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

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

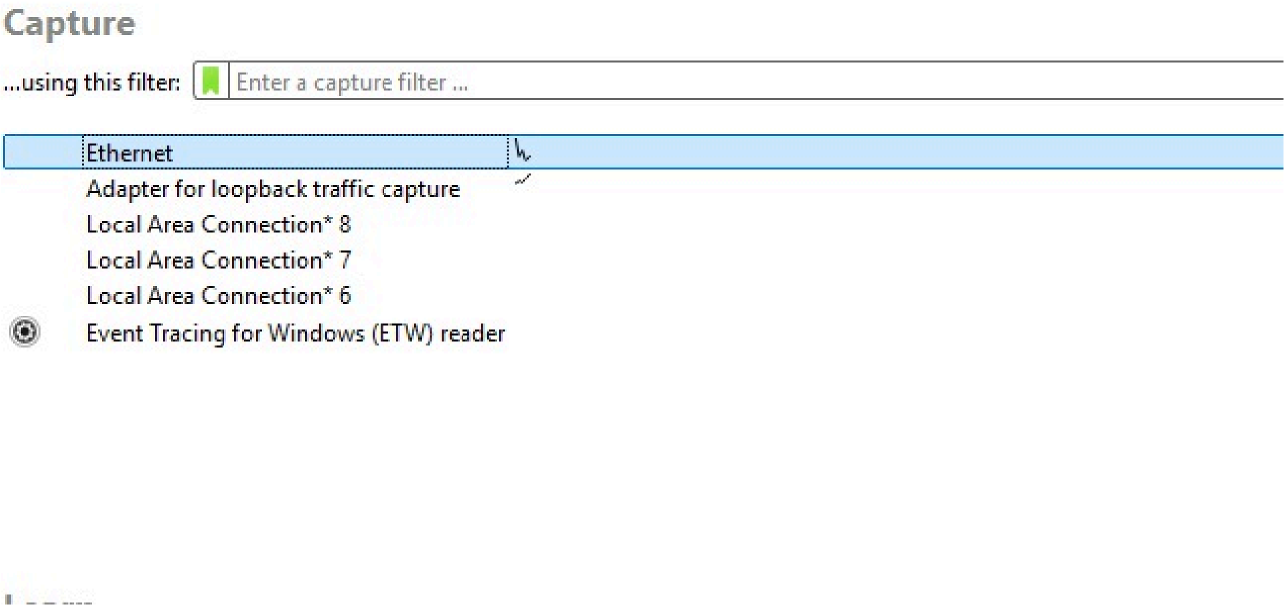
NAME : MK RITHUBARAN

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).



