Assignment 4

Usman Faisal, Abdullah Dar, Sami Khokar

Cyber Security

BSCS-6A

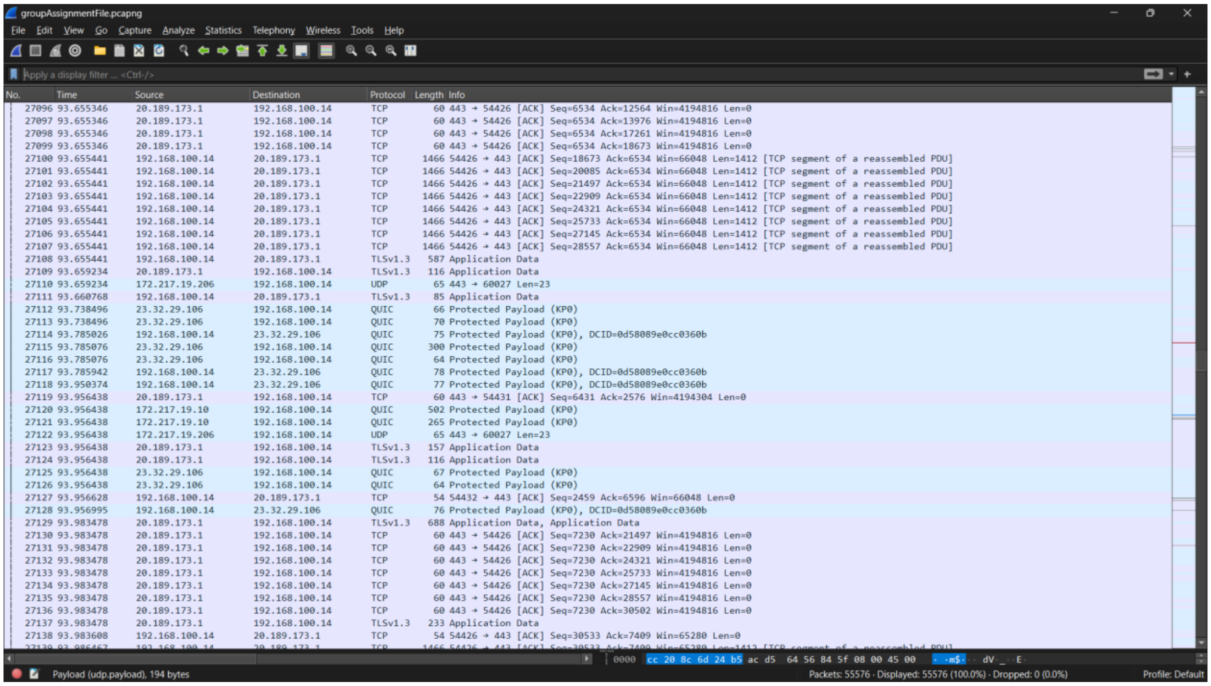
21L-5373, 21L-7512, 21L-1868

Activity 1: Capture Traffic

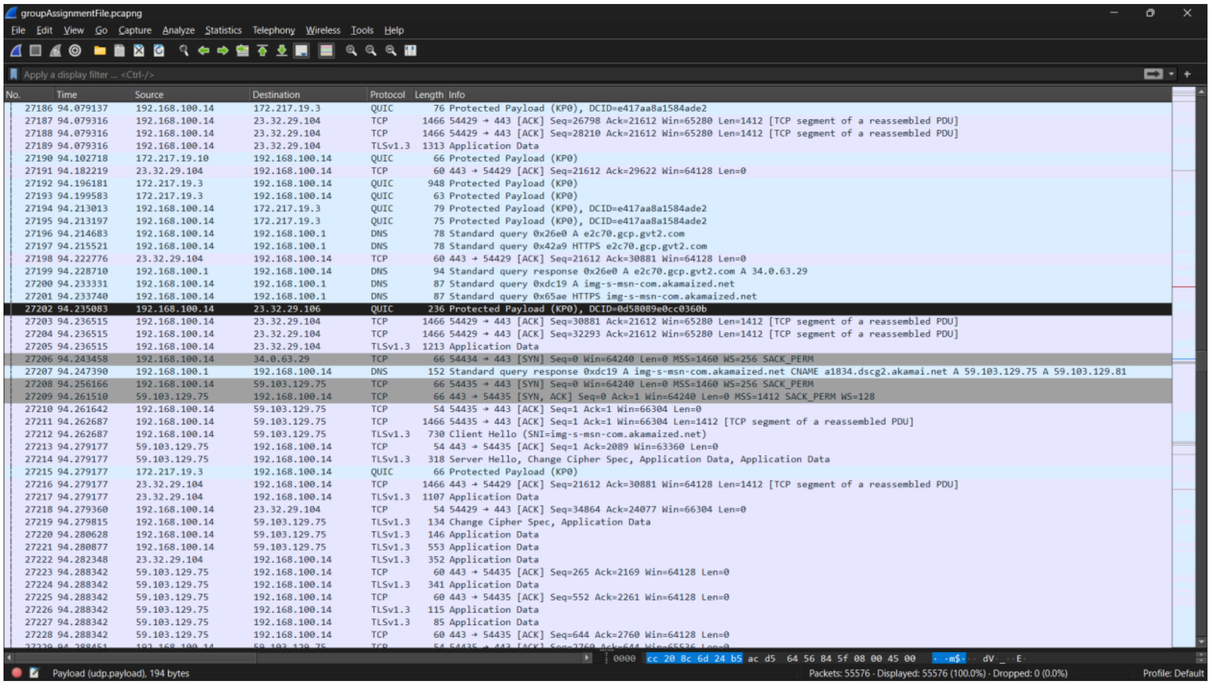
Showing all the traffic captured while doing web browsing and other activities required a local area network connection.

Protocols like UDP, TCP, QUIC, TLS etc. used.

UDP facilitates real-time applications and DNS queries, TCP ensures reliable communication, QUIC enhances web performance, and TLS secures data, collectively ensuring seamless and secure internet interactions.

