Task 5: Capture and Analyze Network Traffic Using Wireshark

1. Objective

Capture live network packets using Wireshark and identify different protocols to understand basic network communication.

2. Tools Used

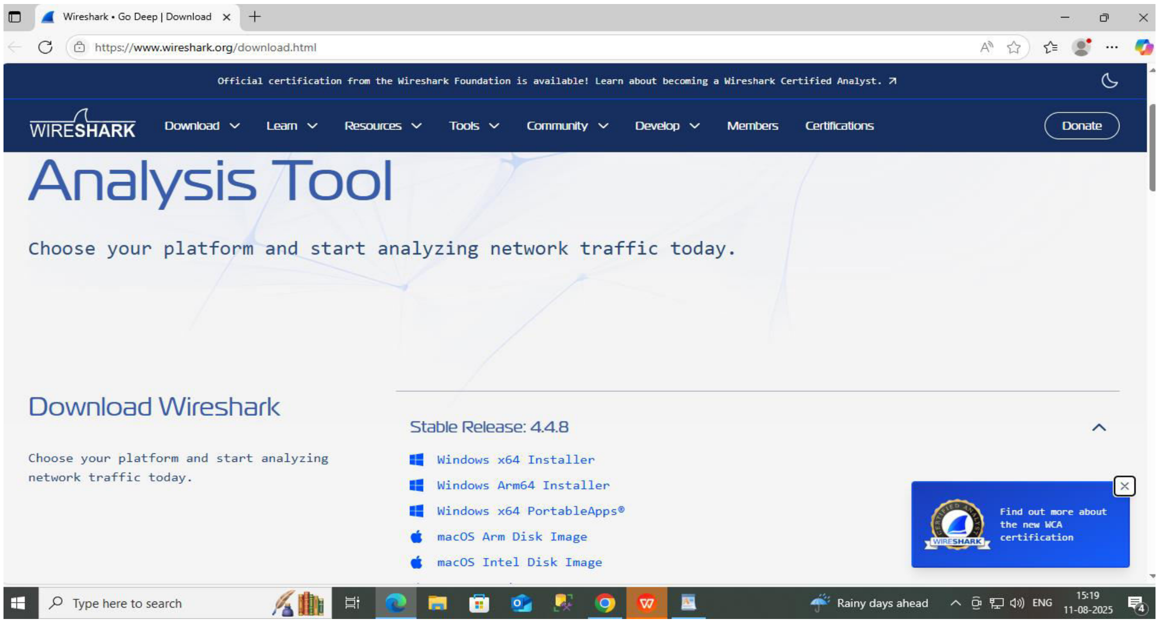
Wireshark (Latest version)

3. Steps Performed

Step 1 – Install Wireshark

Download from https://www.wireshark.org/download.html

Install with WinPcap/Npcap option enabled.



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

Analysis Tool

Choose your platform and start analyzing network traffic today.

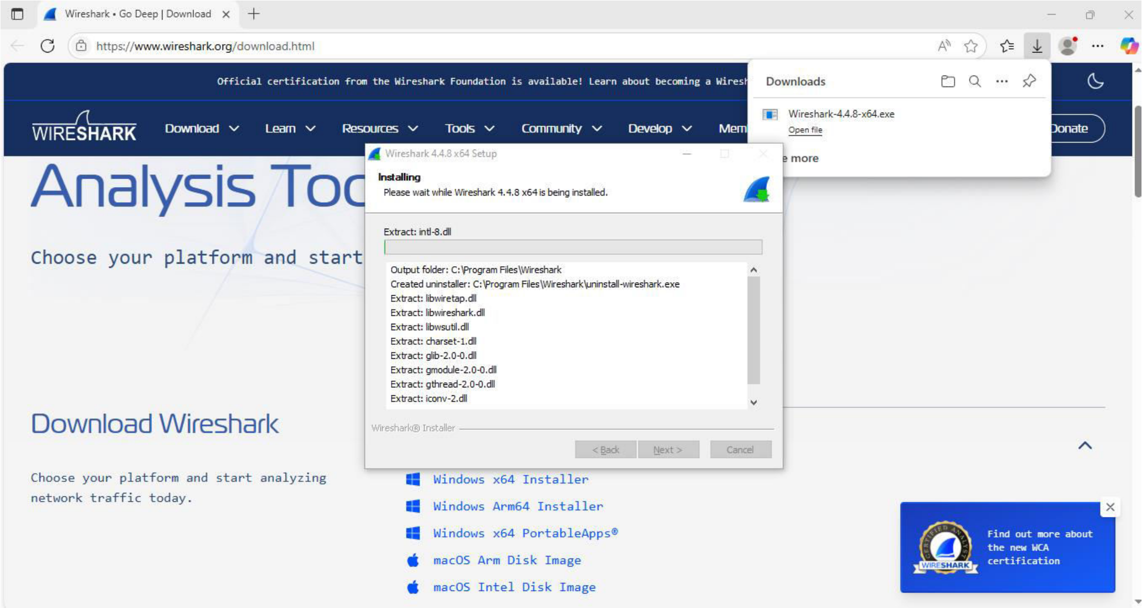
Download Wireshark

Choose your platform and start analyzing network traffic today.

Stable Release: 4.4.8

- Windows x64 Installer
- Windows Arm64 Installer
- Windows x64 PortableApps®
- macOS Arm Disk Image
- macOS Intel Disk Image

Find out more about the new WCA certification



Official certification from the Wireshark Foundation is available! Learn about becoming a Wiresh

Analysis Toc

Choose your platform and start

Download Wireshark

Choose your platform and start analyzing network traffic today.