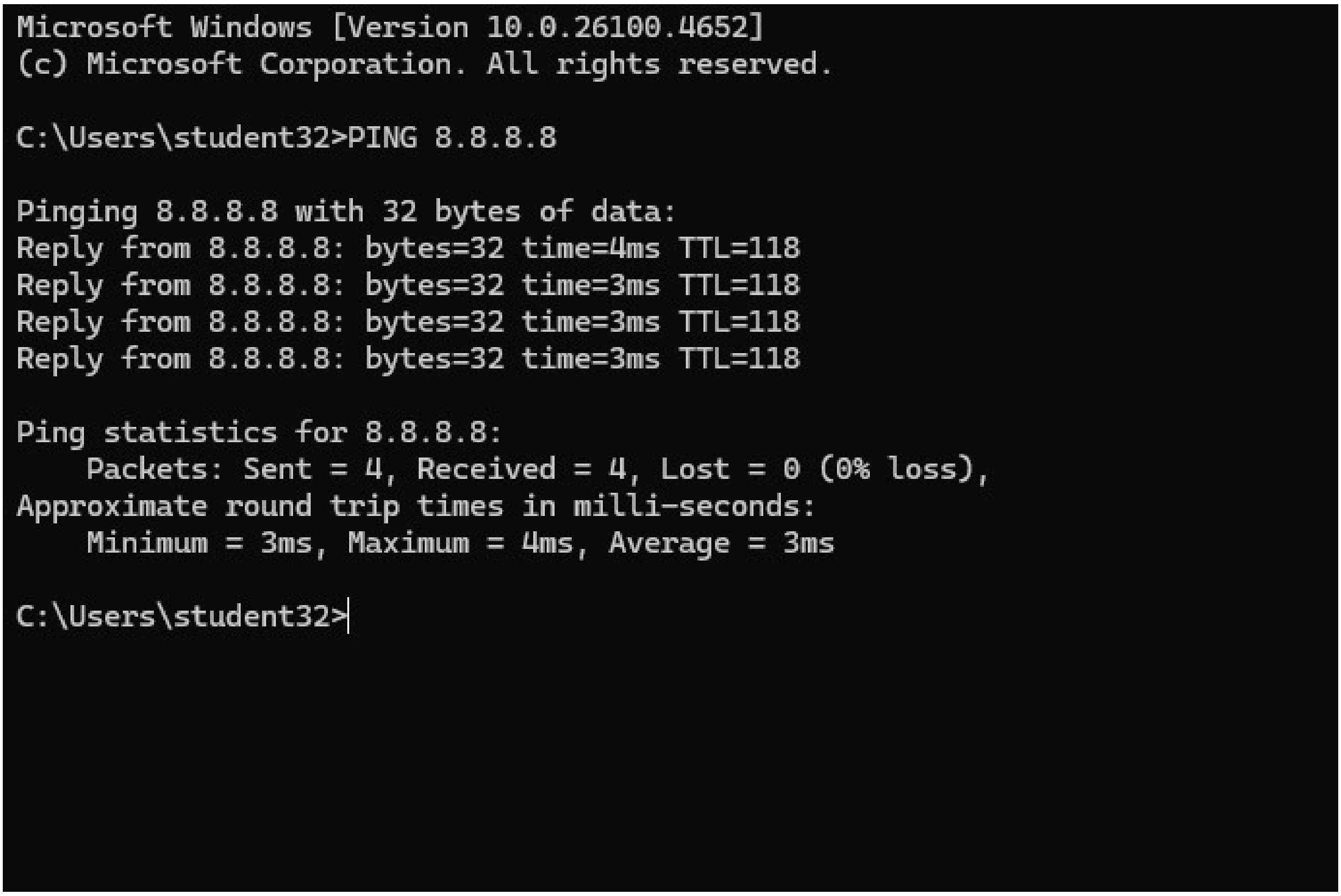
Capture

...using this filter: Enter a capture filter ...

Ethernet
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Event Tracing for Windows (ETW) reader

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.



```
Microsoft Windows [Version 10.0.26100.4652]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student32>PING 8.8.8.8

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

C:\Users\student32>
```

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).

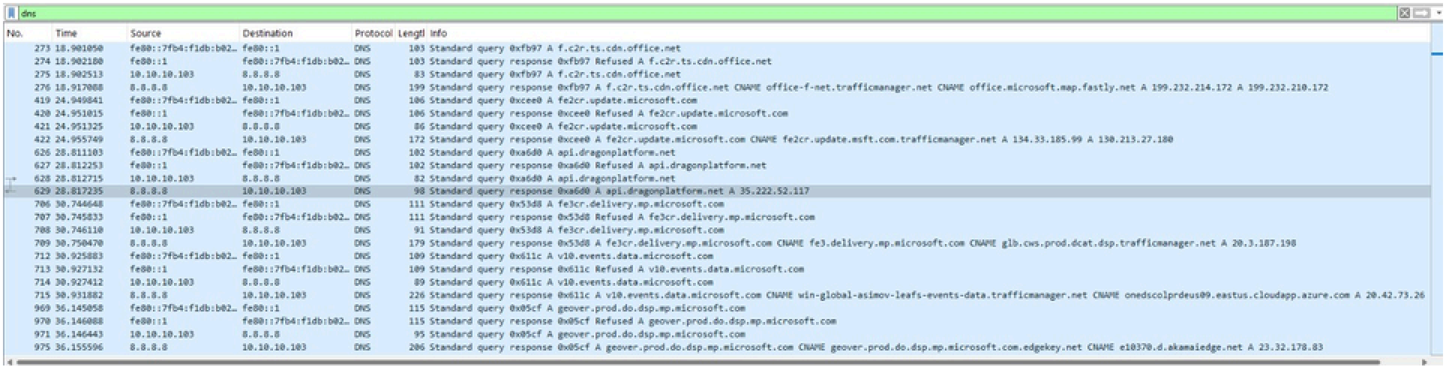
- Expand layers (Ethernet → IP → TCP/UDP → application protocol) to view fields.