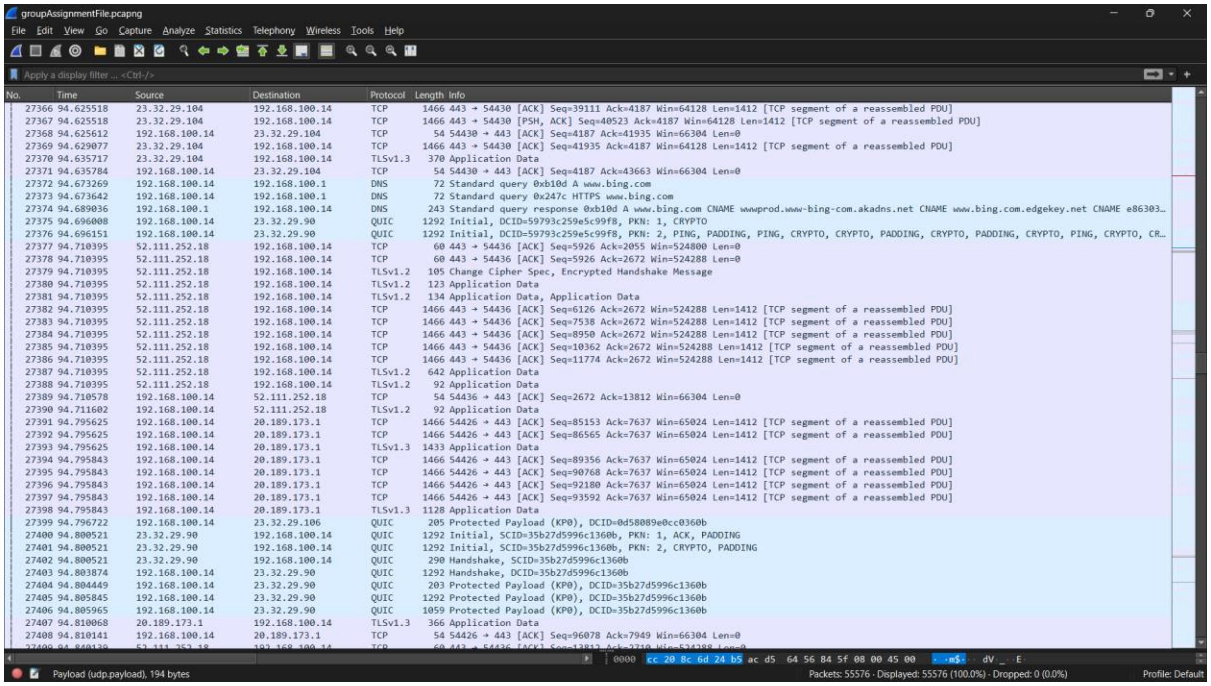

groupAssignmentFile.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source          Destination     Protocol Length Info
27096 93.655346 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=6534 Ack=12564 Win=4194816 Len=0
27097 93.655346 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=6534 Ack=13976 Win=4194816 Len=0
27098 93.655346 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=6534 Ack=17261 Win=4194816 Len=0
27099 93.655346 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=6534 Ack=18673 Win=4194816 Len=0
27100 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=18673 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27101 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=20085 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27102 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=21497 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27103 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=22909 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27104 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=24321 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27105 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=25733 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27106 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=27145 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27107 93.655441 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=28557 Ack=6534 Win=66048 Len=1412 [TCP segment of a reassembled PDU]
27108 93.655441 192.168.100.14  20.189.173.1    TLSv1.3   587 Application Data
27109 93.659234 20.189.173.1    192.168.100.14  TLSv1.3   116 Application Data
27110 93.659234 172.217.19.206  192.168.100.14  UDP        65 443 → 60027 Len=23
27111 93.660768 192.168.100.14  20.189.173.1    TLSv1.3    85 Application Data
27112 93.738496 23.32.29.106    192.168.100.14  QUIC       66 Protected Payload (KP0)
27113 93.738496 23.32.29.106    192.168.100.14  QUIC       70 Protected Payload (KP0)
27114 93.785026 192.168.100.14  23.32.29.106    QUIC       75 Protected Payload (KP0), DCID=0d58089e0cc0360b
27115 93.785076 23.32.29.106    192.168.100.14  QUIC      300 Protected Payload (KP0)
27116 93.785076 23.32.29.106    192.168.100.14  QUIC       64 Protected Payload (KP0)