Find out more about the new WCA certification

Wireshark 4.4.8 x64 Setup

Installing

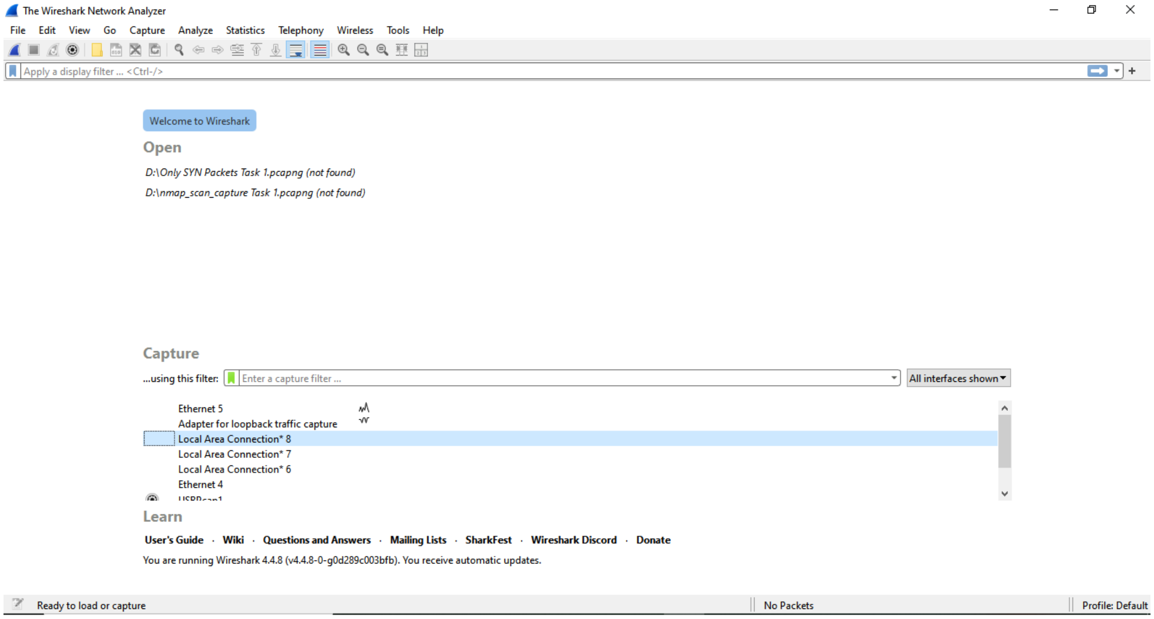
Please wait while Wireshark 4.4.8 x64 is being installed.

Extract: intl-8.dll

```
Output folder: C:\Program Files\Wireshark
Created uninstaller: C:\Program Files\Wireshark\uninstall-wireshark.exe
Extract: libwiretap.dll
Extract: libwireshark.dll
Extract: libwsutil.dll
Extract: charset-1.dll
Extract: glib-2.0-0.dll
Extract: gmodule-2.0-0.dll
Extract: gthread-2.0-0.dll
Extract: iconv-2.dll
```

Step 2 – Launch Wireshark & Select Interface

Open Wireshark.


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

D:\Only SYN Packets Task 1.pcapng (not found)

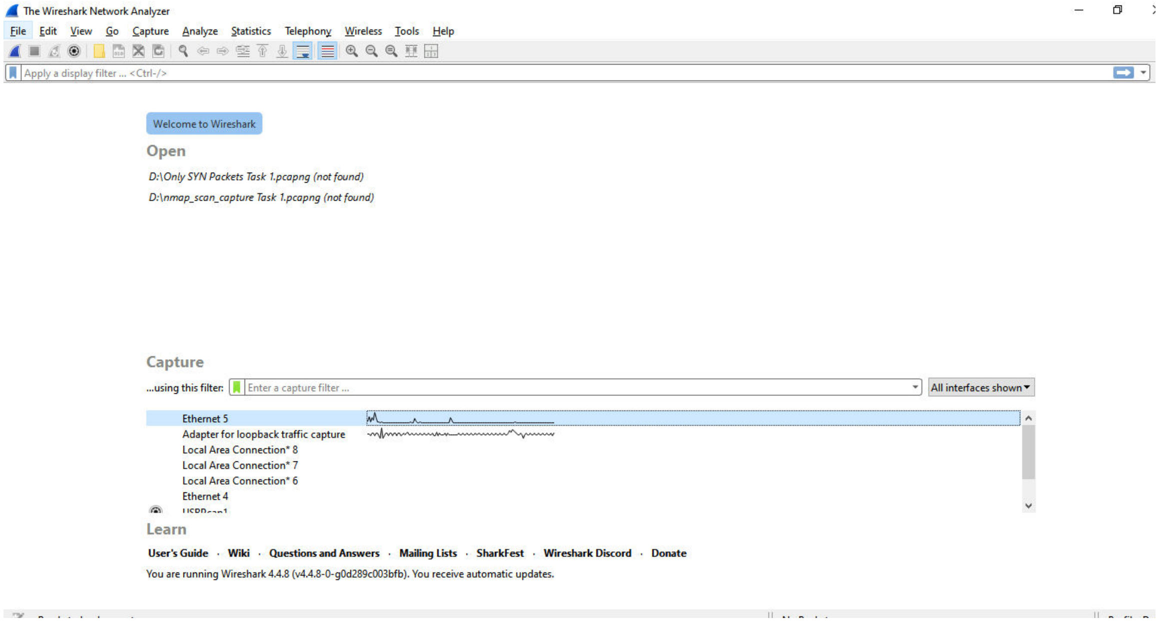
D:\nmap_scan_capture Task 1.pcapng (not found)

```
Ethernet 5
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Ethernet 4
USBPcap1
```

You are running Wireshark 4.4.8 (v4.4.8-0-g0d289c003bfb). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Select your **active network interface** (Ethernet 5)


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Open

D:\Only SYN Packets Task 1.pcapng (not found)

D:\nmap_scan_capture Task 1.pcapng (not found)