5) Find these protocols

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

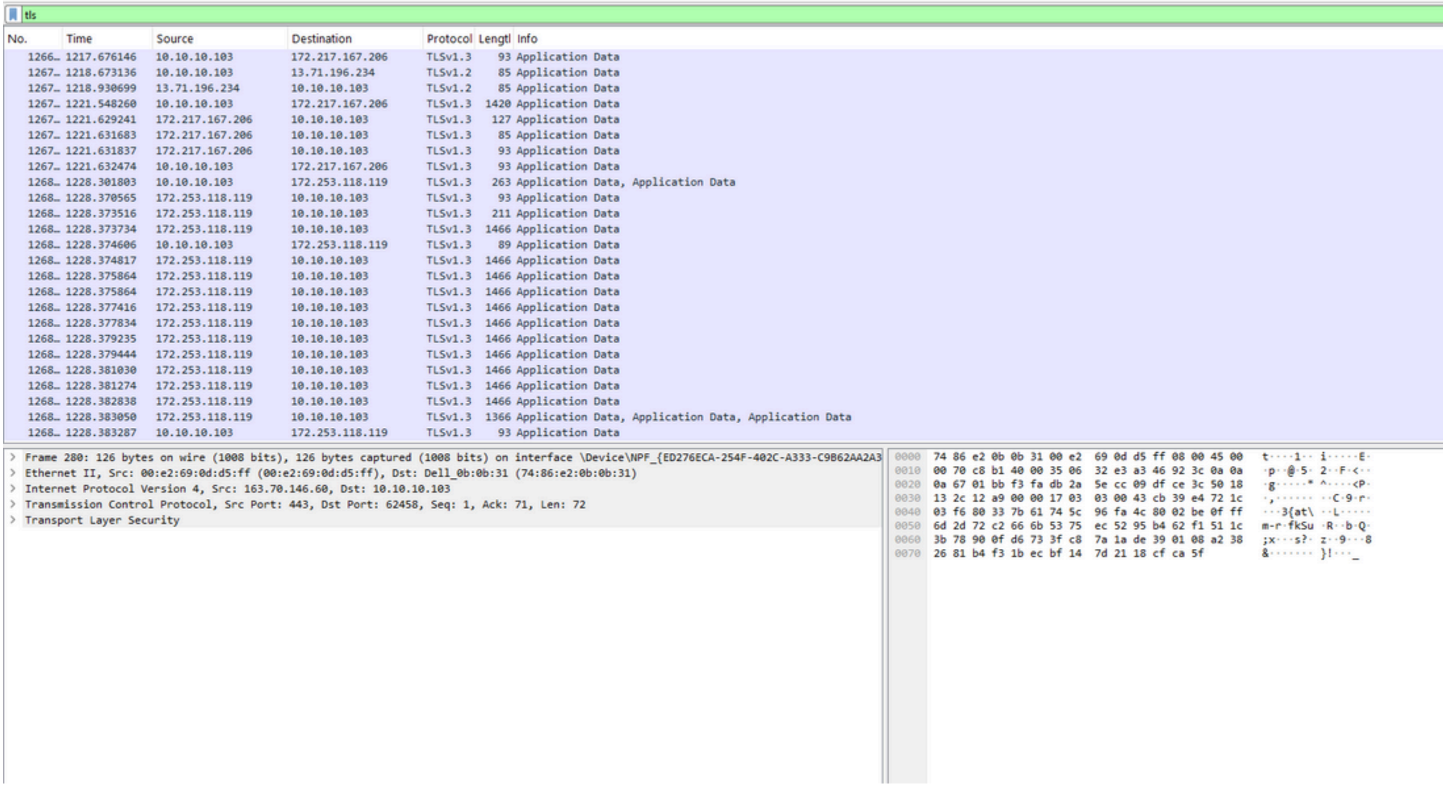
- **DNS Traffic (Domain Resolution)**

Goal: Capture DNS queries to domains



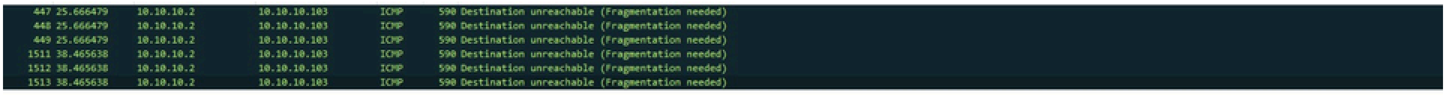
```
dns
No.   Time       Source                 Destination            Protocol Lengtl Info
  273 18.901050  fe80::7fb4:f1db:b02…   fe80::1                DNS      103 Standard query 0xfb97 A f.c2r.ts.cdn.office.net
  274 18.902180  fe80::1                fe80::7fb4:f1db:b02…   DNS      103 Standard query response 0xfb97 Refused A f.c2r.ts.cdn.office.net
  275 18.902513  10.10.10.103           8.8.8.8                DNS       83 Standard query 0xfb97 A f.c2r.ts.cdn.office.net
  276 18.917088  8.8.8.8                10.10.10.103           DNS      199 Standard query response 0xfb97 A f.c2r.ts.cdn.office.net CNAME office-f-net.trafficmanager.net CNAME office.microsoft.map.fastly.net A 199.232.214.172 A 199.232.210.172
  419 24.949841  fe80::7fb4:f1db:b02…   fe80::1                DNS      106 Standard query 0xcee0 A fe2cr.update.microsoft.com
  420 24.951015  fe80::1                fe80::7fb4:f1db:b02…   DNS      106 Standard query response 0xcee0 Refused A fe2cr.update.microsoft.com
  421 24.951325  10.10.10.103           8.8.8.8                DNS       86 Standard query 0xcee0 A fe2cr.update.microsoft.com
  422 24.955749  8.8.8.8                10.10.10.103           DNS      172 Standard query response 0xcee0 A fe2cr.update.microsoft.com CNAME fe2cr.update.msft.com.trafficmanager.net A 134.33.185.99 A 130.213.27.180
  626 28.811103  fe80::7fb4:f1db:b02…   fe80::1                DNS      102 Standard query 0xa6d0 A api.dragonplatform.net
  627 28.812253  fe80::1                fe80::7fb4:f1db:b02…   DNS      102 Standard query response 0xa6d0 Refused A api.dragonplatform.net
  628 28.812715  10.10.10.103           8.8.8.8                DNS       82 Standard query 0xa6d0 A api.dragonplatform.net
  629 28.817235  8.8.8.8                10.10.10.103           DNS       98 Standard query response 0xa6d0 A api.dragonplatform.net A 35.222.52.117
  706 30.744648  fe80::7fb4:f1db:b02…   fe80::1                DNS      111 Standard query 0x53d8 A fe3cr.delivery.mp.microsoft.com
  707 30.745833  fe80::1                fe80::7fb4:f1db:b02…   DNS      111 Standard query response 0x53d8 Refused A fe3cr.delivery.mp.microsoft.com
  708 30.746110  10.10.10.103           8.8.8.8                DNS       91 Standard query 0x53d8 A fe3cr.delivery.mp.microsoft.com
  709 30.750470  8.8.8.8                10.10.10.103           DNS      179 Standard query response 0x53d8 A fe3cr.delivery.mp.microsoft.com CNAME fe3.delivery.mp.microsoft.com CNAME glb.cws.prod.dcat.dsp.trafficmanager.net A 20.3.187.198
  712 30.925883  fe80::7fb4:f1db:b02…   fe80::1                DNS      109 Standard query 0x611c A v10.events.data.microsoft.com
  713 30.927132  fe80::1                fe80::7fb4:f1db:b02…   DNS      109 Standard query response 0x611c Refused A v10.events.data.microsoft.com
  714 30.927412  10.10.10.103           8.8.8.8                DNS       89 Standard query 0x611c A v10.events.data.microsoft.com
  715 30.931882  8.8.8.8                10.10.10.103           DNS      226 Standard query response 0x611c A v10.events.data.microsoft.com CNAME win-global-asimov-leafs-events-data.trafficmanager.net CNAME onedscolprdeus09.eastus.cloudapp.azure.com A 20.42.73.26
  969 36.145058  fe80::7fb4:f1db:b02…   fe80::1                DNS      115 Standard query 0x05cf A geover.prod.do.dsp.mp.microsoft.com
  970 36.146088  fe80::1                fe80::7fb4:f1db:b02…   DNS      115 Standard query response 0x05cf Refused A geover.prod.do.dsp.mp.microsoft.com
  971 36.146443  10.10.10.103           8.8.8.8                DNS       95 Standard query 0x05cf A geover.prod.do.dsp.mp.microsoft.com
  975 36.155596  8.8.8.8                10.10.10.103           DNS      206 Standard query response 0x05cf A geover.prod.do.dsp.mp.microsoft.com CNAME geover.prod.do.dsp.mp.microsoft.com.edgekey.net CNAME e10370.d.akamaiedge.net A 23.32.178.83
```

