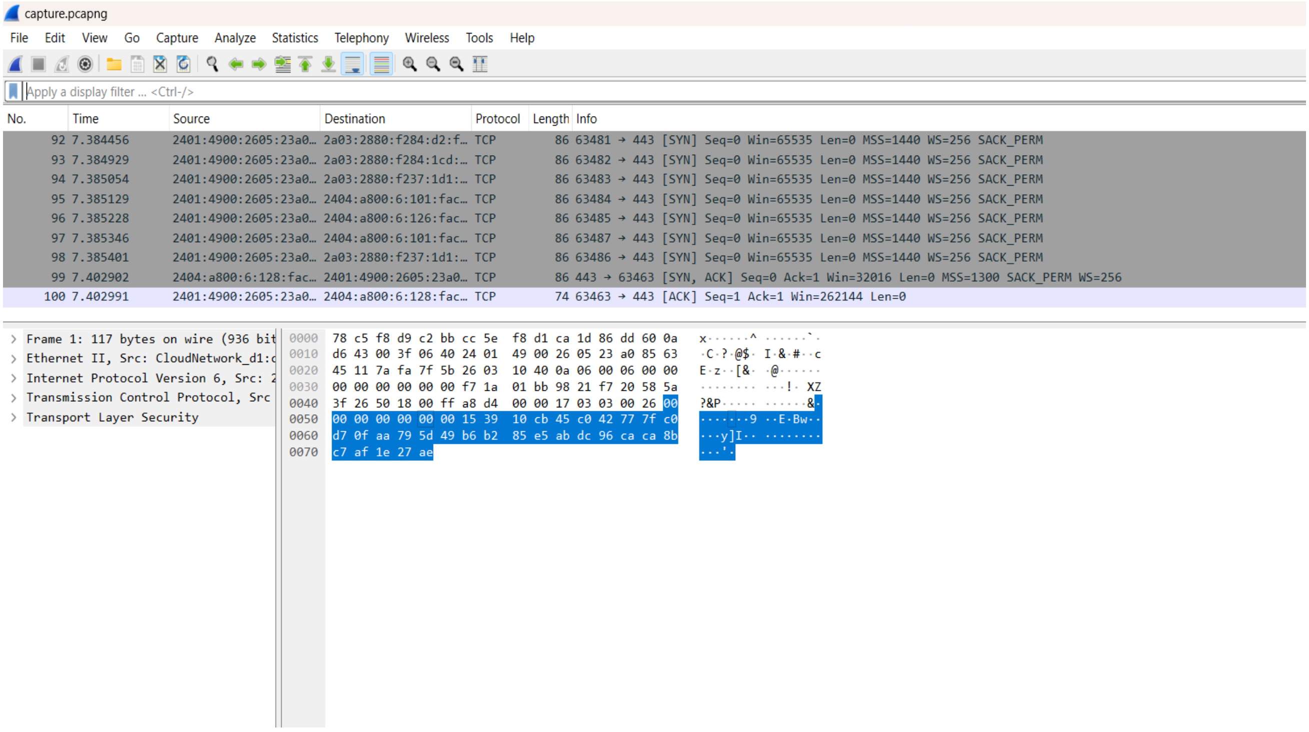
CAPTURING AND ANALYSIS PACKETS USING WIRESHARK TOOL

Wi-fi Capture……

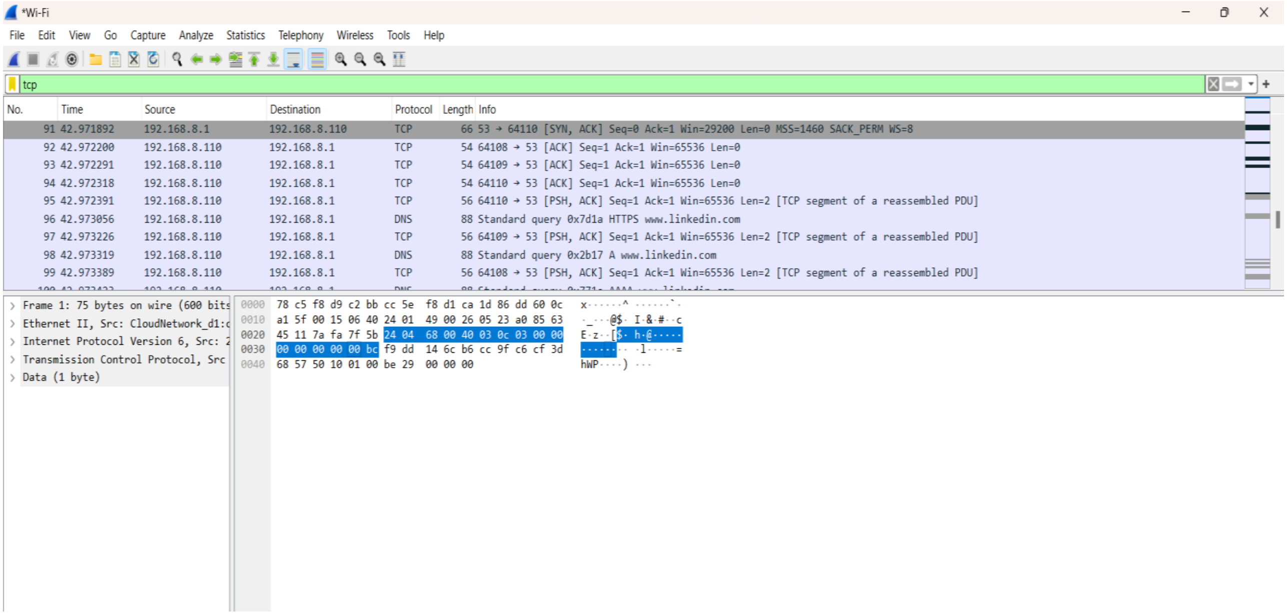


No.	Time	Source	Destination	Protocol	Length	Info
92	7.384456	2401:4900:2605:23a0…	2a03:2880:f284:d2:f…	TCP	86	63481 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
93	7.384929	2401:4900:2605:23a0…	2a03:2880:f284:1cd:…	TCP	86	63482 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
94	7.385054	2401:4900:2605:23a0…	2a03:2880:f237:1d1:…	TCP	86	63483 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
95	7.385129	2401:4900:2605:23a0…	2404:a800:6:101:fac…	TCP	86	63484 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
96	7.385228	2401:4900:2605:23a0…	2404:a800:6:126:fac…	TCP	86	63485 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
97	7.385346	2401:4900:2605:23a0…	2404:a800:6:101:fac…	TCP	86	63487 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
98	7.385401	2401:4900:2605:23a0…	2a03:2880:f237:1d1:…	TCP	86	63486 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
99	7.402902	2404:a800:6:128:fac…	2401:4900:2605:23a0…	TCP	86	443 → 63463 [SYN, ACK] Seq=0 Ack=1 Win=32016 Len=0 MSS=1300 SACK_PERM WS=256
100	7.402991	2401:4900:2605:23a0…	2404:a800:6:128:fac…	TCP	74	63463 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0

```
> Frame 1: 117 bytes on wire (936 bit
> Ethernet II, Src: CloudNetwork_d1:c
> Internet Protocol Version 6, Src: 2
> Transmission Control Protocol, Src
> Transport Layer Security
```

```
0000  78 c5 f8 d9 c2 bb cc 5e  f8 d1 ca 1d 86 dd 60 0a   x·····^ ······`·
0010  d6 43 00 3f 06 40 24 01  49 00 26 05 23 a0 85 63   ·C·?·@$· I·&·#··c
0020  45 11 7a fa 7f 5b 26 03  10 40 0a 06 00 06 00 00   E·z··[&· ·@······
0030  00 00 00 00 00 00 f7 1a  01 bb 98 21 f7 20 58 5a   ········ ···!· XZ
0040  3f 26 50 18 00 ff a8 d4  00 00 17 03 03 00 26 00   ?&P····· ······&·
0050  00 00 00 00 00 00 15 39  10 cb 45 c0 42 77 7f c0   ·······9 ··E·Bw··
0060  d7 0f aa 79 5d 49 b6 b2  85 e5 ab dc 96 ca ca 8b   ···y]I·· ········
0070  c7 af 1e 27 ae                                     ···'·
```