Capture

...using this filter: Enter a capture filter ...   All interfaces shown

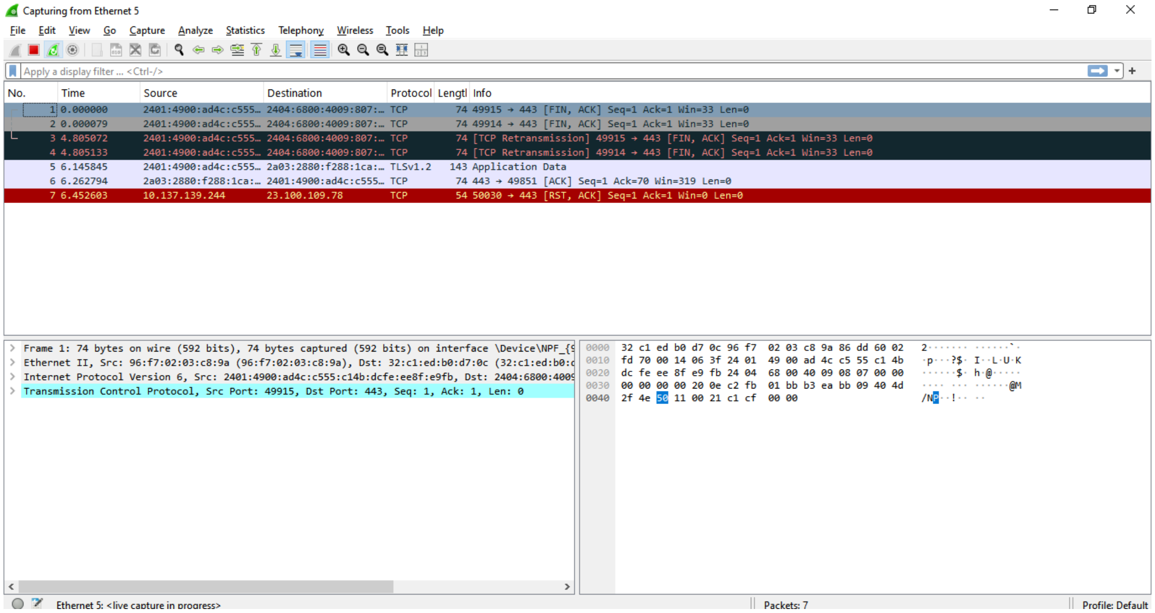
- Ethernet 5
- Adapter for loopback traffic capture
- Local Area Connection* 8
- Local Area Connection* 7
- Local Area Connection* 6
- Ethernet 4

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.8 (v4.4.8-0-g0d289c003bfb). You receive automatic updates.

Click **Start Capturing Packets**.


Capturing from Ethernet 5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source                Destination           Protocol Lengtl Info
  1 0.000000  2401:4900:ad4c:c555… 2404:6800:4009:807:… TCP       74 49915 → 443 [FIN, ACK] Seq=1 Ack=1 Win=33 Len=0
  2 0.000079  2401:4900:ad4c:c555… 2404:6800:4009:807:… TCP       74 49914 → 443 [FIN, ACK] Seq=1 Ack=1 Win=33 Len=0
  3 4.805072  2401:4900:ad4c:c555… 2404:6800:4009:807:… TCP       74 [TCP Retransmission] 49915 → 443 [FIN, ACK] Seq=1 Ack=1 Win=33 Len=0
  4 4.805133  2401:4900:ad4c:c555… 2404:6800:4009:807:… TCP       74 [TCP Retransmission] 49914 → 443 [FIN, ACK] Seq=1 Ack=1 Win=33 Len=0
  5 6.145845  2401:4900:ad4c:c555… 2a03:2880:f288:1ca:… TLSv1.2  143 Application Data
  6 6.262794  2a03:2880:f288:1ca:… 2401:4900:ad4c:c555… TCP       74 443 → 49851 [ACK] Seq=1 Ack=70 Win=319 Len=0
  7 6.452603  10.137.139.244        23.100.109.78         TCP       54 50030 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{9
> Ethernet II, Src: 96:f7:02:03:c8:9a (96:f7:02:03:c8:9a), Dst: 32:c1:ed:b0:d7:0c (32:c1:ed:b0:d
> Internet Protocol Version 6, Src: 2401:4900:ad4c:c555:c14b:dcfe:ee8f:e9fb, Dst: 2404:6800:4009
> Transmission Control Protocol, Src Port: 49915, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

```
0000  32 c1 ed b0 d7 0c 96 f7  02 03 c8 9a 86 dd 60 02   2······· ······`·
0010  fd 70 00 14 06 3f 24 01  49 00 ad 4c c5 55 c1 4b   ·p···?$· I··L·U·K
0020  dc fe ee 8f e9 fb 24 04  68 00 40 09 08 07 00 00   ······$· h·@·····
0030  00 00 00 00 20 0e c2 fb  01 bb b3 ea bb 09 40 4d   ···· ··· ······@M
0040  2f 4e 50 11 00 21 c1 cf  00 00                     /NP··!·· ··
```

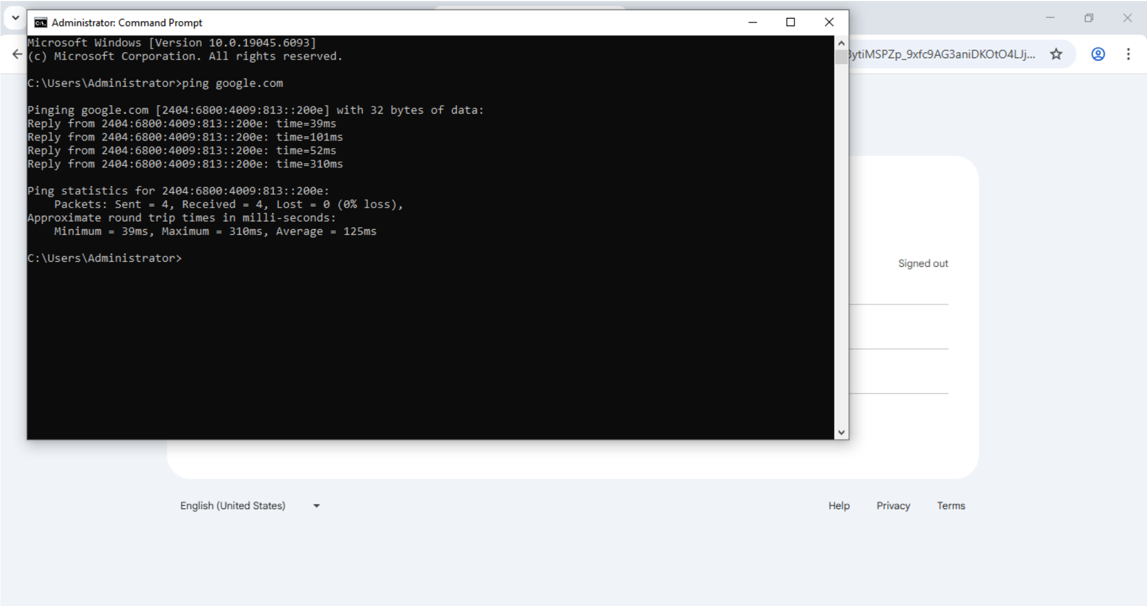
Ethernet 5: <live capture in progress>   Packets: 7   Profile: Default