Goal: TLS (HTTPS) handshakes & records

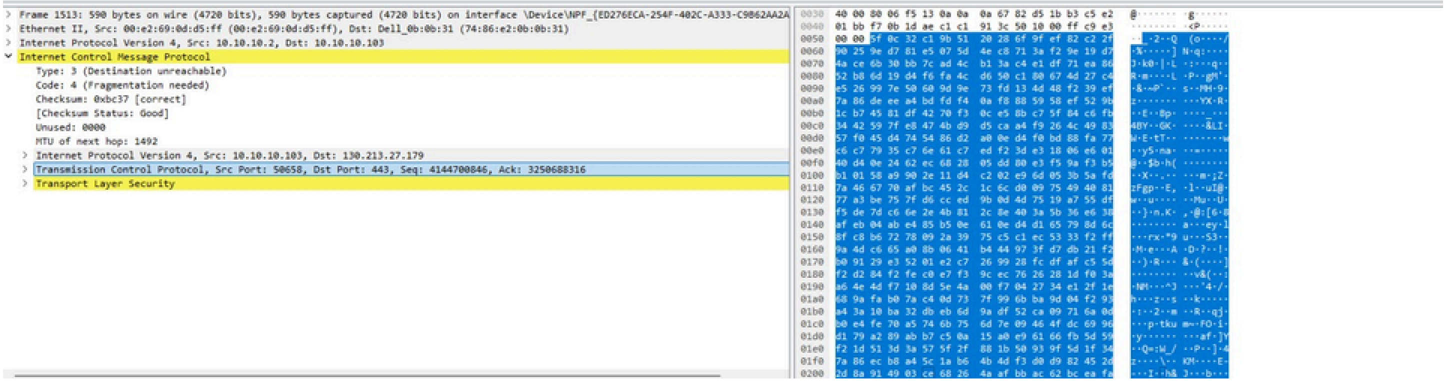


```
tls
No.    Time         Source            Destination       Protocol Lengtl Info
1266…  1217.676146  10.10.10.103      172.217.167.206   TLSv1.3    93 Application Data
1267…  1218.673136  10.10.10.103      13.71.196.234     TLSv1.2    85 Application Data
1267…  1218.930699  13.71.196.234     10.10.10.103      TLSv1.2    85 Application Data
1267…  1221.548260  10.10.10.103      172.217.167.206   TLSv1.3  1420 Application Data
1267…  1221.629241  172.217.167.206   10.10.10.103      TLSv1.3   127 Application Data
1267…  1221.631683  172.217.167.206   10.10.10.103      TLSv1.3    85 Application Data
1267…  1221.631837  172.217.167.206   10.10.10.103      TLSv1.3    93 Application Data
1267…  1221.632474  10.10.10.103      172.217.167.206   TLSv1.3    93 Application Data
1268…  1228.301803  10.10.10.103      172.253.118.119   TLSv1.3   263 Application Data, Application Data
1268…  1228.370565  172.253.118.119   10.10.10.103      TLSv1.3    93 Application Data
1268…  1228.373516  172.253.118.119   10.10.10.103      TLSv1.3   211 Application Data
1268…  1228.373734  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.374606  10.10.10.103      172.253.118.119   TLSv1.3    89 Application Data
1268…  1228.374817  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.375864  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.375864  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.377416  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.377834  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.379235  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.379444  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.381030  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.381274  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.382838  172.253.118.119   10.10.10.103      TLSv1.3  1466 Application Data
1268…  1228.383050  172.253.118.119   10.10.10.103      TLSv1.3  1366 Application Data, Application Data, Application Data
1268…  1228.383287  10.10.10.103      172.253.118.119   TLSv1.3    93 Application Data

> Frame 280: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{ED276ECA-254F-402C-A333-C9B62AA2A3
> Ethernet II, Src: 00:e2:69:0d:d5:ff (00:e2:69:0d:d5:ff), Dst: Dell_0b:0b:31 (74:86:e2:0b:0b:31)
> Internet Protocol Version 4, Src: 163.70.146.60, Dst: 10.10.10.103
> Transmission Control Protocol, Src Port: 443, Dst Port: 62458, Seq: 1, Ack: 71, Len: 72
> Transport Layer Security

0000  74 86 e2 0b 0b 31 00 e2  69 0d d5 ff 08 00 45 00   t····1·· i·····E·
0010  00 70 c8 b1 40 00 35 06  32 e3 a3 46 92 3c 0a 0a   ·p··@·5· 2··F·<··
0020  0a 67 01 bb f3 fa db 2a  5e cc 09 df ce 3c 50 18   ·g·····* ^····<P·
0030  13 2c 12 a9 00 00 17 03  03 00 43 cb 39 e4 72 1c   ·,······ ··C·9·r·
0040  03 f6 80 33 7b 61 74 5c  96 fa 4c 80 02 be 0f ff   ···3{at\ ··L·····
0050  6d 2d 72 c2 66 6b 53 75  ec 52 95 b4 62 f1 51 1c   m-r·fkSu ·R··b·Q·
0060  3b 78 90 0f d6 73 3f c8  7a 1a de 39 01 08 a2 38   ;x···s?· z··9···8
0070  26 81 b4 f3 1b ec bf 14  7d 21 18 cf ca 5f         &······· }!···_
```