27117 93.785942 192.168.100.14  23.32.29.106    QUIC       78 Protected Payload (KP0), DCID=0d58089e0cc0360b
27118 93.950374 192.168.100.14  23.32.29.106    QUIC       77 Protected Payload (KP0), DCID=0d58089e0cc0360b
27119 93.956438 20.189.173.1    192.168.100.14  TCP        60 443 → 54431 [ACK] Seq=6431 Ack=2576 Win=4194304 Len=0
27120 93.956438 172.217.19.10   192.168.100.14  QUIC      502 Protected Payload (KP0)
27121 93.956438 172.217.19.10   192.168.100.14  QUIC      265 Protected Payload (KP0)
27122 93.956438 172.217.19.206  192.168.100.14  UDP        65 443 → 60027 Len=23
27123 93.956438 20.189.173.1    192.168.100.14  TLSv1.3   157 Application Data
27124 93.956438 20.189.173.1    192.168.100.14  TLSv1.3   116 Application Data
27125 93.956438 23.32.29.106    192.168.100.14  QUIC       67 Protected Payload (KP0)
27126 93.956438 23.32.29.106    192.168.100.14  QUIC       64 Protected Payload (KP0)
27127 93.956628 192.168.100.14  20.189.173.1    TCP        54 54432 → 443 [ACK] Seq=2459 Ack=6596 Win=66048 Len=0
27128 93.956995 192.168.100.14  23.32.29.106    QUIC       76 Protected Payload (KP0), DCID=0d58089e0cc0360b
27129 93.983478 20.189.173.1    192.168.100.14  TLSv1.3   688 Application Data, Application Data
27130 93.983478 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=7230 Ack=21497 Win=4194816 Len=0
27131 93.983478 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=7230 Ack=22909 Win=4194816 Len=0
27132 93.983478 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=7230 Ack=24321 Win=4194816 Len=0
27133 93.983478 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=7230 Ack=25733 Win=4194816 Len=0
27134 93.983478 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=7230 Ack=27145 Win=4194816 Len=0
27135 93.983478 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=7230 Ack=28557 Win=4194816 Len=0
27136 93.983478 20.189.173.1    192.168.100.14  TCP        60 443 → 54426 [ACK] Seq=7230 Ack=30502 Win=4194816 Len=0
27137 93.983478 20.189.173.1    192.168.100.14  TLSv1.3   233 Application Data
27138 93.983608 192.168.100.14  20.189.173.1    TCP        54 54426 → 443 [ACK] Seq=30533 Ack=7409 Win=65280 Len=0
27139 93.986467 192.168.100.14  20.189.173.1    TCP      1466 54426 → 443 [ACK] Seq=30533 Ack=7409 Win=65280 Len=1412 [TCP segment of a reassembled PDU]