Step 3 – Generating Network Traffic

Open a browser and visit websites like: www.google.com

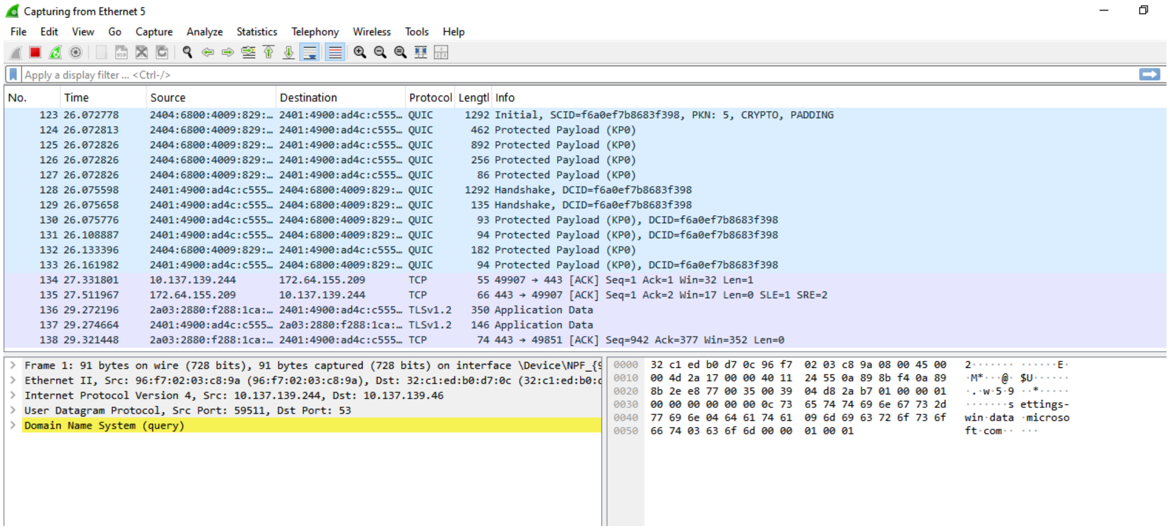
Run a ping command:

ping google.com


Administrator: Command Prompt
ytiMSPZp_9xfc9AG3aniDKOtO4LJj...
Signed out
English (United States)
Help
Privacy
Terms

```
Microsoft Windows [Version 10.0.19045.6093]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping google.com

Pinging google.com [2404:6800:4009:813::200e] with 32 bytes of data:
Reply from 2404:6800:4009:813::200e: time=39ms
Reply from 2404:6800:4009:813::200e: time=101ms
Reply from 2404:6800:4009:813::200e: time=52ms
Reply from 2404:6800:4009:813::200e: time=310ms

Ping statistics for 2404:6800:4009:813::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 310ms, Average = 125ms

C:\Users\Administrator>
```

Network traffic after pinging google.com


Capturing from Ethernet 5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time       Source                 Destination            Protocol Lengtl Info
  123 26.072778  2404:6800:4009:829:…  2401:4900:ad4c:c555…  QUIC     1292 Initial, SCID=f6a0ef7b8683f398, PKN: 5, CRYPTO, PADDING
  124 26.072813  2404:6800:4009:829:…  2401:4900:ad4c:c555…  QUIC      462 Protected Payload (KP0)
  125 26.072826  2404:6800:4009:829:…  2401:4900:ad4c:c555…  QUIC      892 Protected Payload (KP0)
  126 26.072826  2404:6800:4009:829:…  2401:4900:ad4c:c555…  QUIC      256 Protected Payload (KP0)
  127 26.072826  2404:6800:4009:829:…  2401:4900:ad4c:c555…  QUIC       86 Protected Payload (KP0)
  128 26.075598  2401:4900:ad4c:c555…  2404:6800:4009:829:…  QUIC     1292 Handshake, DCID=f6a0ef7b8683f398
  129 26.075658  2401:4900:ad4c:c555…  2404:6800:4009:829:…  QUIC      135 Handshake, DCID=f6a0ef7b8683f398
  130 26.075776  2401:4900:ad4c:c555…  2404:6800:4009:829:…  QUIC       93 Protected Payload (KP0), DCID=f6a0ef7b8683f398
  131 26.108887  2401:4900:ad4c:c555…  2404:6800:4009:829:…  QUIC       94 Protected Payload (KP0), DCID=f6a0ef7b8683f398
  132 26.133396  2404:6800:4009:829:…  2401:4900:ad4c:c555…  QUIC      182 Protected Payload (KP0)
  133 26.161982  2401:4900:ad4c:c555…  2404:6800:4009:829:…  QUIC       94 Protected Payload (KP0), DCID=f6a0ef7b8683f398
  134 27.331801  10.137.139.244         172.64.155.209         TCP        55 49907 → 443 [ACK] Seq=1 Ack=1 Win=32 Len=1
  135 27.511967  172.64.155.209         10.137.139.244         TCP        66 443 → 49907 [ACK] Seq=1 Ack=2 Win=17 Len=0 SLE=1 SRE=2
  136 29.272196  2a03:2880:f288:1ca:…  2401:4900:ad4c:c555…  TLSv1.2   350 Application Data
  137 29.274664  2401:4900:ad4c:c555…  2a03:2880:f288:1ca:…  TLSv1.2   146 Application Data
  138 29.321448  2a03:2880:f288:1ca:…  2401:4900:ad4c:c555…  TCP        74 443 → 49851 [ACK] Seq=942 Ack=377 Win=352 Len=0
```