1.Filter to display only TCP/UDP Packets



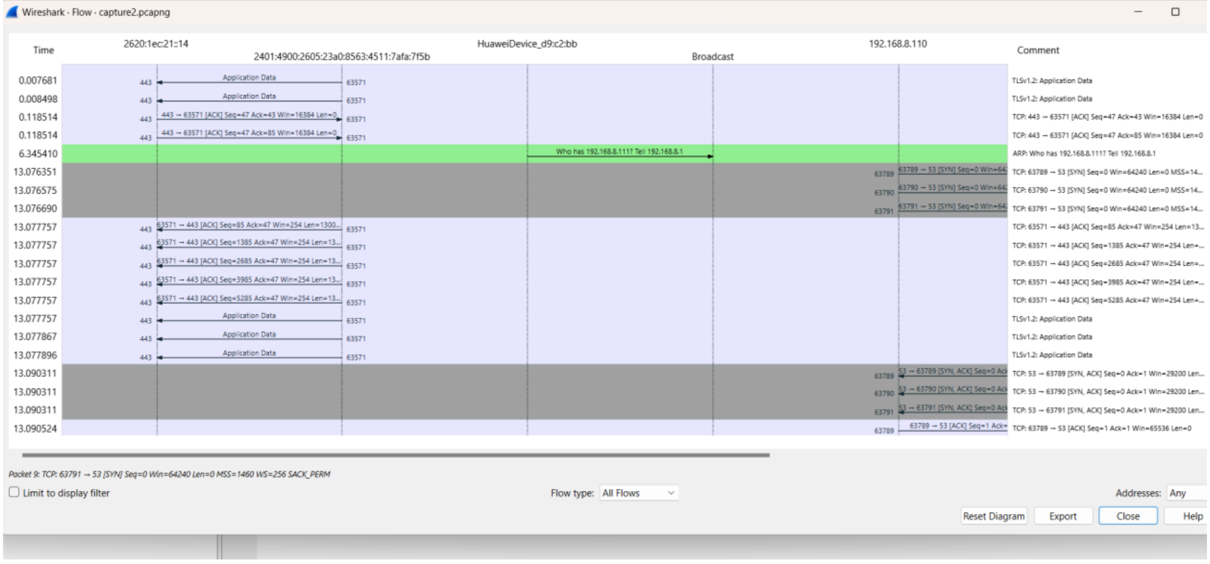
tcp

```
No.   Time        Source          Destination     Protocol Length Info
   91 42.971892   192.168.8.1     192.168.8.110   TCP      66 53 → 64110 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=8
   92 42.972200   192.168.8.110   192.168.8.1     TCP      54 64108 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   93 42.972291   192.168.8.110   192.168.8.1     TCP      54 64109 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   94 42.972318   192.168.8.110   192.168.8.1     TCP      54 64110 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0
   95 42.972391   192.168.8.110   192.168.8.1     TCP      56 64110 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PDU]
   96 42.973056   192.168.8.110   192.168.8.1     DNS      88 Standard query 0x7d1a HTTPS www.linkedin.com
   97 42.973226   192.168.8.110   192.168.8.1     TCP      56 64109 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PDU]
   98 42.973319   192.168.8.110   192.168.8.1     DNS      88 Standard query 0x2b17 A www.linkedin.com
   99 42.973389   192.168.8.110   192.168.8.1     TCP      56 64108 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=2 [TCP segment of a reassembled PDU]
```

```
> Frame 1: 75 bytes on wire (600 bits
> Ethernet II, Src: CloudNetwork_d1:c
> Internet Protocol Version 6, Src: 2
> Transmission Control Protocol, Src
> Data (1 byte)
```

```
0000  78 c5 f8 d9 c2 bb cc 5e  f8 d1 ca 1d 86 dd 60 0c   x······^ ······`·
0010  a1 5f 00 15 06 40 24 01  49 00 26 05 23 a0 85 63   ·_···@$· I·&·#··c
0020  45 11 7a fa 7f 5b 24 04  68 00 40 03 0c 03 00 00   E·z··[$· h·@·····
0030  00 00 00 00 00 bc f9 dd  14 6c b6 cc 9f c6 cf 3d   ········ ·l·····=
0040  68 57 50 10 01 00 be 29  00 00 00                  hWP····) ···
```

Flow Chart



Wireshark · Flow · capture2.pcapng
2620:1ec:21::14
2401:4900:2605:23a0:8563:4511:7afa:7f5b
HuaweiDevice_d9:c2:bb
Broadcast
192.168.8.110
443
63571
63789
63790
63791
Application Data
443 → 63571 [ACK] Seq=47 Ack=43 Win=16384 Len=0
443 → 63571 [ACK] Seq=47 Ack=85 Win=16384 Len=0
Who has 192.168.8.111? Tell 192.168.8.1
63571 → 443 [ACK] Seq=85 Ack=47 Win=254 Len=1300...
63571 → 443 [ACK] Seq=1385 Ack=47 Win=254 Len=13...
63571 → 443 [ACK] Seq=2685 Ack=47 Win=254 Len=13...
63571 → 443 [ACK] Seq=3985 Ack=47 Win=254 Len=13...
63571 → 443 [ACK] Seq=5285 Ack=47 Win=254 Len=13...
Reset Diagram
Export
Close
Help