0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   · ·m$···dV·_··E·

Payload (udp.payload), 194 bytes      Packets: 55576 · Displayed: 55576 (100.0%) · Dropped: 0 (0.0%)      Profile: Default
```



```
No.    Time      Source           Destination      Protocol Length Info
 27186 94.079137 192.168.100.14   172.217.19.3     QUIC       76 Protected Payload (KP0), DCID=e417aa8a1584ade2
 27187 94.079316 192.168.100.14   23.32.29.104     TCP      1466 54429 → 443 [ACK] Seq=26798 Ack=21612 Win=65280 Len=1412 [TCP segment of a reassembled PDU]
 27188 94.079316 192.168.100.14   23.32.29.104     TCP      1466 54429 → 443 [ACK] Seq=28210 Ack=21612 Win=65280 Len=1412 [TCP segment of a reassembled PDU]
 27189 94.079316 192.168.100.14   23.32.29.104     TLSv1.3  1313 Application Data
 27190 94.102718 172.217.19.10    192.168.100.14   QUIC       66 Protected Payload (KP0)
 27191 94.182219 23.32.29.104     192.168.100.14   TCP        60 443 → 54429 [ACK] Seq=21612 Ack=29622 Win=64128 Len=0
 27192 94.196181 172.217.19.3     192.168.100.14   QUIC      948 Protected Payload (KP0)
 27193 94.199583 172.217.19.3     192.168.100.14   QUIC       63 Protected Payload (KP0)
 27194 94.213013 192.168.100.14   172.217.19.3     QUIC       79 Protected Payload (KP0), DCID=e417aa8a1584ade2
 27195 94.213197 192.168.100.14   172.217.19.3     QUIC       75 Protected Payload (KP0), DCID=e417aa8a1584ade2
 27196 94.214683 192.168.100.14   192.168.100.1    DNS        78 Standard query 0x26e0 A e2c70.gcp.gvt2.com
 27197 94.215521 192.168.100.14   192.168.100.1    DNS        78 Standard query 0x42a9 HTTPS e2c70.gcp.gvt2.com
 27198 94.222776 23.32.29.104     192.168.100.14   TCP        60 443 → 54429 [ACK] Seq=21612 Ack=30881 Win=64128 Len=0
 27199 94.228710 192.168.100.1    192.168.100.14   DNS        94 Standard query response 0x26e0 A e2c70.gcp.gvt2.com A 34.0.63.29
 27200 94.233331 192.168.100.14   192.168.100.1    DNS        87 Standard query 0xdc19 A img-s-msn-com.akamaized.net
 27201 94.233740 192.168.100.14   192.168.100.1    DNS        87 Standard query 0x65ae HTTPS img-s-msn-com.akamaized.net
 27202 94.235083 192.168.100.14   23.32.29.106     QUIC      236 Protected Payload (KP0), DCID=0d58089e0cc0360b
 27203 94.236515 192.168.100.14   23.32.29.104     TCP      1466 54429 → 443 [ACK] Seq=30881 Ack=21612 Win=65280 Len=1412 [TCP segment of a reassembled PDU]
 27204 94.236515 192.168.100.14   23.32.29.104     TCP      1466 54429 → 443 [ACK] Seq=32293 Ack=21612 Win=65280 Len=1412 [TCP segment of a reassembled PDU]
 27205 94.236515 192.168.100.14   23.32.29.104     TLSv1.3  1213 Application Data
