 e9  b6 aa 3a 8f ab 5b
01d0  3b 60 3c 04 f8 2a 11 b7  bf 20 d1 68 c4 59
01e0  bf a6 05 ea 50 e7 d1 2d  f2 00 21 20 e1 28
01f0  71 01 61 ff f7 ff 3e 62  c5 9b 98 fc 19 b1
0200  c3 f2 bc b8 a9 a5 2b 9a  60 a7 f2 9a
```

```
Transmission Control Protocol: Protocol
Packets: 35836 · Displayed: 32868 (91.7%) · Dropped: 0 (0.0%)
Profile: Default
```

Step 7: Save the Capture

- File → Save As → network-capture.pcap
- This file is part of deliverables.

5. Protocols Identified & Details

Protocol	Description	Example from Capture
DNS	Resolves human-readable domain names into IP addresses	Query for roadmap.sh and its response
TCP	Provides reliable, ordered data delivery over the network	TCP handshake to a remote web server
ICMP	Used for connectivity tests and diagnostics	Echo request/reply from roadmap.sh

6. Summary & Learning

By using Wireshark, I learned how to:

- Start and stop live traffic captures.
- Filter for specific protocols.
- Identify the role of DNS, TCP, and ICMP in daily network activity.
- Save and document packet captures for analysis.

This task improved my understanding of network operations and protocol-level communication, which is essential for cybersecurity analysis.