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

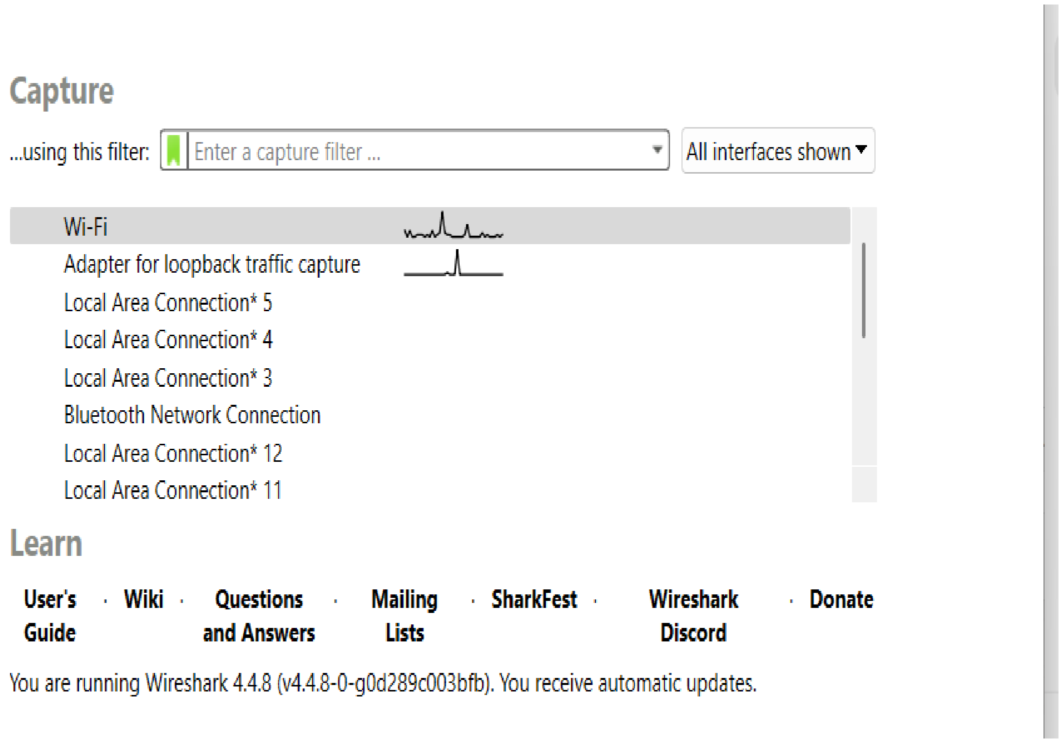
OBJECTIVE : Capture live network packets and identify basic protocols and traffic types

NAME : Priya Rose

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.



Capture

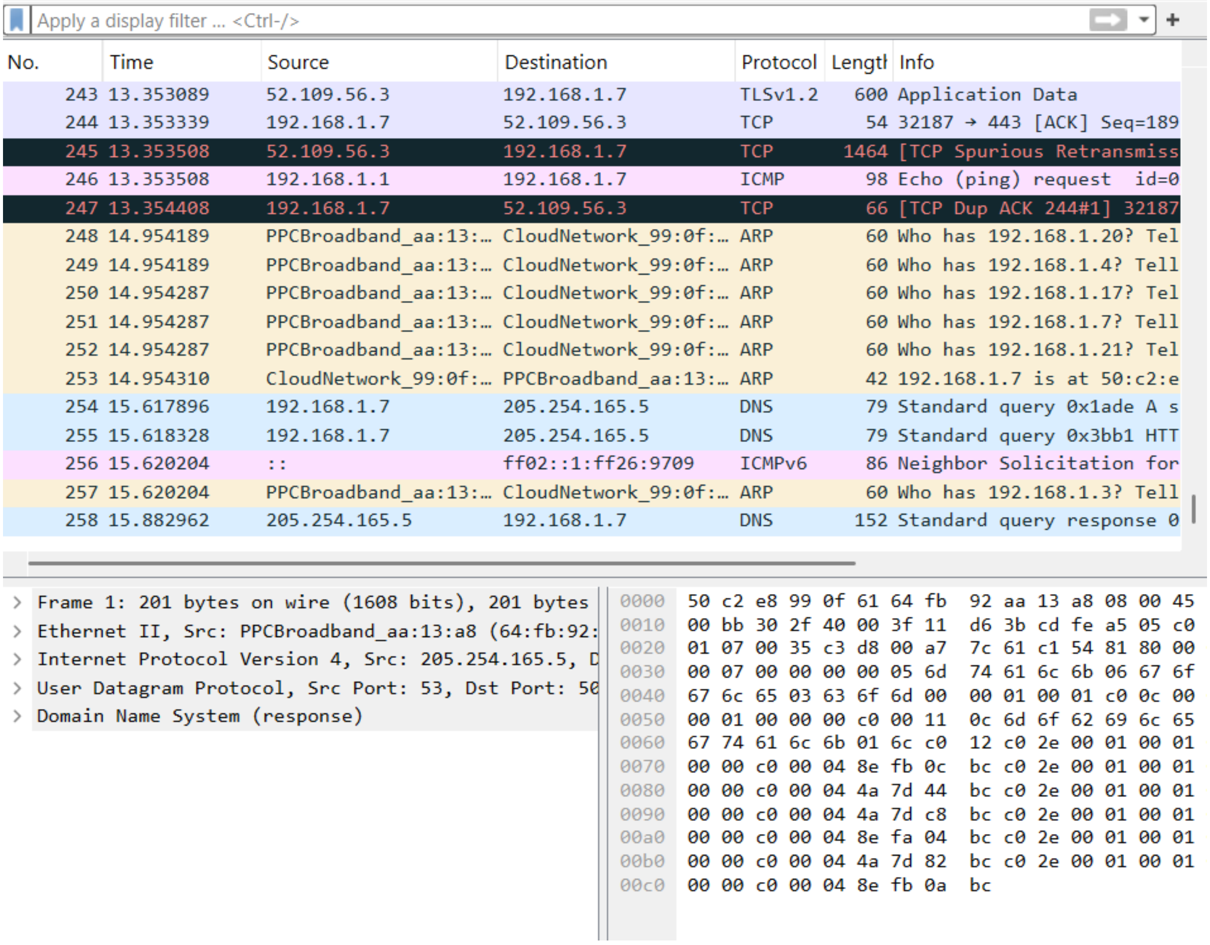
...using this filter: Enter a capture filter ... All interfaces shown

Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 5
Local Area Connection* 4
Local Area Connection* 3
Bluetooth Network Connection
Local Area Connection* 12
Local Area Connection* 11

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.