 27206 94.243458 192.168.100.14   34.0.63.29       TCP        66 54434 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 27207 94.247390 192.168.100.1    192.168.100.14   DNS       152 Standard query response 0xdc19 A img-s-msn-com.akamaized.net CNAME a1834.dscg2.akamai.net A 59.103.129.75 A 59.103.129.81
 27208 94.256166 192.168.100.14   59.103.129.75    TCP        66 54435 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 27209 94.261510 59.103.129.75    192.168.100.14   TCP        66 443 → 54435 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1412 SACK_PERM WS=128
 27210 94.261642 192.168.100.14   59.103.129.75    TCP        54 54435 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=0
 27211 94.262687 192.168.100.14   59.103.129.75    TCP      1466 54435 → 443 [ACK] Seq=1 Ack=1 Win=66304 Len=1412 [TCP segment of a reassembled PDU]
 27212 94.262687 192.168.100.14   59.103.129.75    TLSv1.3   730 Client Hello (SNI=img-s-msn-com.akamaized.net)
 27213 94.279177 59.103.129.75    192.168.100.14   TCP        54 443 → 54435 [ACK] Seq=1 Ack=2089 Win=63360 Len=0
 27214 94.279177 59.103.129.75    192.168.100.14   TLSv1.3   318 Server Hello, Change Cipher Spec, Application Data, Application Data
 27215 94.279177 172.217.19.3     192.168.100.14   QUIC       66 Protected Payload (KP0)
 27216 94.279177 23.32.29.104     192.168.100.14   TCP      1466 443 → 54429 [ACK] Seq=21612 Ack=30881 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
 27217 94.279177 23.32.29.104     192.168.100.14   TLSv1.3  1107 Application Data
 27218 94.279360 192.168.100.14   23.32.29.104     TCP        54 54429 → 443 [ACK] Seq=34864 Ack=24077 Win=66304 Len=0
 27219 94.279815 192.168.100.14   59.103.129.75    TLSv1.3   134 Change Cipher Spec, Application Data
 27220 94.280628 192.168.100.14   59.103.129.75    TLSv1.3   146 Application Data
 27221 94.280877 192.168.100.14   59.103.129.75    TLSv1.3   553 Application Data
 27222 94.282348 23.32.29.104     192.168.100.14   TLSv1.3   352 Application Data
 27223 94.288342 59.103.129.75    192.168.100.14   TCP        60 443 → 54435 [ACK] Seq=265 Ack=2169 Win=64128 Len=0
 27224 94.288342 59.103.129.75    192.168.100.14   TLSv1.3   341 Application Data
 27225 94.288342 59.103.129.75    192.168.100.14   TCP        60 443 → 54435 [ACK] Seq=552 Ack=2261 Win=64128 Len=0
 27226 94.288342 59.103.129.75    192.168.100.14   TLSv1.3   115 Application Data
 27227 94.288342 59.103.129.75    192.168.100.14   TLSv1.3    85 Application Data
 27228 94.288342 59.103.129.75    192.168.100.14   TCP        60 443 → 54435 [ACK] Seq=644 Ack=2760 Win=64128 Len=0
```