Time	Comment
0.007681	TLSv1.2: Application Data
0.008498	TLSv1.2: Application Data
0.118514	TCP: 443 → 63571 [ACK] Seq=47 Ack=43 Win=16384 Len=0
0.118514	TCP: 443 → 63571 [ACK] Seq=47 Ack=85 Win=16384 Len=0
6.345410	ARP: Who has 192.168.8.111? Tell 192.168.8.1
13.076351	TCP: 63789 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=14...
13.076575	TCP: 63790 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=14...
13.076690	TCP: 63791 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=14...
13.077757	TCP: 63571 → 443 [ACK] Seq=85 Ack=47 Win=254 Len=13...
13.077757	TCP: 63571 → 443 [ACK] Seq=1385 Ack=47 Win=254 Len=...
13.077757	TCP: 63571 → 443 [ACK] Seq=2685 Ack=47 Win=254 Len=...
13.077757	TCP: 63571 → 443 [ACK] Seq=3985 Ack=47 Win=254 Len=...
13.077757	TCP: 63571 → 443 [ACK] Seq=5285 Ack=47 Win=254 Len=...
13.077757	TLSv1.2: Application Data
13.077867	TLSv1.2: Application Data
13.077896	TLSv1.2: Application Data
13.090311	TCP: 53 → 63789 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len...
13.090311	TCP: 53 → 63790 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len...
13.090311	TCP: 53 → 63791 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len...
13.090524	TCP: 63789 → 53 [ACK] Seq=1 Ack=1 Win=65536 Len=0

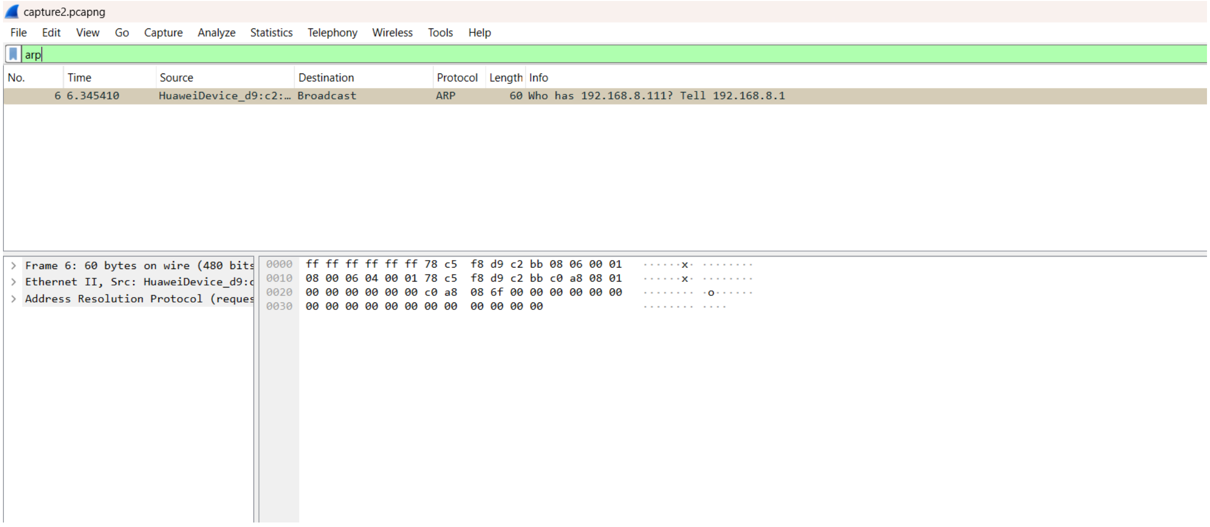
Packet 9: TCP: 63791 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