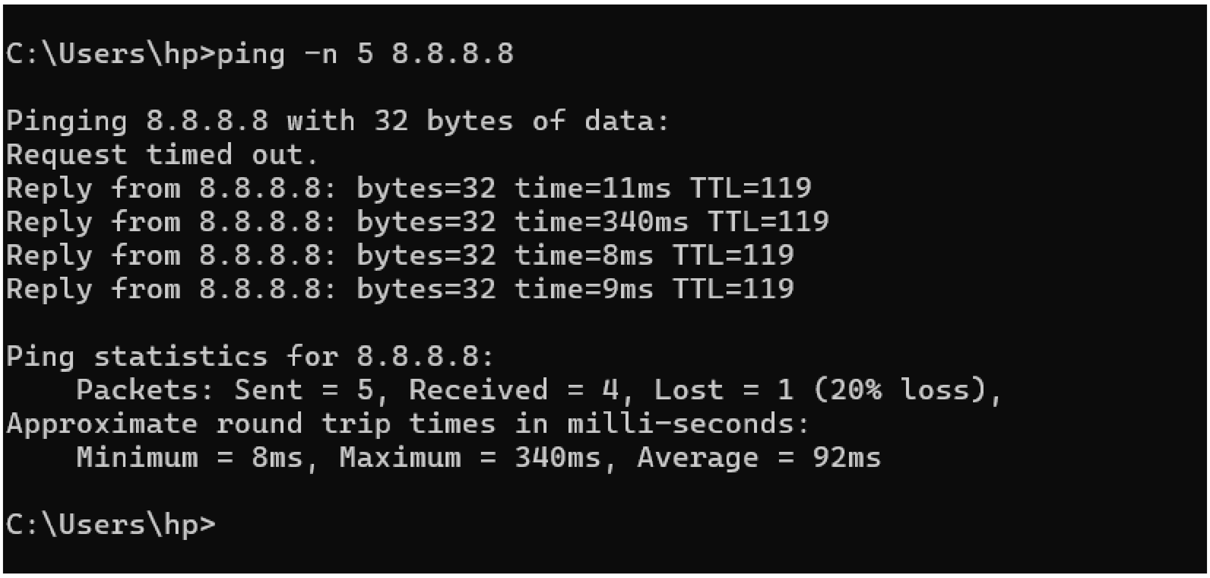
No.	Time	Source	Destination	Protocol	Lengtl	Info
243	13.353089	52.109.56.3	192.168.1.7	TLSv1.2	600	Application Data
244	13.353339	192.168.1.7	52.109.56.3	TCP	54	32187 → 443 [ACK] Seq=189
245	13.353508	52.109.56.3	192.168.1.7	TCP	1464	[TCP Spurious Retransmiss
246	13.353508	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request id=0
247	13.354408	192.168.1.7	52.109.56.3	TCP	66	[TCP Dup ACK 244#1] 32187
248	14.954189	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.20? Tel
249	14.954189	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.4? Tell
250	14.954287	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.17? Tel
251	14.954287	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.7? Tell
252	14.954287	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.21? Tel
253	14.954310	CloudNetwork_99:0f:…	PPCBroadband_aa:13:…	ARP	42	192.168.1.7 is at 50:c2:e
254	15.617896	192.168.1.7	205.254.165.5	DNS	79	Standard query 0x1ade A s
255	15.618328	192.168.1.7	205.254.165.5	DNS	79	Standard query 0x3bb1 HTT
256	15.620204	::	ff02::1:ff26:9709	ICMPv6	86	Neighbor Solicitation for
257	15.620204	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.3? Tell
258	15.882962	205.254.165.5	192.168.1.7	DNS	152	Standard query response 0

```
> Frame 1: 201 bytes on wire (1608 bits), 201 bytes
> Ethernet II, Src: PPCBroadband_aa:13:a8 (64:fb:92:
> Internet Protocol Version 4, Src: 205.254.165.5, D
> User Datagram Protocol, Src Port: 53, Dst Port: 50
> Domain Name System (response)
```

```
0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 00 45
0010  00 bb 30 2f 40 00 3f 11  d6 3b cd fe a5 05 c0
0020  01 07 00 35 c3 d8 00 a7  7c 61 c1 54 81 80 00
0030  00 07 00 00 00 00 05 6d  74 61 6c 6b 06 67 6f
0040  67 6c 65 03 63 6f 6d 00  00 01 00 01 c0 0c 00
0050  00 01 00 00 00 c0 00 11  0c 6d 6f 62 69 6c 65
0060  67 74 61 6c 6b 01 6c c0  12 c0 2e 00 01 00 01
0070  00 00 c0 00 04 8e fb 0c  bc c0 2e 00 01 00 01
0080  00 00 c0 00 04 4a 7d 44  bc c0 2e 00 01 00 01
0090  00 00 c0 00 04 4a 7d c8  bc c0 2e 00 01 00 01
00a0  00 00 c0 00 04 8e fa 04  bc c0 2e 00 01 00 01
00b0  00 00 c0 00 04 4a 7d 82  bc c0 2e 00 01 00 01
00c0  00 00 c0 00 04 8e fb 0a  bc
```

2) Generate traffic (do this while capture runs)

- Open a web page in your browser (HTTP or HTTPS).
- From **Command Prompt** run: ping -n 5 8.8.8.8 (sends 5 pings).
- Optionally: nslookup example.com or curl http://example.com (if installed). These produce ICMP, DNS, TCP and HTTP/TLS packets.