```
0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   · ·m$· · dV·_· ·E·
Payload (udp.payload), 194 bytes
Packets: 55576 · Displayed: 55576 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
```



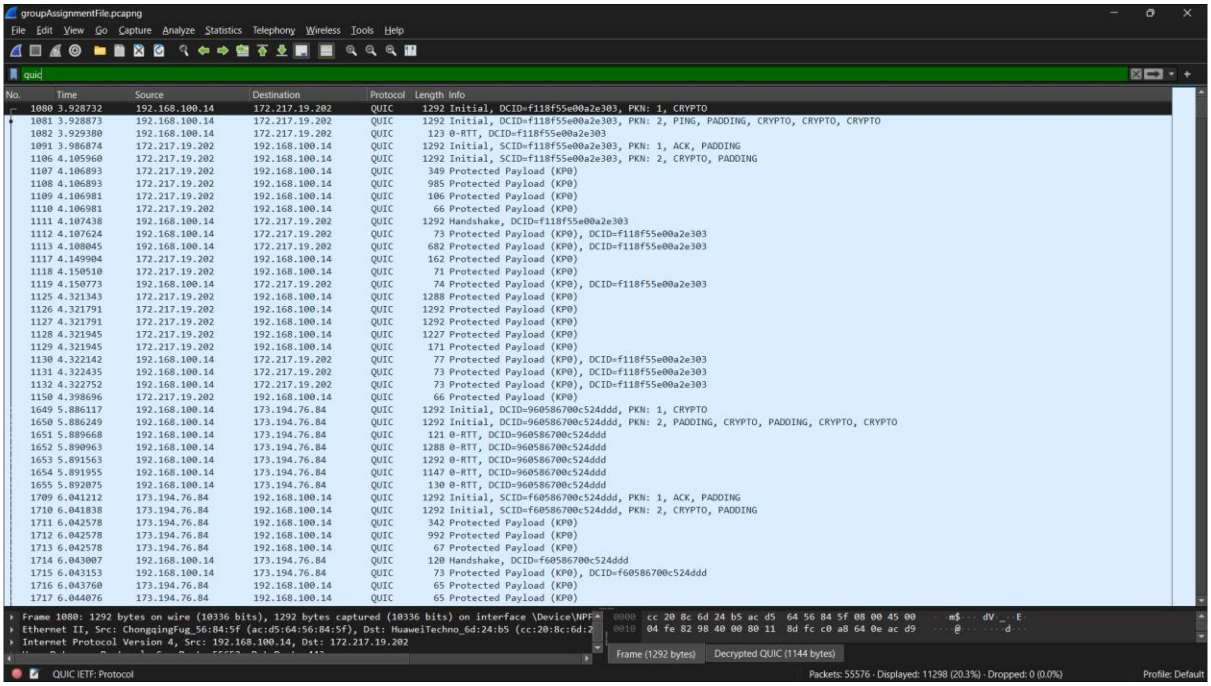
```
No.    Time      Source           Destination      Protocol Length Info
 27366 94.625518 23.32.29.104     192.168.100.14   TCP      1466 443 → 54430 [ACK] Seq=39111 Ack=4187 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
 27367 94.625518 23.32.29.104     192.168.100.14   TCP      1466 443 → 54430 [PSH, ACK] Seq=40523 Ack=4187 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
 27368 94.625612 192.168.100.14   23.32.29.104     TCP        54 54430 → 443 [ACK] Seq=4187 Ack=41935 Win=66304 Len=0
 27369 94.629077 23.32.29.104     192.168.100.14   TCP      1466 443 → 54430 [ACK] Seq=41935 Ack=4187 Win=64128 Len=1412 [TCP segment of a reassembled PDU]
 27370 94.635717 23.32.29.104     192.168.100.14   TLSv1.3   370 Application Data
 27371 94.635784 192.168.100.14   23.32.29.104     TCP        54 54430 → 443 [ACK] Seq=4187 Ack=43663 Win=66304 Len=0
 27372 94.673269 192.168.100.14   192.168.100.1    DNS        72 Standard query 0xb10d A www.bing.com
 27373 94.673642 192.168.100.14   192.168.100.1    DNS        72 Standard query 0x247c HTTPS www.bing.com
 27374 94.689036 192.168.100.1    192.168.100.14   DNS       243 Standard query response 0xb10d A www.bing.com CNAME wwwprod.www-bing-com.akadns.net CNAME www.bing.com.edgekey.net CNAME e86303…
 27375 94.696008 192.168.100.14   23.32.29.90      QUIC     1292 Initial, DCID=59793c259e5c99f8, PKN: 1, CRYPTO
 27376 94.696151 192.168.100.14   23.32.29.90      QUIC     1292 Initial, DCID=59793c259e5c99f8, PKN: 2, PING, PADDING, PING, CRYPTO, CRYPTO, PADDING, CRYPTO, PADDING, CRYPTO, PING, CRYPTO, CR…
 27377 94.710395 52.111.252.18    192.168.100.14   TCP        60 443 → 54436 [ACK] Seq=5926 Ack=2055 Win=524800 Len=0
 27378 94.710395 52.111.252.18    192.168.100.14   TCP        60 443 → 54436 [ACK] Seq=5926 Ack=2672 Win=524288 Len=0
 27379 94.710395 52.111.252.18    192.168.100.14   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
 27380 94.710395 52.111.252.18    192.168.100.14   TLSv1.2   123 Application Data
 27381 94.710395 52.111.252.18    192.168.100.14   TLSv1.2   134 Application Data, Application Data
 27382 94.710395 52.111.252.18    192.168.100.14   TCP      1466 443 → 54436 [ACK] Seq=6126 Ack=2672 Win=524288 Len=1412 [TCP segment of a reassembled PDU]
 27383 94.710395 52.111.252.18    192.168.100.14   TCP      1466 443 → 54436 [ACK] Seq=7538 Ack=2672 Win=524288 Len=1412 [TCP segment of a reassembled PDU]
 27384 94.710395 52.111.252.18    192.168.100.14   TCP      1466 443 → 54436 [ACK] Seq=8950 Ack=2672 Win=524288 Len=1412 [TCP segment of a reassembled PDU]