☐ Limit to display filter

Flow type: All Flows

Addresses: Any

2.Filter to display ARP Packets


capture2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

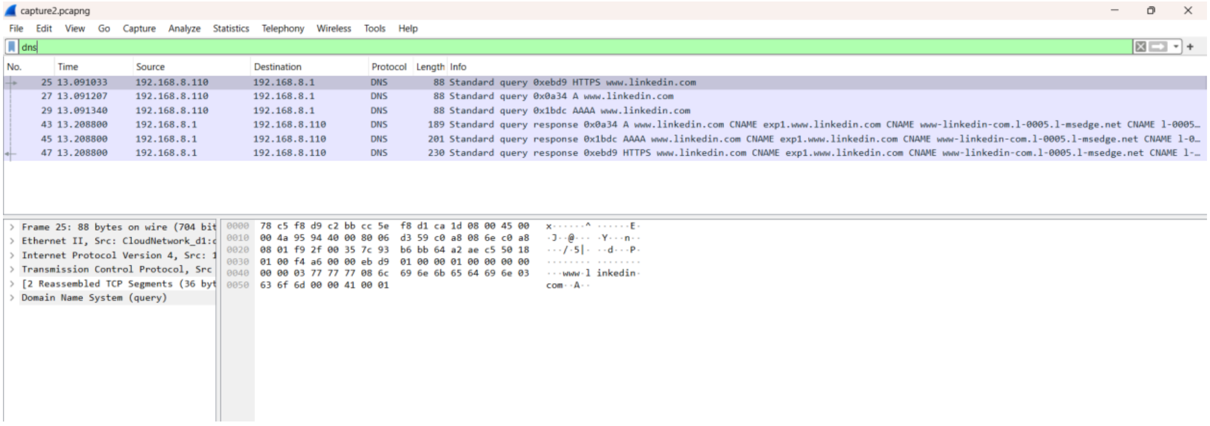
arp

```
No.    Time        Source              Destination  Protocol  Length  Info
     6 6.345410    HuaweiDevice_d9:c2:… Broadcast    ARP           60 Who has 192.168.8.111? Tell 192.168.8.1
```

```
> Frame 6: 60 bytes on wire (480 bits
> Ethernet II, Src: HuaweiDevice_d9:c
> Address Resolution Protocol (reques
```

```
0000  ff ff ff ff ff ff 78 c5  f8 d9 c2 bb 08 06 00 01   ······x· ········
0010  08 00 06 04 00 01 78 c5  f8 d9 c2 bb c0 a8 08 01   ······x· ········
0020  00 00 00 00 00 00 c0 a8  08 6f 00 00 00 00 00 00   ········ ·o······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

3.Filter only DNS Packets

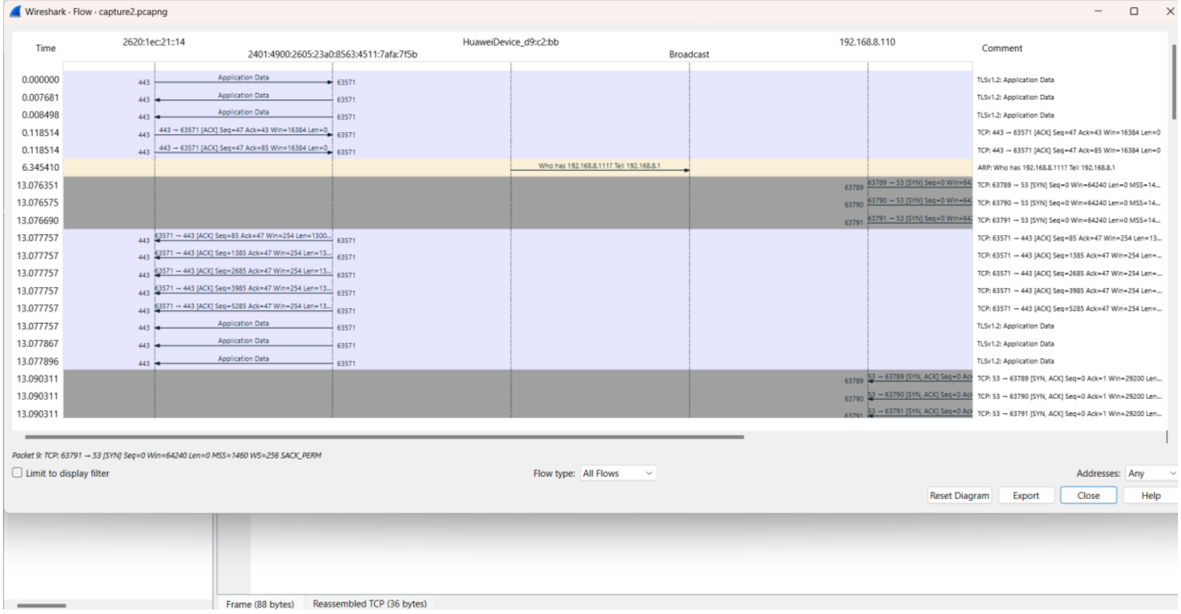

capture2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