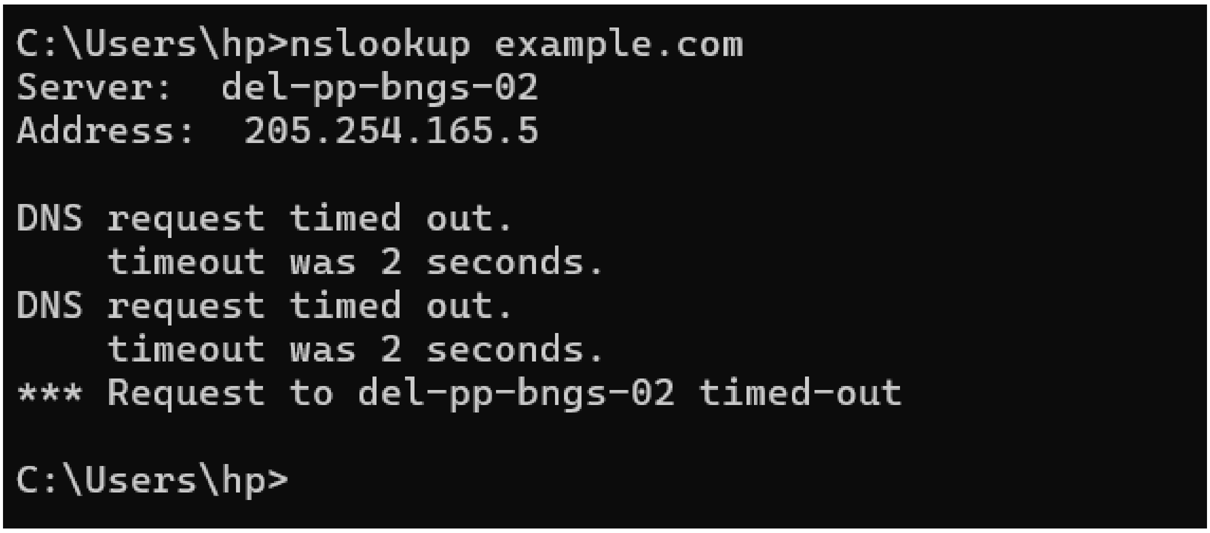


```
C:\Users\hp>ping -n 5 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Reply from 8.8.8.8: bytes=32 time=11ms TTL=119
Reply from 8.8.8.8: bytes=32 time=340ms TTL=119
Reply from 8.8.8.8: bytes=32 time=8ms TTL=119
Reply from 8.8.8.8: bytes=32 time=9ms TTL=119

Ping statistics for 8.8.8.8:
    Packets: Sent = 5, Received = 4, Lost = 1 (20% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 340ms, Average = 92ms

C:\Users\hp>
```



```
C:\Users\hp>nslookup example.com
Server:  del-pp-bngs-02
Address:  205.254.165.5

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to del-pp-bngs-02 timed-out

C:\Users\hp>
```

3) Stop capture

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

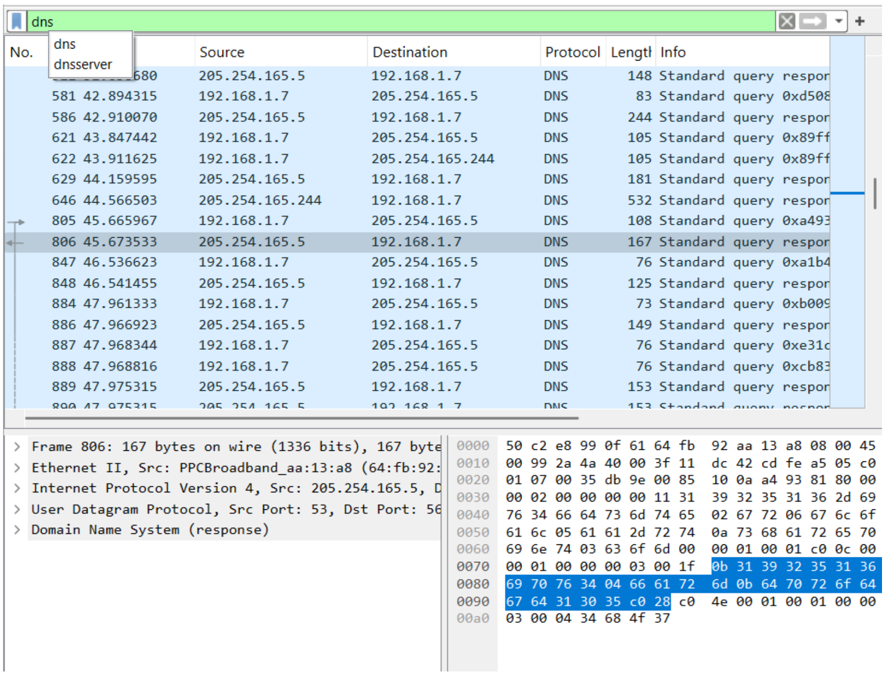
4) Inspect captured packets (basic)