 27385 94.710395 52.111.252.18    192.168.100.14   TCP      1466 443 → 54436 [ACK] Seq=10362 Ack=2672 Win=524288 Len=1412 [TCP segment of a reassembled PDU]
 27386 94.710395 52.111.252.18    192.168.100.14   TCP      1466 443 → 54436 [ACK] Seq=11774 Ack=2672 Win=524288 Len=1412 [TCP segment of a reassembled PDU]
 27387 94.710395 52.111.252.18    192.168.100.14   TLSv1.2   642 Application Data
 27388 94.710395 52.111.252.18    192.168.100.14   TLSv1.2    92 Application Data
 27389 94.710578 192.168.100.14   52.111.252.18    TCP        54 54436 → 443 [ACK] Seq=2672 Ack=13812 Win=66304 Len=0
 27390 94.711602 192.168.100.14   52.111.252.18    TLSv1.2    92 Application Data
 27391 94.795625 192.168.100.14   20.189.173.1     TCP      1466 54426 → 443 [ACK] Seq=85153 Ack=7637 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
 27392 94.795625 192.168.100.14   20.189.173.1     TCP      1466 54426 → 443 [ACK] Seq=86565 Ack=7637 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
 27393 94.795625 192.168.100.14   20.189.173.1     TLSv1.3  1433 Application Data
 27394 94.795843 192.168.100.14   20.189.173.1     TCP      1466 54426 → 443 [ACK] Seq=89356 Ack=7637 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
 27395 94.795843 192.168.100.14   20.189.173.1     TCP      1466 54426 → 443 [ACK] Seq=90768 Ack=7637 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
 27396 94.795843 192.168.100.14   20.189.173.1     TCP      1466 54426 → 443 [ACK] Seq=92180 Ack=7637 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
 27397 94.795843 192.168.100.14   20.189.173.1     TCP      1466 54426 → 443 [ACK] Seq=93592 Ack=7637 Win=65024 Len=1412 [TCP segment of a reassembled PDU]
 27398 94.795843 192.168.100.14   20.189.173.1     TLSv1.3  1128 Application Data
 27399 94.796722 192.168.100.14   23.32.29.106     QUIC      205 Protected Payload (KP0), DCID=0d58089e0cc0360b
 27400 94.800521 23.32.29.90      192.168.100.14   QUIC     1292 Initial, SCID=35b27d5996c1360b, PKN: 1, ACK, PADDING
 27401 94.800521 23.32.29.90      192.168.100.14   QUIC     1292 Initial, SCID=35b27d5996c1360b, PKN: 2, CRYPTO, PADDING
 27402 94.800521 23.32.29.90      192.168.100.14   QUIC      290 Handshake, SCID=35b27d5996c1360b
 27403 94.803874 192.168.100.14   23.32.29.90      QUIC     1292 Handshake, DCID=35b27d5996c1360b
 27404 94.804449 192.168.100.14   23.32.29.90      QUIC      203 Protected Payload (KP0), DCID=35b27d5996c1360b
 27405 94.805845 192.168.100.14   23.32.29.90      QUIC     1292 Protected Payload (KP0), DCID=35b27d5996c1360b
 27406 94.805965 192.168.100.14   23.32.29.90      QUIC     1059 Protected Payload (KP0), DCID=35b27d5996c1360b
 27407 94.810068 20.189.173.1     192.168.100.14   TLSv1.3   366 Application Data
 27408 94.810141 192.168.100.14   20.189.173.1     TCP        54 54426 → 443 [ACK] Seq=96078 Ack=7949 Win=66304 Len=0
```