```
No.   Time       Source         Destination    Protocol Length Info
   25 13.091033  192.168.8.110  192.168.8.1    DNS          88 Standard query 0xebd9 HTTPS www.linkedin.com
   27 13.091207  192.168.8.110  192.168.8.1    DNS          88 Standard query 0x0a34 A www.linkedin.com
   29 13.091340  192.168.8.110  192.168.8.1    DNS          88 Standard query 0x1bdc AAAA www.linkedin.com
   43 13.208800  192.168.8.1    192.168.8.110  DNS         189 Standard query response 0x0a34 A www.linkedin.com CNAME exp1.www.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-0005…
   45 13.208800  192.168.8.1    192.168.8.110  DNS         201 Standard query response 0x1bdc AAAA www.linkedin.com CNAME exp1.www.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-0…
   47 13.208800  192.168.8.1    192.168.8.110  DNS         230 Standard query response 0xebd9 HTTPS www.linkedin.com CNAME exp1.www.linkedin.com CNAME www-linkedin-com.l-0005.l-msedge.net CNAME l-…
```

```
> Frame 25: 88 bytes on wire (704 bit
> Ethernet II, Src: CloudNetwork_d1:c
> Internet Protocol Version 4, Src: 1
> Transmission Control Protocol, Src
> [2 Reassembled TCP Segments (36 byt
> Domain Name System (query)
```

```
0000  78 c5 f8 d9 c2 bb cc 5e  f8 d1 ca 1d 08 00 45 00   x······^ ······E·
0010  00 4a 95 94 40 00 80 06  d3 59 c0 a8 08 6e c0 a8   ·J··@··· ·Y···n··
0020  08 01 f9 2f 00 35 7c 93  b6 bb 64 a2 ae c5 50 18   ···/·5|· ··d···P·
0030  01 00 f4 a6 00 00 eb d9  01 00 00 01 00 00 00 00   ········ ········
0040  00 00 03 77 77 77 08 6c  69 6e 6b 65 64 69 6e 03   ···www·l inkedin·
0050  63 6f 6d 00 00 41 00 01                            com··A··
```