- 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 → DNS queries/responses

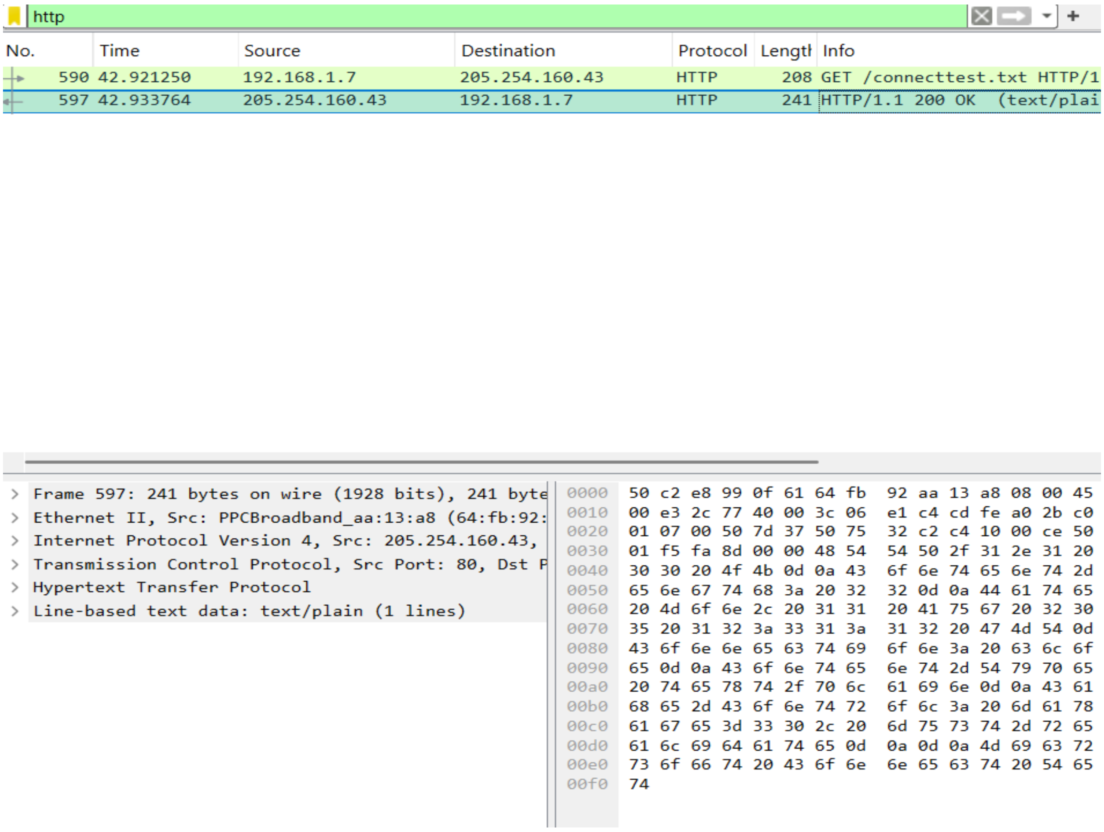


No.		Source	Destination	Protocol	Lengtl	Info
[illegible]	[illegible]680	205.254.165.5	192.168.1.7	DNS	148	Standard query respor
581	42.894315	192.168.1.7	205.254.165.5	DNS	83	Standard query 0xd508
586	42.910070	205.254.165.5	192.168.1.7	DNS	244	Standard query respor
621	43.847442	192.168.1.7	205.254.165.5	DNS	105	Standard query 0x89ff
622	43.911625	192.168.1.7	205.254.165.244	DNS	105	Standard query 0x89ff
629	44.159595	205.254.165.5	192.168.1.7	DNS	181	Standard query respor
646	44.566503	205.254.165.244	192.168.1.7	DNS	532	Standard query respor
805	45.665967	192.168.1.7	205.254.165.5	DNS	108	Standard query 0xa493
806	45.673533	205.254.165.5	192.168.1.7	DNS	167	Standard query respor
847	46.536623	192.168.1.7	205.254.165.5	DNS	76	Standard query 0xa1b4
848	46.541455	205.254.165.5	192.168.1.7	DNS	125	Standard query respor
884	47.961333	192.168.1.7	205.254.165.5	DNS	73	Standard query 0xb009
886	47.966923	205.254.165.5	192.168.1.7	DNS	149	Standard query respor
887	47.968344	192.168.1.7	205.254.165.5	DNS	76	Standard query 0xe31c
888	47.968816	192.168.1.7	205.254.165.5	DNS	76	Standard query 0xcb83
889	47.975315	205.254.165.5	192.168.1.7	DNS	153	Standard query respor
890	47.975315	205.254.165.5	192.168.1.7	DNS	153	Standard query respor

```
> Frame 806: 167 bytes on wire (1336 bits), 167 byte
> Ethernet II, Src: PPCBroadband_aa:13:a8 (64:fb:92:
> Internet Protocol Version 4, Src: 205.254.165.5, D
> User Datagram Protocol, Src Port: 53, Dst Port: 56
> Domain Name System (response)
```

```
0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 00 45
0010  00 99 2a 4a 40 00 3f 11  dc 42 cd fe a5 05 c0
0020  01 07 00 35 db 9e 00 85  10 0a a4 93 81 80 00
0030  00 02 00 00 00 00 11 31  39 32 35 31 36 2d 69
0040  76 34 66 64 73 6d 74 65  02 67 72 06 67 6c 6f
0050  61 6c 05 61 61 2d 72 74  0a 73 68 61 72 65 70
0060  69 6e 74 03 63 6f 6d 00  00 01 00 01 c0 0c 00
0070  00 01 00 00 00 03 00 1f  0b 31 39 32 35 31 36
0080  69 70 76 34 04 66 61 72  6d 0b 64 70 72 6f 64
0090  67 64 31 30 35 c0 28 c0  4e 00 01 00 01 00 00
00a0  03 00 04 34 68 4f 37
```