icmp



```
  447 25.666479   10.10.10.2     10.10.10.103    ICMP    590 Destination unreachable (Fragmentation needed)
  448 25.666479   10.10.10.2     10.10.10.103    ICMP    590 Destination unreachable (Fragmentation needed)
  449 25.666479   10.10.10.2     10.10.10.103    ICMP    590 Destination unreachable (Fragmentation needed)
 1511 38.465638   10.10.10.2     10.10.10.103    ICMP    590 Destination unreachable (Fragmentation needed)
 1512 38.465638   10.10.10.2     10.10.10.103    ICMP    590 Destination unreachable (Fragmentation needed)
 1513 38.465638   10.10.10.2     10.10.10.103    ICMP    590 Destination unreachable (Fragmentation needed)
```



```
> Frame 1513: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \Device\NPF_{ED276ECA-254F-402C-A333-C9862AA2A
> Ethernet II, Src: 00:e2:69:0d:d5:ff (00:e2:69:0d:d5:ff), Dst: Dell_0b:0b:31 (74:86:e2:0b:0b:31)
> Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.10.10.103
v Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 4 (Fragmentation needed)
    Checksum: 0xbc37 [correct]
    [Checksum Status: Good]
    Unused: 0000
    MTU of next hop: 1492
  > Internet Protocol Version 4, Src: 10.10.10.103, Dst: 130.213.27.179
  > Transmission Control Protocol, Src Port: 50658, Dst Port: 443, Seq: 4144700846, Ack: 3250688316
  > Transport Layer Security
```