```
0.000000    TLSv1.2: Application Data
0.007681    TLSv1.2: Application Data
0.008498    TLSv1.2: Application Data
0.118514    TCP: 443 → 63571 [ACK] Seq=47 Ack=43 Win=16384 Len=0
0.118514    TCP: 443 → 63571 [ACK] Seq=47 Ack=85 Win=16384 Len=0
6.345410    ARP: Who has 192.168.8.111? Tell 192.168.8.1
13.076351   TCP: 63789 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=14…
13.076575   TCP: 63790 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=14…
13.076690   TCP: 63791 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=14…
13.077757   TCP: 63571 → 443 [ACK] Seq=85 Ack=47 Win=254 Len=13…
13.077757   TCP: 63571 → 443 [ACK] Seq=1385 Ack=47 Win=254 Len=…
13.077757   TCP: 63571 → 443 [ACK] Seq=2685 Ack=47 Win=254 Len=…
13.077757   TCP: 63571 → 443 [ACK] Seq=3985 Ack=47 Win=254 Len=…
13.077757   TCP: 63571 → 443 [ACK] Seq=5285 Ack=47 Win=254 Len=…
13.077757   TLSv1.2: Application Data
13.077867   TLSv1.2: Application Data
13.077896   TLSv1.2: Application Data
13.090311   TCP: 53 → 63789 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len…
13.090311   TCP: 53 → 63790 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len…
13.090311   TCP: 53 → 63791 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len…
```

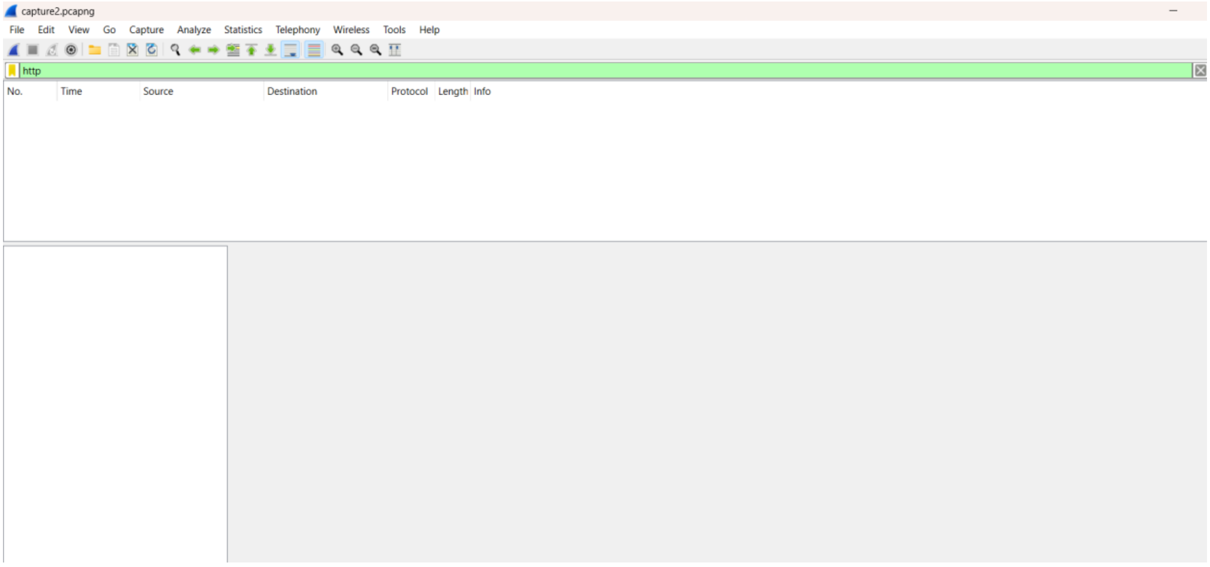
Packet 9: TCP: 63791 → 53 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

☐ Limit to display filter

Flow type: All Flows

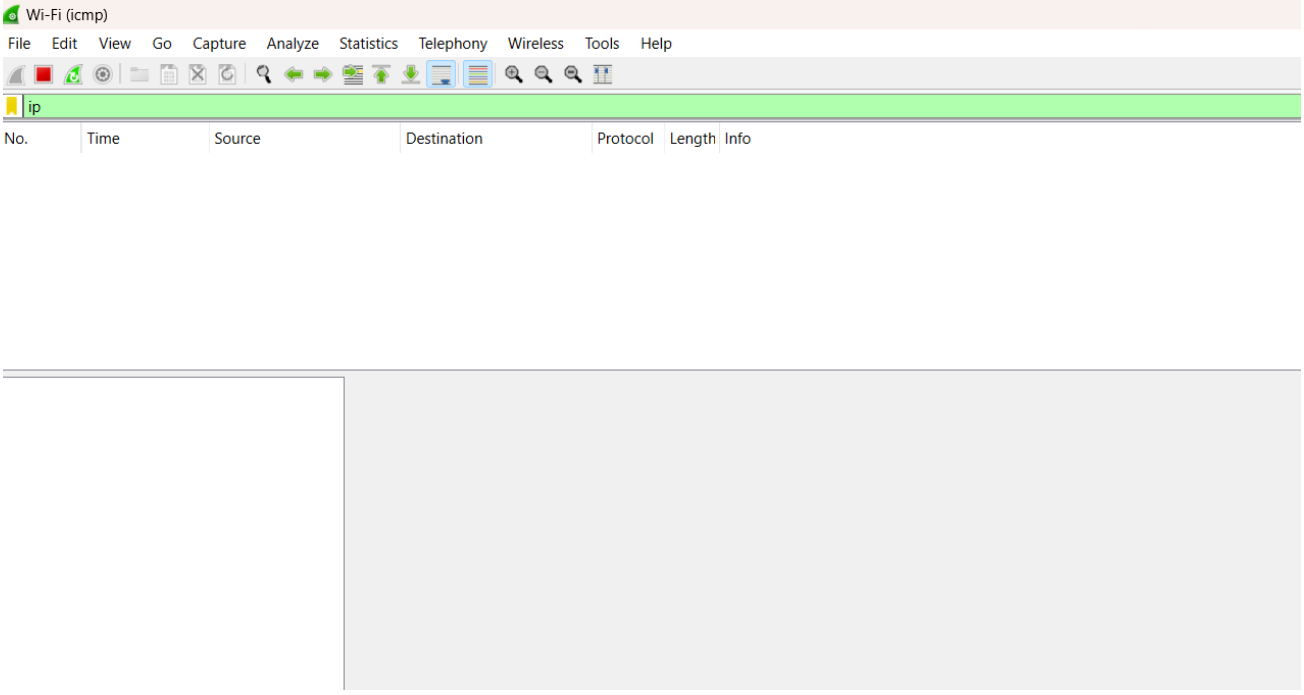
Addresses: Any

4.Display only HTTP Packets


capture2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info

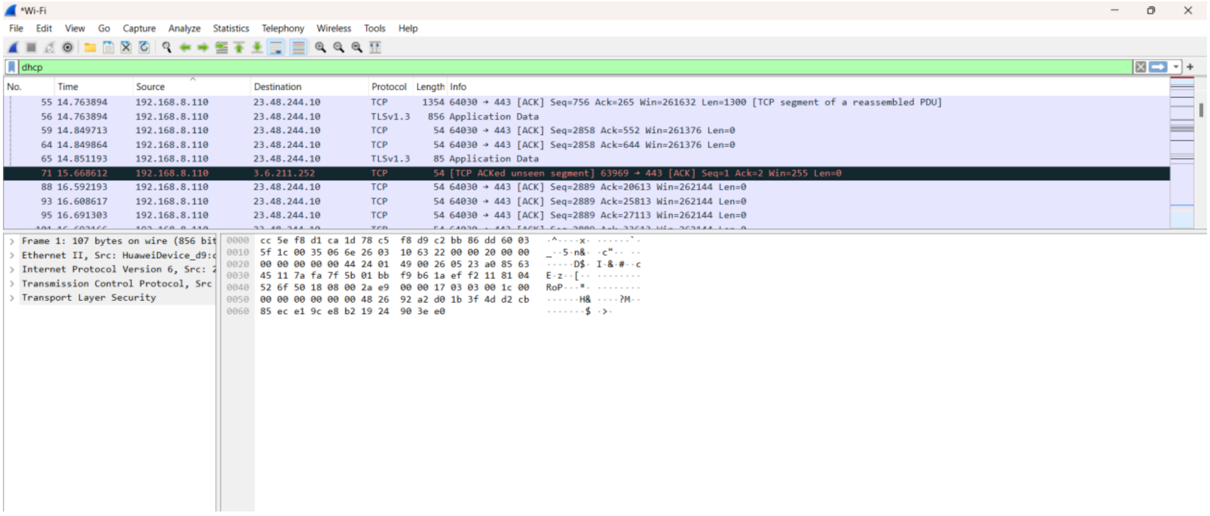
http

5.Filter to display IP/ICMP Packets


Wi-Fi (icmp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info

ip

6.Display only DHCP Packets


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

dhcp