- http → unencrypted HTTP traffic

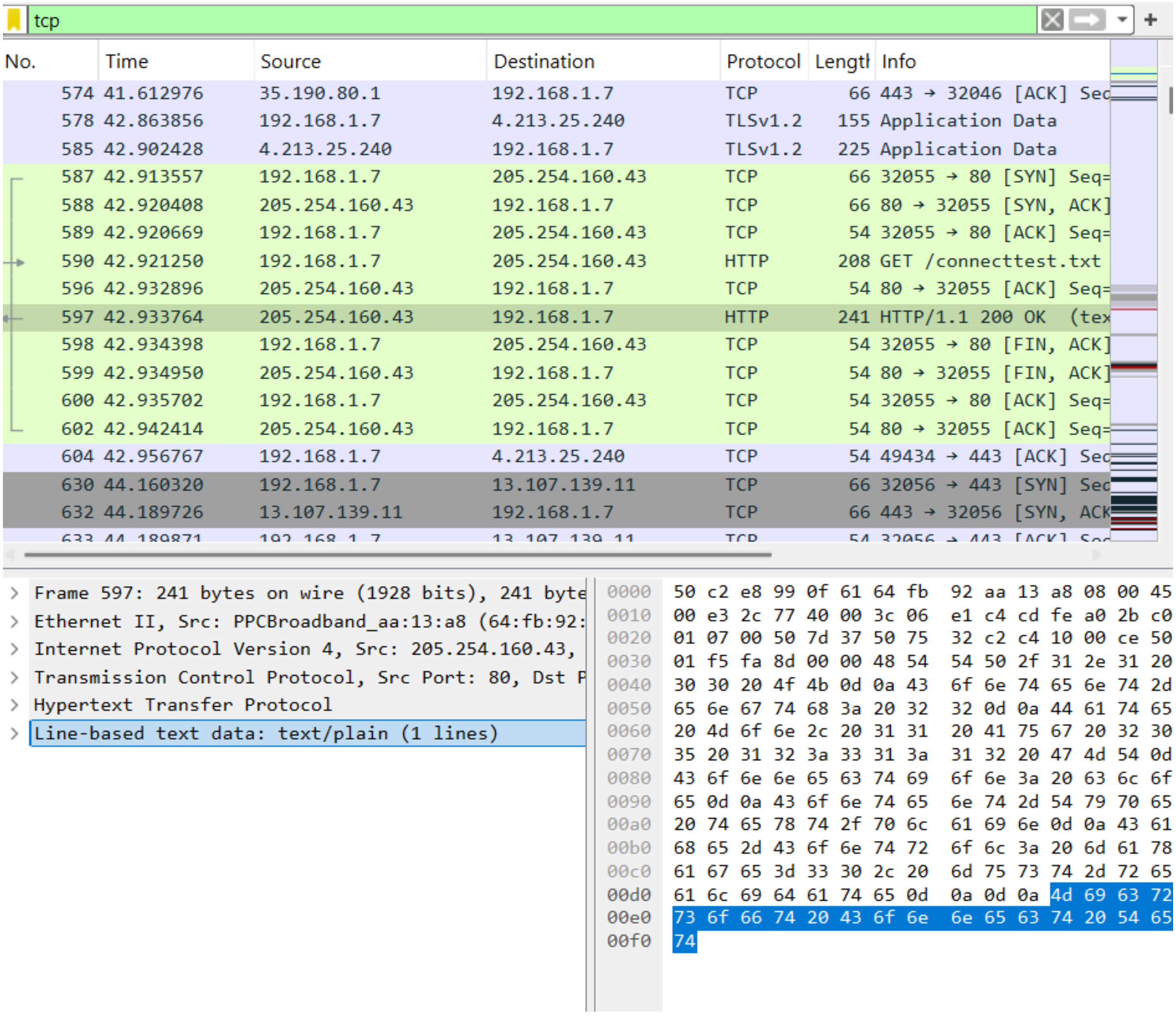


No.	Time	Source	Destination	Protocol	Lengtl	Info
590	42.921250	192.168.1.7	205.254.160.43	HTTP	208	GET /connecttest.txt HTTP/1
597	42.933764	205.254.160.43	192.168.1.7	HTTP	241	HTTP/1.1 200 OK (text/plai

```
> Frame 597: 241 bytes on wire (1928 bits), 241 byte
> Ethernet II, Src: PPCBroadband_aa:13:a8 (64:fb:92:
> Internet Protocol Version 4, Src: 205.254.160.43,
> Transmission Control Protocol, Src Port: 80, Dst P
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 00 45
0010  00 e3 2c 77 40 00 3c 06  e1 c4 cd fe a0 2b c0
0020  01 07 00 50 7d 37 50 75  32 c2 c4 10 00 ce 50
0030  01 f5 fa 8d 00 00 48 54  54 50 2f 31 2e 31 20
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65
0060  20 4d 6f 6e 2c 20 31 31  20 41 75 67 20 32 30
0070  35 20 31 32 3a 33 31 3a  31 32 20 47 4d 54 0d
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65
00f0  74
```

- tcp → all TCP packets



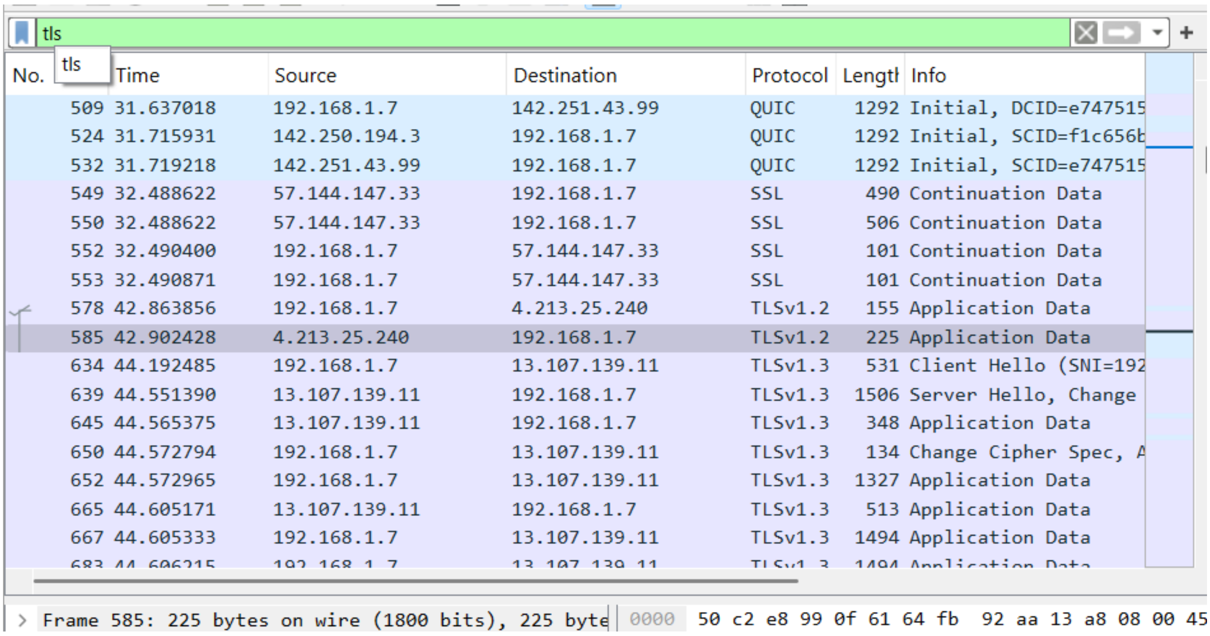
```
tcp

No.     Time        Source           Destination      Protocol Lengtl Info
    574 41.612976   35.190.80.1      192.168.1.7      TCP        66 443 → 32046 [ACK] Sec
    578 42.863856   192.168.1.7      4.213.25.240     TLSv1.2   155 Application Data
    585 42.902428   4.213.25.240     192.168.1.7      TLSv1.2   225 Application Data
    587 42.913557   192.168.1.7      205.254.160.43   TCP        66 32055 → 80 [SYN] Seq=
    588 42.920408   205.254.160.43   192.168.1.7      TCP        66 80 → 32055 [SYN, ACK]
    589 42.920669   192.168.1.7      205.254.160.43   TCP        54 32055 → 80 [ACK] Seq=
    590 42.921250   192.168.1.7      205.254.160.43   HTTP      208 GET /connecttest.txt
    596 42.932896   205.254.160.43   192.168.1.7      TCP        54 80 → 32055 [ACK] Seq=
    597 42.933764   205.254.160.43   192.168.1.7      HTTP      241 HTTP/1.1 200 OK  (tex
    598 42.934398   192.168.1.7      205.254.160.43   TCP        54 32055 → 80 [FIN, ACK]
    599 42.934950   205.254.160.43   192.168.1.7      TCP        54 80 → 32055 [FIN, ACK]
    600 42.935702   192.168.1.7      205.254.160.43   TCP        54 32055 → 80 [ACK] Seq=
    602 42.942414   205.254.160.43   192.168.1.7      TCP        54 80 → 32055 [ACK] Seq=
    604 42.956767   192.168.1.7      4.213.25.240     TCP        54 49434 → 443 [ACK] Sec
    630 44.160320   192.168.1.7      13.107.139.11    TCP        66 32056 → 443 [SYN] Sec
    632 44.189726   13.107.139.11    192.168.1.7      TCP        66 443 → 32056 [SYN, ACK
    633 44.189871   192.168.1.7      13.107.139.11    TCP        54 32056 → 443 [ACK] Sec
```

```
> Frame 597: 241 bytes on wire (1928 bits), 241 byte
> Ethernet II, Src: PPCBroadband_aa:13:a8 (64:fb:92:
> Internet Protocol Version 4, Src: 205.254.160.43,
> Transmission Control Protocol, Src Port: 80, Dst P
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 00 45
0010  00 e3 2c 77 40 00 3c 06  e1 c4 cd fe a0 2b c0
0020  01 07 00 50 7d 37 50 75  32 c2 c4 10 00 ce 50
0030  01 f5 fa 8d 00 00 48 54  54 50 2f 31 2e 31 20
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65
0060  20 4d 6f 6e 2c 20 31 31  20 41 75 67 20 32 30
0070  35 20 31 32 3a 33 31 3a  31 32 20 47 4d 54 0d
0080  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 63 6c 6f
0090  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65
00a0  20 74 65 78 74 2f 70 6c  61 69 6e 0d 0a 43 61
00b0  68 65 2d 43 6f 6e 74 72  6f 6c 3a 20 6d 61 78
00c0  61 67 65 3d 33 30 2c 20  6d 75 73 74 2d 72 65
00d0  61 6c 69 64 61 74 65 0d  0a 0d 0a 4d 69 63 72
00e0  73 6f 66 74 20 43 6f 6e  6e 65 63 74 20 54 65
00f0  74
```