```
> Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{9
> Ethernet II, Src: 96:f7:02:03:c8:9a (96:f7:02:03:c8:9a), Dst: 32:c1:ed:b0:d7:0c (32:c1:ed:b0:c
> Internet Protocol Version 4, Src: 10.137.139.244, Dst: 10.137.139.46
> User Datagram Protocol, Src Port: 59511, Dst Port: 53
> Domain Name System (query)
```

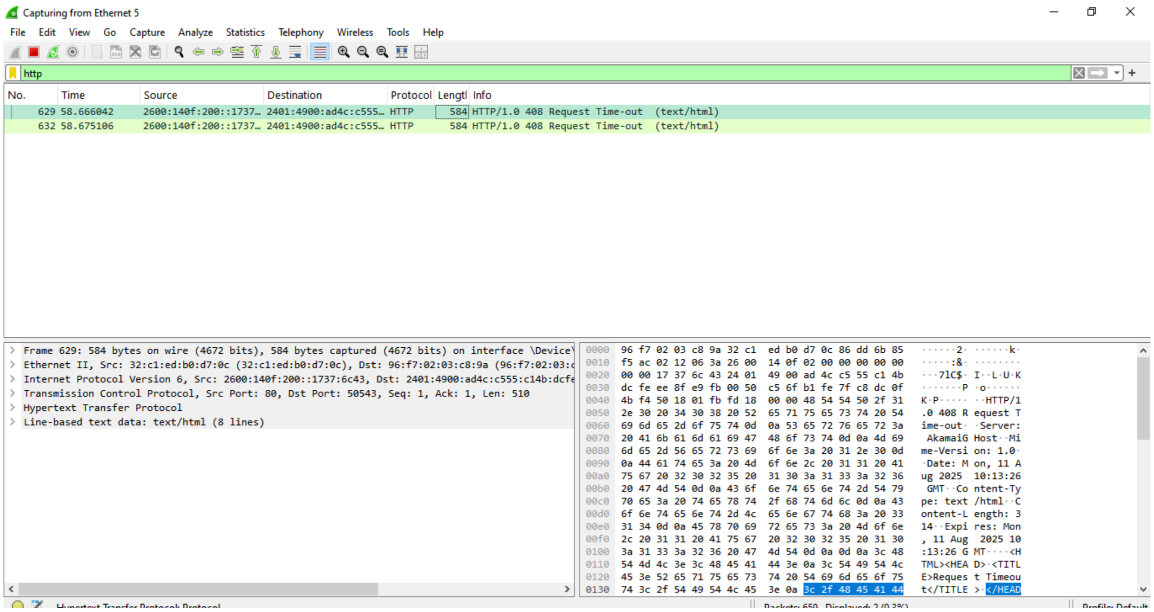
```
0000  32 c1 ed b0 d7 0c 96 f7  02 03 c8 9a 08 00 45 00   2······· ······E·
0010  00 4d 2a 17 00 00 40 11  24 55 0a 89 8b f4 0a 89   ·M*···@· $U······
0020  8b 2e e8 77 00 35 00 39  04 d8 2a b7 01 00 00 01   ·.·w·5·9 ··*·····
0030  00 00 00 00 00 00 0c 73  65 74 74 69 6e 67 73 2d   ·······s ettings-
0040  77 69 6e 04 64 61 74 61  09 6d 69 63 72 6f 73 6f   win·data ·microso
0050  66 74 03 63 6f 6d 00 00  01 00 01                  ft·com·· ···
```

Step 4

After 1-2 minutes, I have stopped the packet capturing.

Step 5 – Applying Protocol Filters

`http` – for web traffic

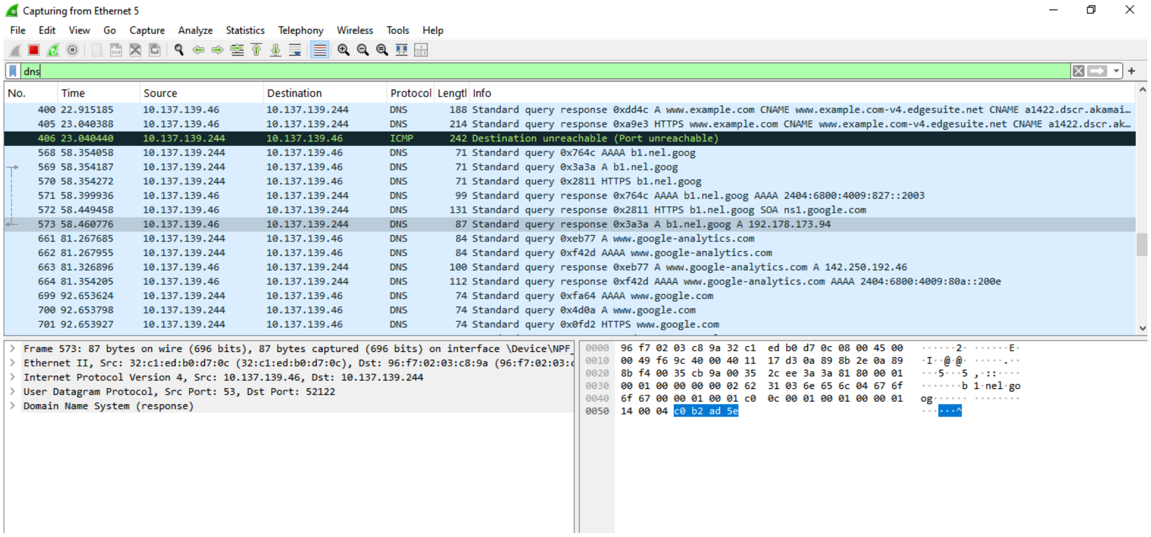

Capturing from Ethernet 5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.  Time       Source               Destination          Protocol Lengtl Info
 629 58.666042  2600:140f:200::1737… 2401:4900:ad4c:c555… HTTP     584 HTTP/1.0 408 Request Time-out  (text/html)
 632 58.675106  2600:140f:200::1737… 2401:4900:ad4c:c555… HTTP     584 HTTP/1.0 408 Request Time-out  (text/html)
```

```
> Frame 629: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface \Device\
> Ethernet II, Src: 32:c1:ed:b0:d7:0c (32:c1:ed:b0:d7:0c), Dst: 96:f7:02:03:c8:9a (96:f7:02:03:c
> Internet Protocol Version 6, Src: 2600:140f:200::1737:6c43, Dst: 2401:4900:ad4c:c555:c14b:dcfe
> Transmission Control Protocol, Src Port: 80, Dst Port: 50543, Seq: 1, Ack: 1, Len: 510
> Hypertext Transfer Protocol
> Line-based text data: text/html (8 lines)
```

```
0000  96 f7 02 03 c8 9a 32 c1  ed b0 d7 0c 86 dd 6b 85   ······2· ······k·
0010  f5 ac 02 12 06 3a 26 00  14 0f 02 00 00 00 00 00   ·····:&· ········
0020  00 00 17 37 6c 43 24 01  49 00 ad 4c c5 55 c1 4b   ···7lC$· I··L·U·K
0030  dc fe ee 8f e9 fb 00 50  c5 6f b1 fe 7f c8 dc 0f   ·······P ·o······
0040  4b f4 50 18 01 fb fd 18  00 00 48 54 54 50 2f 31   K·P····· ··HTTP/1
0050  2e 30 20 34 30 38 20 52  65 71 75 65 73 74 20 54   .0 408 R equest T
0060  69 6d 65 2d 6f 75 74 0d  0a 53 65 72 76 65 72 3a   ime-out· ·Server:
0070  20 41 6b 61 6d 61 69 47  48 6f 73 74 0d 0a 4d 69    AkamaiG Host··Mi
0080  6d 65 2d 56 65 72 73 69  6f 6e 3a 20 31 2e 30 0d   me-Versi on: 1.0·
0090  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 31 31 20 41   ·Date: M on, 11 A
00a0  75 67 20 32 30 32 35 20  31 30 3a 31 33 3a 32 36   ug 2025  10:13:26
00b0  20 47 4d 54 0d 0a 43 6f  6e 74 65 6e 74 2d 54 79    GMT··Co ntent-Ty
00c0  70 65 3a 20 74 65 78 74  2f 68 74 6d 6c 0d 0a 43   pe: text /html··C
00d0  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 33   ontent-L ength: 3
00e0  31 34 0d 0a 45 78 70 69  72 65 73 3a 20 4d 6f 6e   14··Expi res: Mon
00f0  2c 20 31 31 20 41 75 67  20 32 30 32 35 20 31 30   , 11 Aug  2025 10
0100  3a 31 33 3a 32 36 20 47  4d 54 0d 0a 0d 0a 3c 48   :13:26 G MT····<H
0110  54 4d 4c 3e 3c 48 45 41  44 3e 0a 3c 54 49 54 4c   TML><HEA D>·<TITL
0120  45 3e 52 65 71 75 65 73  74 20 54 69 6d 65 6f 75   E>Reques t Timeou
0130  74 3c 2f 54 49 54 4c 45  3e 0a 3c 2f 48 45 41 44   t</TITLE >·</HEAD
```