```
No.   Time        Source          Destination    Protocol  Length Info
   55 14.763894   192.168.8.110   23.48.244.10   TCP       1354 64030 → 443 [ACK] Seq=756 Ack=265 Win=261632 Len=1300 [TCP segment of a reassembled PDU]
   56 14.763894   192.168.8.110   23.48.244.10   TLSv1.3    856 Application Data
   59 14.849713   192.168.8.110   23.48.244.10   TCP         54 64030 → 443 [ACK] Seq=2858 Ack=552 Win=261376 Len=0
   64 14.849864   192.168.8.110   23.48.244.10   TCP         54 64030 → 443 [ACK] Seq=2858 Ack=644 Win=261376 Len=0
   65 14.851193   192.168.8.110   23.48.244.10   TLSv1.3     85 Application Data
   71 15.668612   192.168.8.110   3.6.211.252    TCP         54 [TCP ACKed unseen segment] 63969 → 443 [ACK] Seq=1 Ack=2 Win=255 Len=0
   88 16.592193   192.168.8.110   23.48.244.10   TCP         54 64030 → 443 [ACK] Seq=2889 Ack=20613 Win=262144 Len=0
   93 16.608617   192.168.8.110   23.48.244.10   TCP         54 64030 → 443 [ACK] Seq=2889 Ack=25813 Win=262144 Len=0
   95 16.691303   192.168.8.110   23.48.244.10   TCP         54 64030 → 443 [ACK] Seq=2889 Ack=27113 Win=262144 Len=0
```

```
> Frame 1: 107 bytes on wire (856 bit
> Ethernet II, Src: HuaweiDevice_d9:c
> Internet Protocol Version 6, Src: 2
> Transmission Control Protocol, Src
> Transport Layer Security
```

```
0000  cc 5e f8 d1 ca 1d 78 c5  f8 d9 c2 bb 86 dd 60 03   ·^····x· ······`·
0010  5f 1c 00 35 06 6e 26 03  10 63 22 00 00 20 00 00   _··5·n&· ·c"·· ··
0020  00 00 00 00 00 44 24 01  49 00 26 05 23 a0 85 63   ·····D$· I·&·#··c
0030  45 11 7a fa 7f 5b 01 bb  f9 b6 1a ef f2 11 81 04   E·z··[·· ········
0040  52 6f 50 18 08 00 2a e9  00 00 17 03 03 00 1c 00   RoP···*· ········
0050  00 00 00 00 00 00 48 26  92 a2 d0 1b 3f 4d d2 cb   ······H& ····?M··
0060  85 ec e1 9c e8 b2 19 24  90 3e e0                  ·······$ ·>·
```