- tls (or ssl) → TLS (HTTPS) handshakes & records

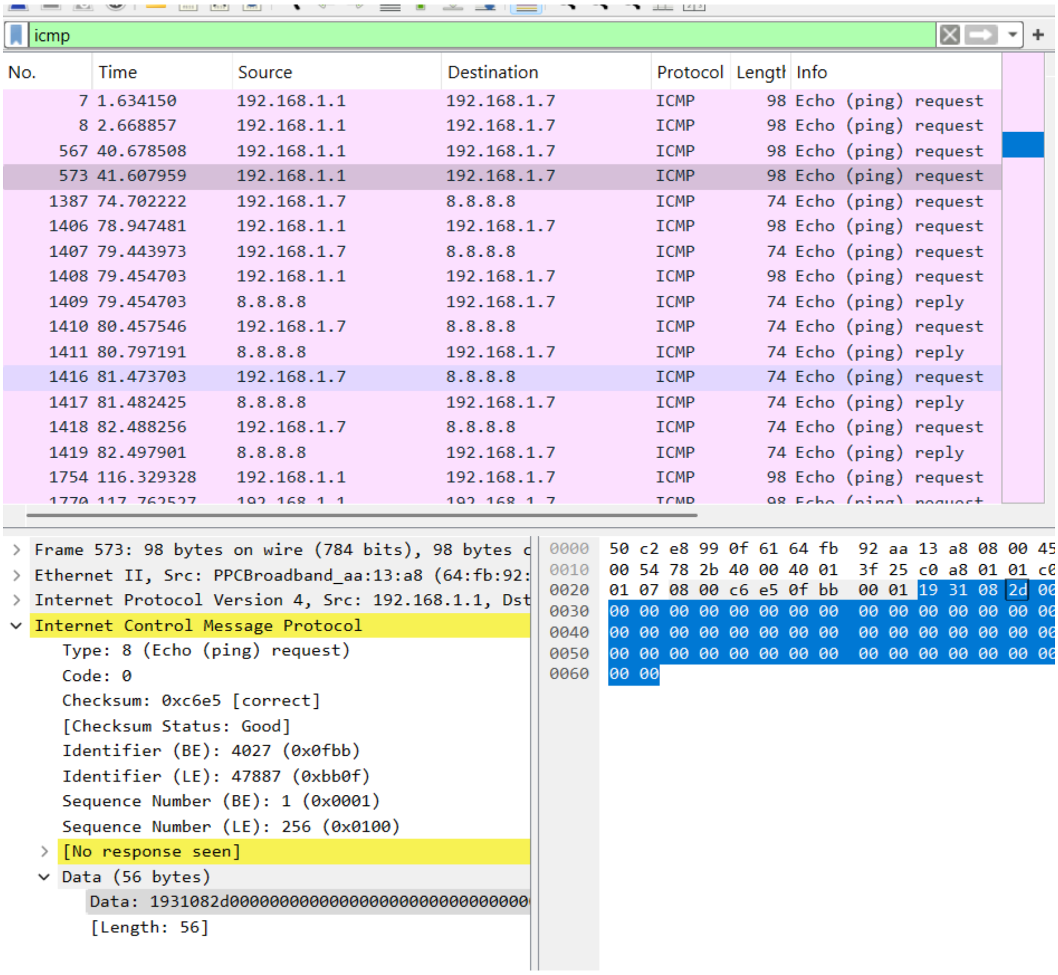


```
tls

No.  tls  Time        Source           Destination      Protocol Lengtl Info
    509 31.637018   192.168.1.7      142.251.43.99    QUIC     1292 Initial, DCID=e747515
    524 31.715931   142.250.194.3    192.168.1.7      QUIC     1292 Initial, SCID=f1c656b
    532 31.719218   142.251.43.99    192.168.1.7      QUIC     1292 Initial, SCID=e747515
    549 32.488622   57.144.147.33    192.168.1.7      SSL       490 Continuation Data
    550 32.488622   57.144.147.33    192.168.1.7      SSL       506 Continuation Data
    552 32.490400   192.168.1.7      57.144.147.33    SSL       101 Continuation Data
    553 32.490871   192.168.1.7      57.144.147.33    SSL       101 Continuation Data
    578 42.863856   192.168.1.7      4.213.25.240     TLSv1.2   155 Application Data
    585 42.902428   4.213.25.240     192.168.1.7      TLSv1.2   225 Application Data
    634 44.192485   192.168.1.7      13.107.139.11    TLSv1.3   531 Client Hello (SNI=192
    639 44.551390   13.107.139.11    192.168.1.7      TLSv1.3  1506 Server Hello, Change
    645 44.565375   13.107.139.11    192.168.1.7      TLSv1.3   348 Application Data
    650 44.572794   192.168.1.7      13.107.139.11    TLSv1.3   134 Change Cipher Spec, A
    652 44.572965   192.168.1.7      13.107.139.11    TLSv1.3  1327 Application Data
    665 44.605171   13.107.139.11    192.168.1.7      TLSv1.3   513 Application Data
    667 44.605333   192.168.1.7      13.107.139.11    TLSv1.3  1494 Application Data
    683 44.606215   192.168.1.7      13.107.139.11    TLSv1.3  1494 Application Data
```

```
> Frame 585: 225 bytes on wire (1800 bits), 225 byte  0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 00 45
```