`dns` – for domain name lookups

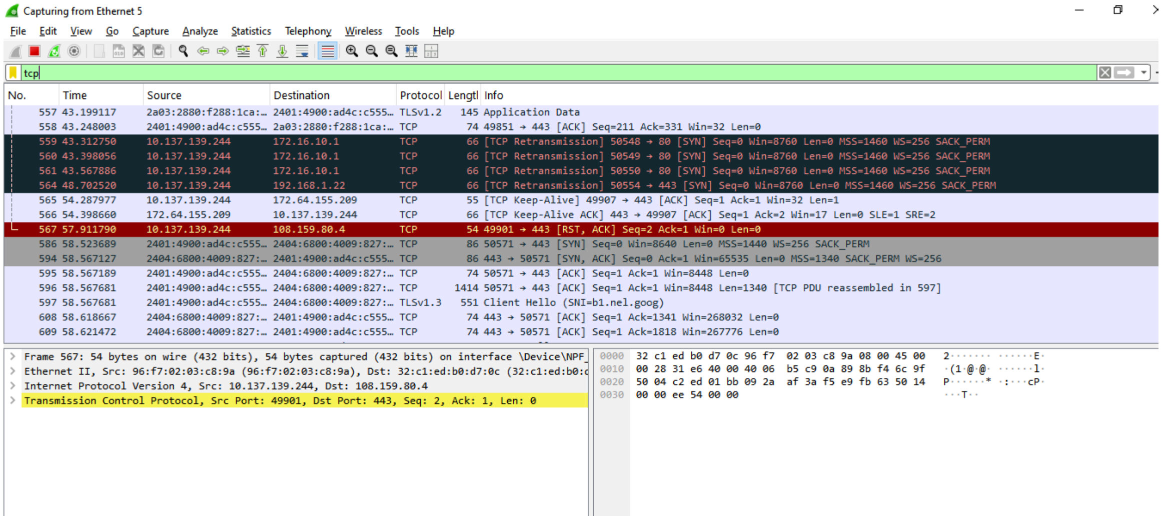

Capturing from Ethernet 5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dns

No.  Time       Source          Destination     Protocol Lengtl Info
 400 22.915185  10.137.139.46   10.137.139.244  DNS      188 Standard query response 0xdd4c A www.example.com CNAME www.example.com-v4.edgesuite.net CNAME a1422.dscr.akamai…
 405 23.040388  10.137.139.46   10.137.139.244  DNS      214 Standard query response 0xa9e3 HTTPS www.example.com CNAME www.example.com-v4.edgesuite.net CNAME a1422.dscr.ak…
 406 23.040440  10.137.139.244  10.137.139.46   ICMP     242 Destination unreachable (Port unreachable)
 568 58.354058  10.137.139.244  10.137.139.46   DNS       71 Standard query 0x764c AAAA b1.nel.goog
 569 58.354187  10.137.139.244  10.137.139.46   DNS       71 Standard query 0x3a3a A b1.nel.goog
 570 58.354272  10.137.139.244  10.137.139.46   DNS       71 Standard query 0x2811 HTTPS b1.nel.goog
 571 58.399936  10.137.139.46   10.137.139.244  DNS       99 Standard query response 0x764c AAAA b1.nel.goog AAAA 2404:6800:4009:827::2003
 572 58.449458  10.137.139.46   10.137.139.244  DNS      131 Standard query response 0x2811 HTTPS b1.nel.goog SOA ns1.google.com
 573 58.460776  10.137.139.46   10.137.139.244  DNS       87 Standard query response 0x3a3a A b1.nel.goog A 192.178.173.94
 661 81.267685  10.137.139.244  10.137.139.46   DNS       84 Standard query 0xeb77 A www.google-analytics.com
 662 81.267955  10.137.139.244  10.137.139.46   DNS       84 Standard query 0xf42d AAAA www.google-analytics.com
 663 81.326896  10.137.139.46   10.137.139.244  DNS      100 Standard query response 0xeb77 A www.google-analytics.com A 142.250.192.46
 664 81.354205  10.137.139.46   10.137.139.244  DNS      112 Standard query response 0xf42d AAAA www.google-analytics.com AAAA 2404:6800:4009:80a::200e
 699 92.653624  10.137.139.244  10.137.139.46   DNS       74 Standard query 0xfa64 AAAA www.google.com
 700 92.653798  10.137.139.244  10.137.139.46   DNS       74 Standard query 0x4d0a A www.google.com
 701 92.653927  10.137.139.244  10.137.139.46   DNS       74 Standard query 0x0fd2 HTTPS www.google.com
```