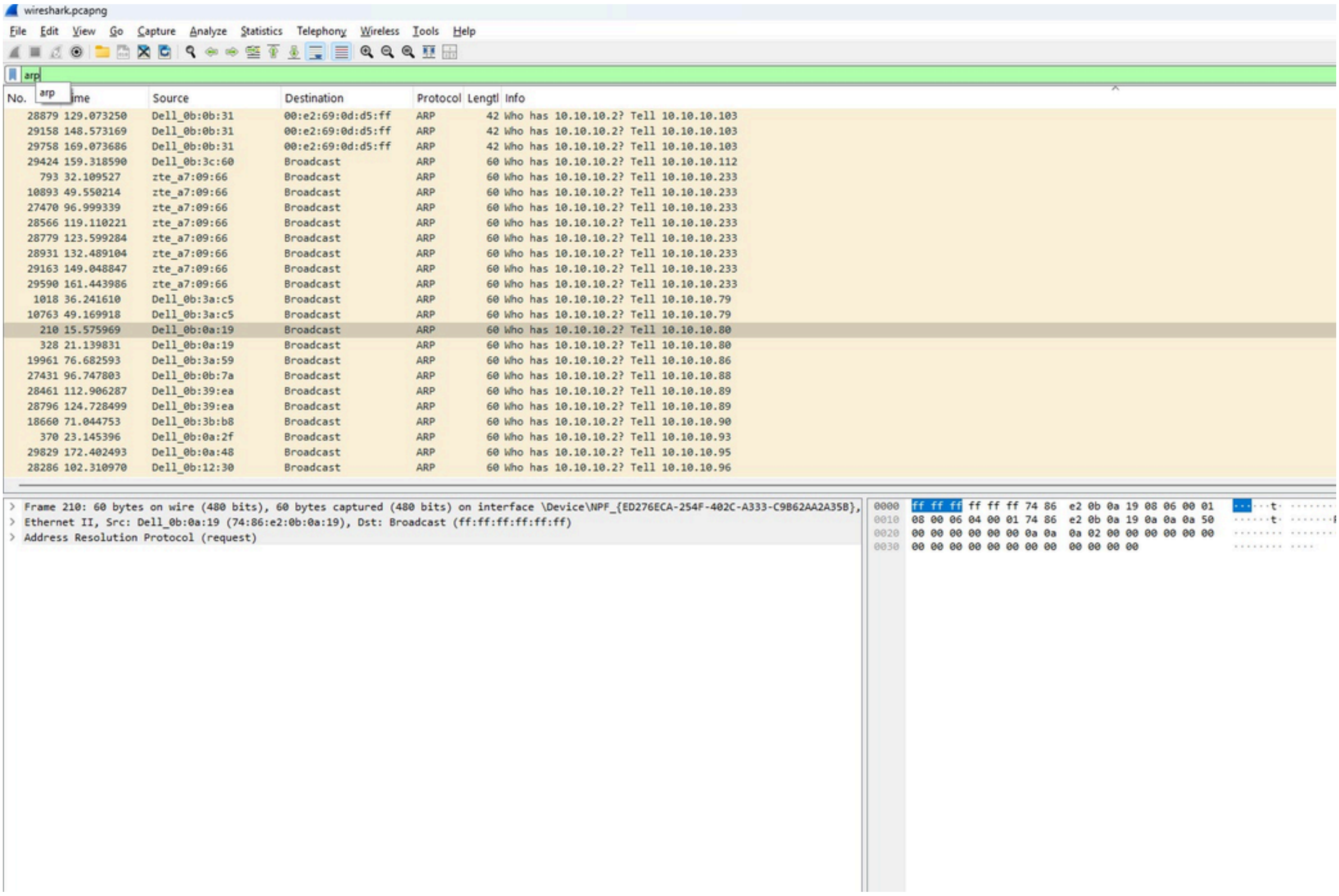
```
0030  40 00 80 06 f5 13 0a 0a  0a 67 82 d5 1b b3 c5 e2   @·······  ·g······
0040  01 bb f7 0b 1d ae c1 c1  91 3c 50 10 00 ff c9 e3   ········  ·<P·····
0050  00 00 5f 0c 32 c1 9b 51  20 28 6f 9f ef 82 c2 2f   ··_·2··Q  (o····/
0060  90 25 9e d7 81 e5 07 5d  4e c8 71 3a f2 9e 19 d7   ·%·····]  N·q:····
0070  4a ce 6b 30 bb 7c ad 4c  b1 3a c4 e1 df 71 ea 86   J·k0·|·L  ·:···q··
0080  52 b8 6d 19 d4 f6 fa 4c  d6 50 c1 80 67 4d 27 c4   R·m····L  ·P··gM'·
0090  e5 26 99 7e 50 60 9d 9e  73 fd 13 4d 48 f2 39 ef   ·&·~P`··  s··MH·9·
00a0  7a 86 de ee a4 bd fd f4  0a f8 88 59 58 ef 52 9b   z·······  ···YX·R·
00b0  1c b7 45 81 df 42 70 f3  0c e5 8b c7 5f 84 c6 fb   ··E··Bp·  ····_···
00c0  34 42 59 7f e8 47 4b d9  d5 ca a4 f9 26 4c 49 83   4BY··GK·  ····&LI·
00d0  57 f0 45 d4 74 54 86 d2  a0 0e d4 f0 bd 88 fa 77   W·E·tT··  ·······w
00e0  c6 c7 79 35 c7 6e 61 c7  ed f2 3d e3 18 06 e6 01   ··y5·na·  ··=·····
00f0  40 d4 0e 24 62 ec 68 28  05 dd 80 e3 f5 9a f3 b5   @··$b·h(  ········
0100  b1 01 58 a9 90 2e 11 d4  c2 02 e9 6d 05 3b 5a fd   ··X··.··  ···m·;Z·
0110  7a 46 67 70 af bc 45 2c  1c 6c d0 09 75 49 40 81   zFgp··E,  ·l··uI@·
0120  77 a3 be 75 7f d6 cc ed  9b 0d 4d 75 19 a7 55 df   w··u····  ··Mu··U·
0130  f5 de 7d c6 6e 2e 4b 81  2c 8e 40 3a 5b 36 e6 38   ··}·n.K·  ,·@:[6·8
0140  af eb 04 ab e4 85 b5 0e  61 0e d4 d1 65 79 8d 6c   ········  a···ey·l
0150  8f c8 b6 72 78 09 2a 39  75 c5 c1 ec 53 33 f2 ff   ···rx·*9  u···S3··
0160  9a 4d c6 65 a0 8b 06 41  b4 44 97 3f d7 db 21 f2   ·M·e···A  ·D·?··!·
0170  b0 91 29 e3 52 01 e2 c7  26 99 28 fc df af c5 5d   ··)·R···  &·(····]
0180  f2 d2 84 f2 fe c0 e7 f3  9c ec 76 26 28 1d f0 3a   ········  ··v&(··:
0190  a6 4e 4d f7 10 8d 5e 4a  00 f7 04 27 34 e1 2f 1e   ·NM···^J  ···'4·/·
01a0  68 9a fa b0 7a c4 0d 73  7f 99 6b ba 9d 04 f2 93   h···z··s  ··k·····
01b0  a4 3a 10 ba 32 db eb 6d  9a df 52 ca 09 71 6a 0d   ·:··2··m  ··R··qj·
01c0  b0 e4 fe 70 a5 74 6b 75  6d 7e 09 46 4f dc 69 96   ···p·tku  m~·FO·i·
01d0  d1 79 a2 89 ab b7 c5 0a  15 a0 e9 61 66 fb 5d 59   ·y······  ···af·]Y
01e0  f2 1d 51 3d 3a 57 5f 2f  88 1b 50 93 9f 5d 1f 34   ··Q=:W_/  ··P··]·4
01f0  7a 86 ec b8 a4 5c 1a b6  4b 4d f3 d0 d9 82 45 2d   z····\··  KM····E-
0200  2d 8a 91 49 03 ce 68 26  4a af bb ac 62 bc ea fa   -··I··h&  J···b···
```