- icmp → ping/Echo request & reply



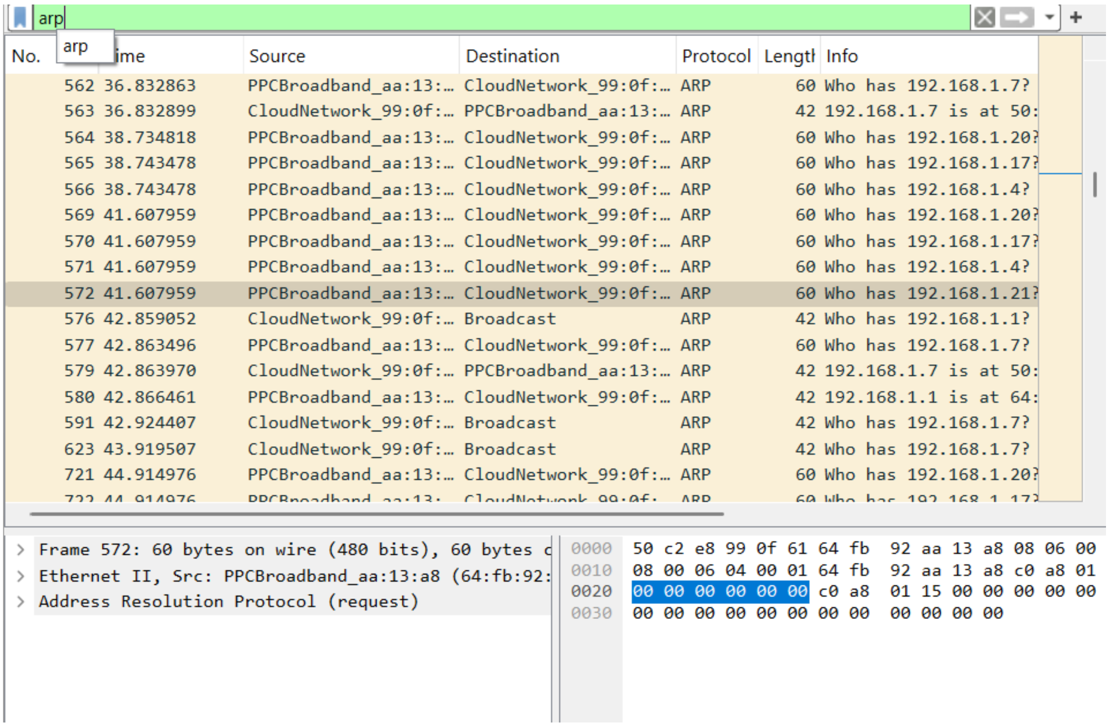
icmp

No.	Time	Source	Destination	Protocol	Lengtl	Info
7	1.634150	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request
8	2.668857	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request
567	40.678508	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request
573	41.607959	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request
1387	74.702222	192.168.1.7	8.8.8.8	ICMP	74	Echo (ping) request
1406	78.947481	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request
1407	79.443973	192.168.1.7	8.8.8.8	ICMP	74	Echo (ping) request
1408	79.454703	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request
1409	79.454703	8.8.8.8	192.168.1.7	ICMP	74	Echo (ping) reply
1410	80.457546	192.168.1.7	8.8.8.8	ICMP	74	Echo (ping) request
1411	80.797191	8.8.8.8	192.168.1.7	ICMP	74	Echo (ping) reply
1416	81.473703	192.168.1.7	8.8.8.8	ICMP	74	Echo (ping) request
1417	81.482425	8.8.8.8	192.168.1.7	ICMP	74	Echo (ping) reply
1418	82.488256	192.168.1.7	8.8.8.8	ICMP	74	Echo (ping) request
1419	82.497901	8.8.8.8	192.168.1.7	ICMP	74	Echo (ping) reply
1754	116.329328	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request
1770	117.762527	192.168.1.1	192.168.1.7	ICMP	98	Echo (ping) request

```
> Frame 573: 98 bytes on wire (784 bits), 98 bytes c
> Ethernet II, Src: PPCBroadband_aa:13:a8 (64:fb:92:
> Internet Protocol Version 4, Src: 192.168.1.1, Dst
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xc6e5 [correct]
    [Checksum Status: Good]
    Identifier (BE): 4027 (0x0fbb)
    Identifier (LE): 47887 (0xbb0f)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
  > [No response seen]
  v Data (56 bytes)
      Data: 1931082d00000000000000000000000000000
      [Length: 56]
```

```
0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 00 45
0010  00 54 78 2b 40 00 40 01  3f 25 c0 a8 01 01 c0
0020  01 07 08 00 c6 e5 0f bb  00 01 19 31 08 2d 00
0030  00 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 00
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00
0060  00 00
```