```
> Frame 573: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF_
> Ethernet II, Src: 32:c1:ed:b0:d7:0c (32:c1:ed:b0:d7:0c), Dst: 96:f7:02:03:c8:9a (96:f7:02:03:c
> Internet Protocol Version 4, Src: 10.137.139.46, Dst: 10.137.139.244
> User Datagram Protocol, Src Port: 53, Dst Port: 52122
> Domain Name System (response)
```

```
0000  96 f7 02 03 c8 9a 32 c1  ed b0 d7 0c 08 00 45 00   ······2· ······E·
0010  00 49 f6 9c 40 00 40 11  17 d3 0a 89 8b 2e 0a 89   ·I··@·@· ·····.··
0020  8b f4 00 35 cb 9a 00 35  2c ee 3a 3a 81 80 00 01   ···5···5 ,·::····
0030  00 01 00 00 00 00 02 62  31 03 6e 65 6c 04 67 6f   ·······b 1·nel·go
0040  6f 67 00 00 01 00 01 c0  0c 00 01 00 01 00 00 01   og······ ········
0050  14 00 04 c0 b2 ad 5e                               ···^
```

`tcp` – for Transmission Control Protocol packets


Capturing from Ethernet 5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

```
No.   Time       Source                   Destination              Protocol Lengtl Info
  557 43.199117  2a03:2880:f288:1ca:…     2401:4900:ad4c:c555…     TLSv1.2   145 Application Data
  558 43.248003  2401:4900:ad4c:c555…     2a03:2880:f288:1ca:…     TCP        74 49851 → 443 [ACK] Seq=211 Ack=331 Win=32 Len=0
  559 43.312750  10.137.139.244           172.16.10.1              TCP        66 [TCP Retransmission] 50548 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 WS=256 SACK_PERM
  560 43.398056  10.137.139.244           172.16.10.1              TCP        66 [TCP Retransmission] 50549 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 WS=256 SACK_PERM
  561 43.567886  10.137.139.244           172.16.10.1              TCP        66 [TCP Retransmission] 50550 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 WS=256 SACK_PERM
  564 48.702520  10.137.139.244           192.168.1.22             TCP        66 [TCP Retransmission] 50554 → 443 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 WS=256 SACK_PERM
  565 54.287977  10.137.139.244           172.64.155.209           TCP        55 [TCP Keep-Alive] 49907 → 443 [ACK] Seq=1 Ack=1 Win=32 Len=1
  566 54.398660  172.64.155.209           10.137.139.244           TCP        66 [TCP Keep-Alive ACK] 443 → 49907 [ACK] Seq=1 Ack=2 Win=17 Len=0 SLE=1 SRE=2
  567 57.911790  10.137.139.244           108.159.80.4             TCP        54 49901 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
  586 58.523689  2401:4900:ad4c:c555…     2404:6800:4009:827:…     TCP        86 50571 → 443 [SYN] Seq=0 Win=8640 Len=0 MSS=1440 WS=256 SACK_PERM
  594 58.567127  2404:6800:4009:827:…     2401:4900:ad4c:c555…     TCP        86 443 → 50571 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1340 SACK_PERM WS=256
  595 58.567189  2401:4900:ad4c:c555…     2404:6800:4009:827:…     TCP        74 50571 → 443 [ACK] Seq=1 Ack=1 Win=8448 Len=0
  596 58.567681  2401:4900:ad4c:c555…     2404:6800:4009:827:…     TCP      1414 50571 → 443 [ACK] Seq=1 Ack=1 Win=8448 Len=1340 [TCP PDU reassembled in 597]
  597 58.567681  2401:4900:ad4c:c555…     2404:6800:4009:827:…     TLSv1.3   551 Client Hello (SNI=b1.nel.goog)
  608 58.618667  2404:6800:4009:827:…     2401:4900:ad4c:c555…     TCP        74 443 → 50571 [ACK] Seq=1 Ack=1341 Win=268032 Len=0
  609 58.621472  2404:6800:4009:827:…     2401:4900:ad4c:c555…     TCP        74 443 → 50571 [ACK] Seq=1 Ack=1818 Win=267776 Len=0
```

```
> Frame 567: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_
> Ethernet II, Src: 96:f7:02:03:c8:9a (96:f7:02:03:c8:9a), Dst: 32:c1:ed:b0:d7:0c (32:c1:ed:b0:c
> Internet Protocol Version 4, Src: 10.137.139.244, Dst: 108.159.80.4
> Transmission Control Protocol, Src Port: 49901, Dst Port: 443, Seq: 2, Ack: 1, Len: 0
```