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


wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

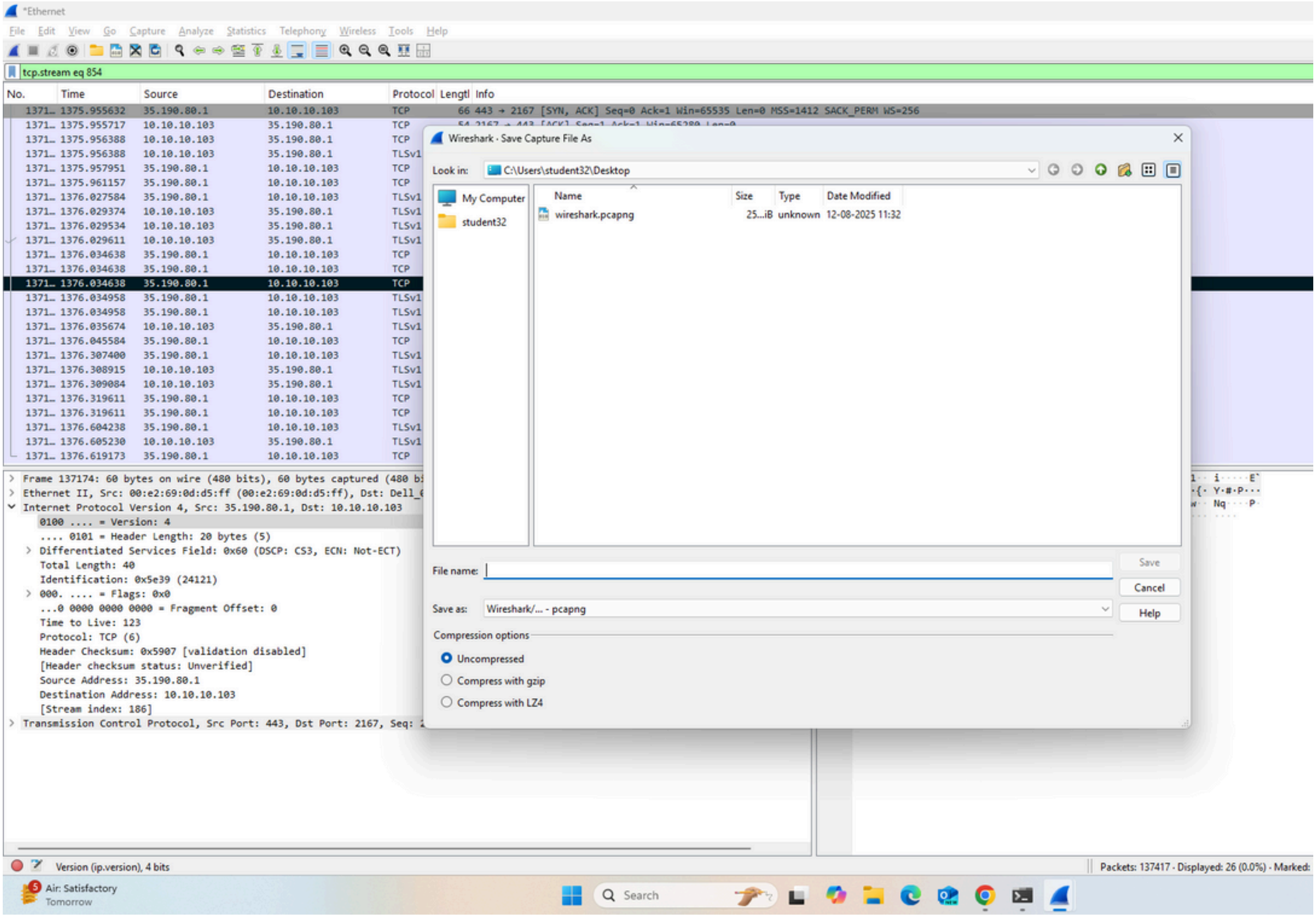
```
arp

No.   ime          Source           Destination        Protocol Lengtl Info
28879 129.073250   Dell_0b:0b:31    00:e2:69:0d:d5:ff  ARP      42 Who has 10.10.10.2? Tell 10.10.10.103
29158 148.573169   Dell_0b:0b:31    00:e2:69:0d:d5:ff  ARP      42 Who has 10.10.10.2? Tell 10.10.10.103
29758 169.073686   Dell_0b:0b:31    00:e2:69:0d:d5:ff  ARP      42 Who has 10.10.10.2? Tell 10.10.10.103
29424 159.318590   Dell_0b:3c:60    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.112
  793 32.109527    zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
10893 49.550214    zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
27470 96.999339    zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
28566 119.110221   zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
28779 123.599284   zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
28931 132.489104   zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
29163 149.048847   zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
29590 161.443986   zte_a7:09:66     Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.233
 1018 36.241610    Dell_0b:3a:c5    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.79
10763 49.169918    Dell_0b:3a:c5    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.79
  210 15.575969    Dell_0b:0a:19    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.80
  328 21.139831    Dell_0b:0a:19    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.80
19961 76.682593    Dell_0b:3a:59    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.86
27431 96.747803    Dell_0b:0b:7a    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.88
28461 112.906287   Dell_0b:39:ea    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.89
28796 124.728499   Dell_0b:39:ea    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.89
18660 71.044753    Dell_0b:3b:b8    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.90
  370 23.145396    Dell_0b:0a:2f    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.93
29829 172.402493   Dell_0b:0a:48    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.95
28286 102.310970   Dell_0b:12:30    Broadcast          ARP      60 Who has 10.10.10.2? Tell 10.10.10.96
```

```
> Frame 210: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{ED276ECA-254F-402C-A333-C9B62AA2A35B},
> Ethernet II, Src: Dell_0b:0a:19 (74:86:e2:0b:0a:19), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 74 86  e2 0b 0a 19 08 06 00 01   ······t· ········
0010  08 00 06 04 00 01 74 86  e2 0b 0a 19 0a 0a 0a 50   ······t· ·······
0020  00 00 00 00 00 00 0a 0a  0a 02 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Save and Document the Capture

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



tcp.stream eq 854