- arp → ARP requests/replies



arp

arp

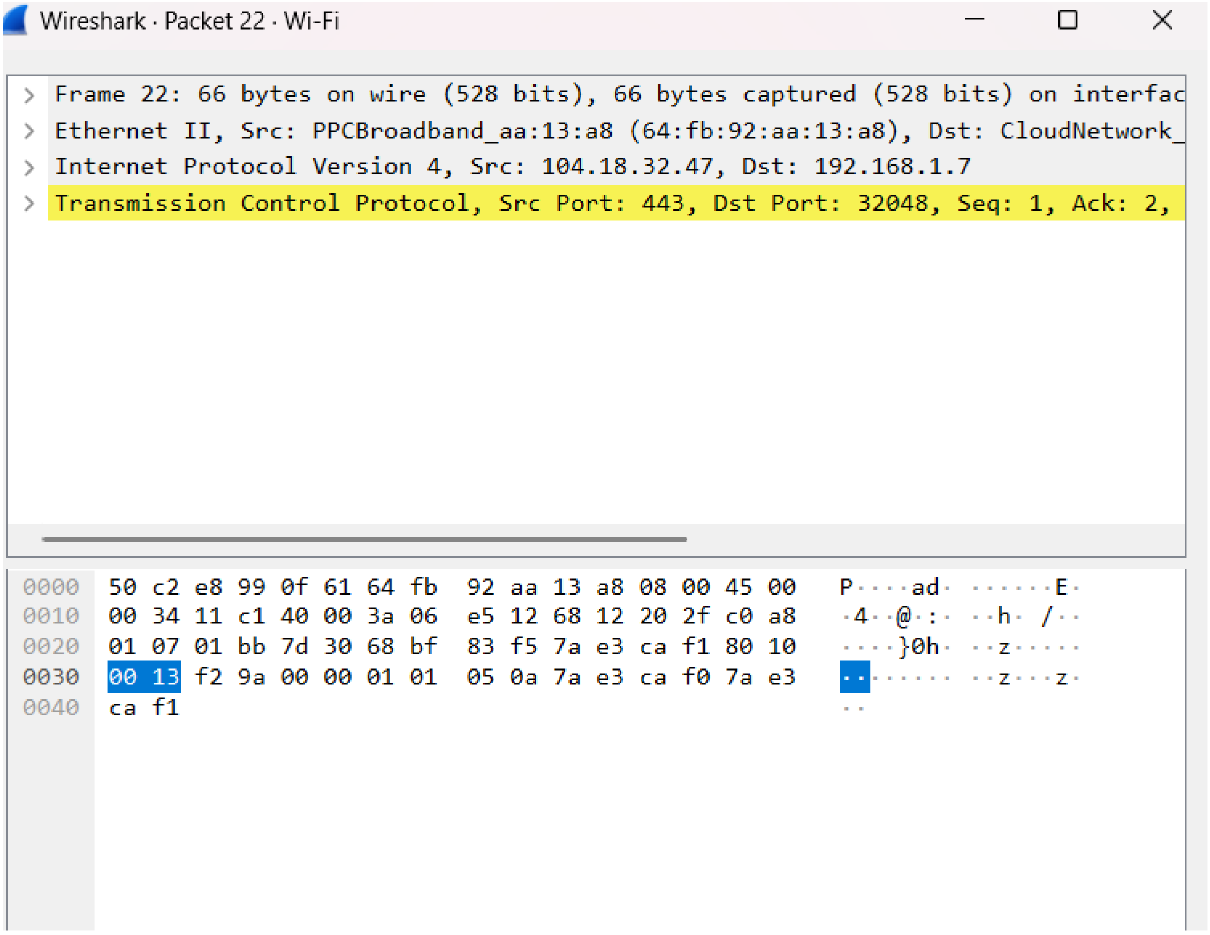
No.	Time	Source	Destination	Protocol	Lengtl	Info
562	36.832863	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.7?
563	36.832899	CloudNetwork_99:0f:…	PPCBroadband_aa:13:…	ARP	42	192.168.1.7 is at 50:
564	38.734818	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.20?
565	38.743478	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.17?
566	38.743478	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.4?
569	41.607959	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.20?
570	41.607959	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.17?
571	41.607959	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.4?
572	41.607959	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.21?
576	42.859052	CloudNetwork_99:0f:…	Broadcast	ARP	42	Who has 192.168.1.1?
577	42.863496	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.7?
579	42.863970	CloudNetwork_99:0f:…	PPCBroadband_aa:13:…	ARP	42	192.168.1.7 is at 50:
580	42.866461	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	42	192.168.1.1 is at 64:
591	42.924407	CloudNetwork_99:0f:…	Broadcast	ARP	42	Who has 192.168.1.7?
623	43.919507	CloudNetwork_99:0f:…	Broadcast	ARP	42	Who has 192.168.1.7?
721	44.914976	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.20?
722	44.914976	PPCBroadband_aa:13:…	CloudNetwork_99:0f:…	ARP	60	Who has 192.168.1.17?

```
> Frame 572: 60 bytes on wire (480 bits), 60 bytes c
> Ethernet II, Src: PPCBroadband_aa:13:a8 (64:fb:92:
> Address Resolution Protocol (request)
```

```
0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 06 00
0010  08 00 06 04 00 01 64 fb  92 aa 13 a8 c0 a8 01
0020  00 00 00 00 00 00 c0 a8  01 15 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

6) 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.



Wireshark · Packet 22 · Wi-Fi

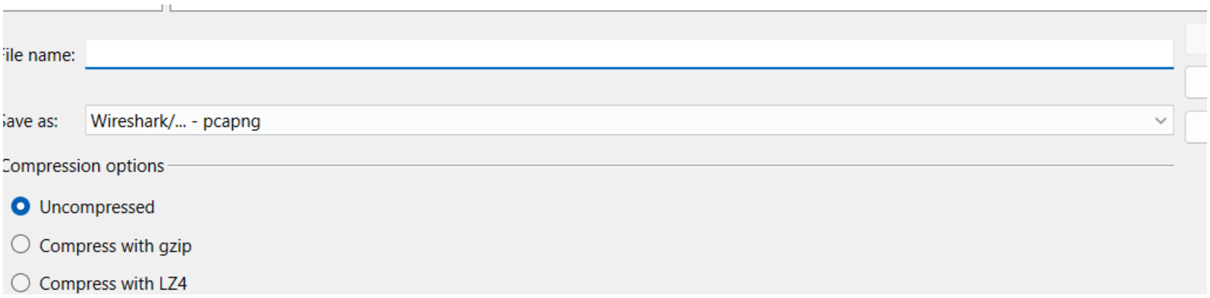
```
> Frame 22: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interfac
> Ethernet II, Src: PPCBroadband_aa:13:a8 (64:fb:92:aa:13:a8), Dst: CloudNetwork_
> Internet Protocol Version 4, Src: 104.18.32.47, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 443, Dst Port: 32048, Seq: 1, Ack: 2,
```

```
0000  50 c2 e8 99 0f 61 64 fb  92 aa 13 a8 08 00 45 00   P····ad· ······E·
0010  00 34 11 c1 40 00 3a 06  e5 12 68 12 20 2f c0 a8   ·4··@·:· ··h· /··
0020  01 07 01 bb 7d 30 68 bf  83 f5 7a e3 ca f1 80 10   ····}0h· ··z·····
0030  00 13 f2 9a 00 00 01 01  05 0a 7a e3 ca f0 7a e3   ········ ··z···z·
0040  ca f1                                              ··
```

7) Save/export as .pcap

1. To save entire capture: **File → Save As…**
2. In the Save dialog: choose location and filename.
3. **Save as type:** choose **“libpcap (tcpdump) - pcap”** if you specifically need .pcap (default is usually .pcapng).

4. If you only want the currently displayed packets exported: **File → Export Specified Packets…** → choose *Displayed* or *Selected* → choose file type .pcap.



ile name:

ave as: Wireshark/... - pcapng

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).

Summary Conclusion

The capture demonstrated normal and expected network behavior during the 1-minute observation window. At least three distinct protocols—**DNS**, **ICMP**, and **TCP/TLS**—were successfully identified and analyzed. DNS queries resolved hostnames correctly, ICMP verified network reachability, and TLS confirmed the use of secure encrypted communication for web browsing. The traffic volume and patterns aligned with the controlled actions taken during the test, and no anomalies or malicious activity were present.