```
0000  32 c1 ed b0 d7 0c 96 f7  02 03 c8 9a 08 00 45 00   2······ ······E·
0010  00 28 31 e6 40 00 40 06  b5 c9 0a 89 8b f4 6c 9f   ·(1·@·@· ······l·
0020  50 04 c2 ed 01 bb 09 2a  af 3a f5 e9 fb 63 50 14   P······* ·:···cP·
0030  00 00 ee 54 00 00                                  ···T··
```

1. DNS (Domain Name System)

Layer: Application layer (OSI Layer 7)

Purpose: Translates human-readable domain names (e.g., google.com) into IP addresses (e.g., 142.250.193.78).

Wireshark Filter: dns

Example Packet:

Frame Info: 74 bytes on wire

Source IP: 192.168.1.5 (client)

Destination IP: 8.8.8.8 (Google DNS server)

Query Name: www.google.com

Observation:

When I typed a website into the browser, a DNS Query packet was sent to the DNS server, followed by a DNS Response containing the IP address.

2. HTTP (Hypertext Transfer Protocol)

Layer: Application layer (OSI Layer 7)

Purpose: Transmits hypertext data between client (browser) and server.

Wireshark Filter: http

Example Packet:

Method: GET

Host: www.example.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

Status Code: 200 OK

Observation:

HTTP packets showed the exact URL paths requested, headers sent, and HTML content returned by the server. Since HTTP is not encrypted, the request and response data were fully visible in the capture.

3. TCP (Transmission Control Protocol)

Layer: Transport layer (OSI Layer 4)

Purpose: Provides reliable, ordered, and error-checked delivery of data between applications.

Wireshark Filter: tcp

Example Packet:

Flags: SYN, SYN-ACK, ACK (TCP 3-way handshake)

Source Port: 56782

Destination Port: 443 (HTTPS)

Sequence Number: 0 → 1 → 2 (example)

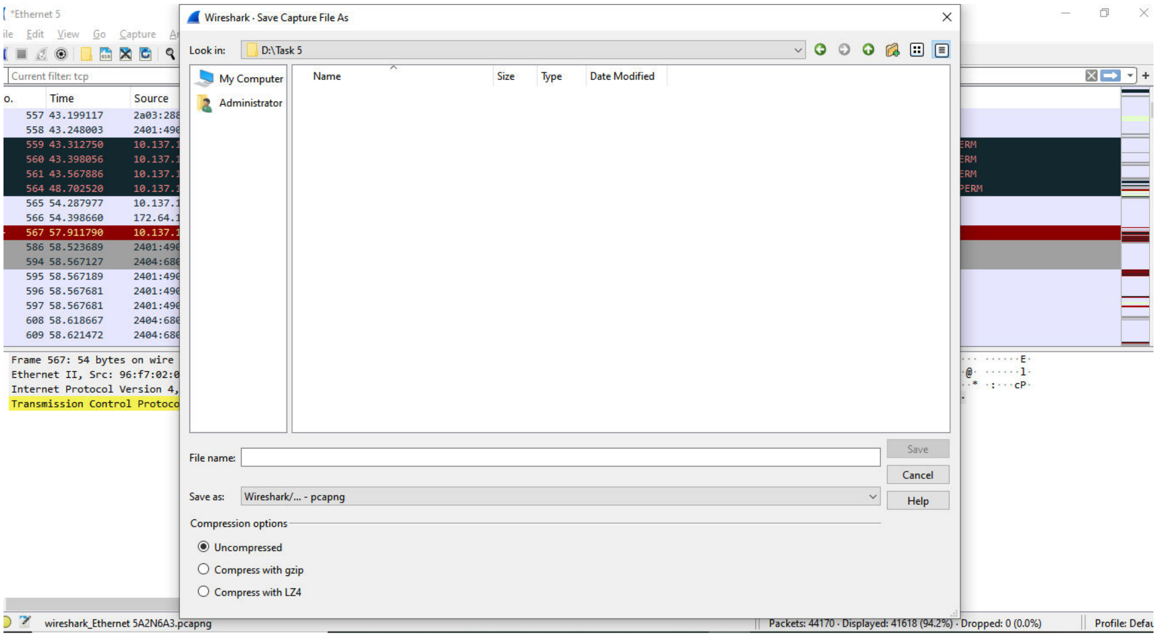
Observation:

Capturing TCP traffic allowed me to see the connection establishment process and data transmission segments. For HTTPS traffic (port 443), the payload was encrypted, but the TCP handshake details were still visible.

Step 7 – Export Capture as .pcap

Go to File → Save As → .pcap format.

Named it network_capture.pcap.



Current filter: tcp

```
o.    Time       Source
  557 43.199117  2a03:288
  558 43.248003  2401:490
  559 43.312750  10.137.1
  560 43.398056  10.137.1
  561 43.567886  10.137.1
  564 48.702520  10.137.1
  565 54.287977  10.137.1
  566 54.398660  172.64.1
  567 57.911790  10.137.1
  586 58.523689  2401:490
  594 58.567127  2404:680
  595 58.567189  2401:490
  596 58.567681  2401:490
  597 58.567681  2401:490
  608 58.618667  2404:680
  609 58.621472  2404:680

Frame 567: 54 bytes on wire
Ethernet II, Src: 96:f7:02:0
Internet Protocol Version 4,
Transmission Control Protoco
```

Look in: D:\Task 5

File name:

Save as: Wireshark/... - pcapng

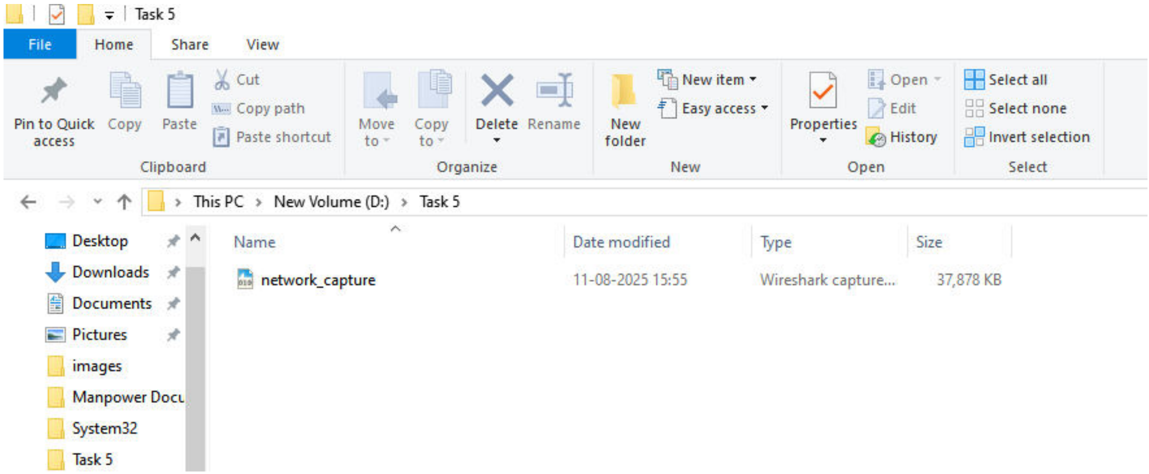
Compression options

● Uncompressed

○ Compress with gzip

○ Compress with LZ4

wireshark_Ethernet 5A2N6A3.pcapng | Packets: 44170 · Displayed: 41618 (94.2%) · Dropped: 0 (0.0%) | Profile: Defau



This PC › New Volume (D:) › Task 5

Name	Date modified	Type	Size
network_capture	11-08-2025 15:55	Wireshark capture...	37,878 KB