```
No.     Time         Source          Destination     Protocol Lengtl Info
1371… 1375.955632  35.190.80.1     10.10.10.103    TCP         66 443 → 2167 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=256
1371… 1375.955717  10.10.10.103    35.190.80.1     TCP         54 2167 → 443 [ACK] Seq=1 Ack=1 Win=65280 Len=0
1371… 1375.956388  10.10.10.103    35.190.80.1     TCP
1371… 1375.956388  10.10.10.103    35.190.80.1     TLSv1
1371… 1375.957951  35.190.80.1     10.10.10.103    TCP
1371… 1375.961157  35.190.80.1     10.10.10.103    TCP
1371… 1376.027584  35.190.80.1     10.10.10.103    TLSv1
1371… 1376.029374  10.10.10.103    35.190.80.1     TLSv1
1371… 1376.029534  10.10.10.103    35.190.80.1     TLSv1
1371… 1376.029611  10.10.10.103    35.190.80.1     TLSv1
1371… 1376.034638  35.190.80.1     10.10.10.103    TCP
1371… 1376.034638  35.190.80.1     10.10.10.103    TCP
1371… 1376.034638  35.190.80.1     10.10.10.103    TCP
1371… 1376.034958  35.190.80.1     10.10.10.103    TLSv1
1371… 1376.034958  35.190.80.1     10.10.10.103    TLSv1
1371… 1376.035674  10.10.10.103    35.190.80.1     TLSv1
1371… 1376.045584  35.190.80.1     10.10.10.103    TCP
1371… 1376.307400  35.190.80.1     10.10.10.103    TLSv1
1371… 1376.308915  10.10.10.103    35.190.80.1     TLSv1
1371… 1376.309084  10.10.10.103    35.190.80.1     TLSv1
1371… 1376.319611  35.190.80.1     10.10.10.103    TCP
1371… 1376.319611  35.190.80.1     10.10.10.103    TCP
1371… 1376.604238  35.190.80.1     10.10.10.103    TLSv1
1371… 1376.605230  10.10.10.103    35.190.80.1     TLSv1
1371… 1376.619173  35.190.80.1     10.10.10.103    TCP
```

```
> Frame 137174: 60 bytes on wire (480 bits), 60 bytes captured (480 bi
> Ethernet II, Src: 00:e2:69:0d:d5:ff (00:e2:69:0d:d5:ff), Dst: Dell_(
v Internet Protocol Version 4, Src: 35.190.80.1, Dst: 10.10.10.103
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x60 (DSCP: CS3, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x5e39 (24121)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 123
    Protocol: TCP (6)
    Header Checksum: 0x5907 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 35.190.80.1
    Destination Address: 10.10.10.103
    [Stream index: 186]
> Transmission Control Protocol, Src Port: 443, Dst Port: 2167, Seq: 
```

Wireshark · Save Capture File As

Look in: C:\Users\student32\Desktop

My Computer
student32

Name	Size	Type	Date Modified
wireshark.pcapng	25...iB	unknown	12-08-2025 11:32

File name:

Save as: Wireshark/... - pcapng

Save | Cancel | Help

Compression options

● Uncompressed

○ Compress with gzip

○ Compress with LZ4

Version (ip.version), 4 bits

Packets: 137417 · Displayed: 26 (0.0%) · Marked:

Analysis :

- **DNS (Domain Name System)** traffic was observed, resolving domain names such as openai.com and example.com into IP addresses.

- **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.