```
0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   · ·m$· · dV·_· ·E·
Payload (udp.payload), 194 bytes
Packets: 55576 · Displayed: 55576 (100.0%) · Dropped: 0 (0.0%)
Profile: Default
```

Activity 2: Filter Traffic

QUIC, a protocol favored by Google for its speed and security advantages, is extensively utilized in web browsing. To review all captured protocol data in Wireshark, apply the "filetype" filter. This simple step allows a thorough examination of QUIC's influence on network traffic, illustrating its role in enhancing browsing speed and safeguarding online activities. By utilizing the "filetype" filter in Wireshark analysis, one can effectively showcase QUIC's significance in optimizing browsing experiences and ensuring secure internet interactions.

QUIC filter applied:



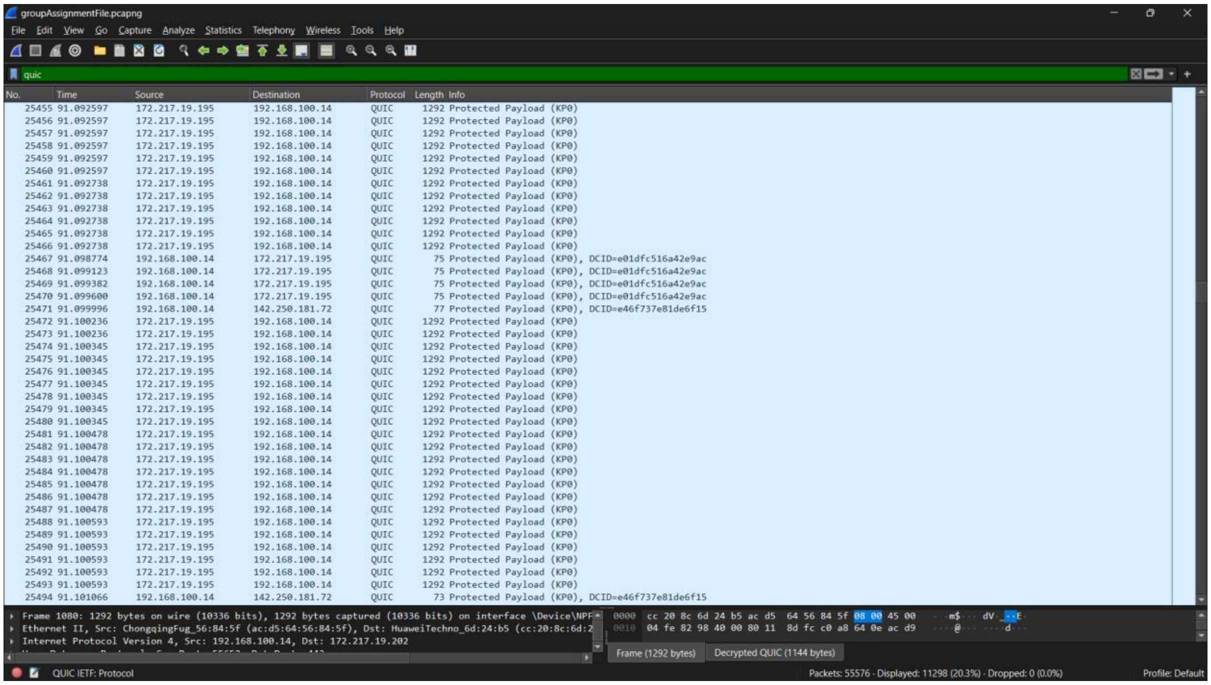
quic

```
No.   Time       Source            Destination       Protocol Length Info
 1080 3.928732   192.168.100.14    172.217.19.202    QUIC     1292 Initial, DCID=f118f55e00a2e303, PKN: 1, CRYPTO
 1081 3.928873   192.168.100.14    172.217.19.202    QUIC     1292 Initial, DCID=f118f55e00a2e303, PKN: 2, PING, PADDING, CRYPTO, CRYPTO, CRYPTO
 1082 3.929380   192.168.100.14    172.217.19.202    QUIC      123 0-RTT, DCID=f118f55e00a2e303
 1091 3.986874   172.217.19.202    192.168.100.14    QUIC     1292 Initial, SCID=f118f55e00a2e303, PKN: 1, ACK, PADDING
 1106 4.105960   172.217.19.202    192.168.100.14    QUIC     1292 Initial, SCID=f118f55e00a2e303, PKN: 2, CRYPTO, PADDING
 1107 4.106893   172.217.19.202    192.168.100.14    QUIC      349 Protected Payload (KP0)
 1108 4.106893   172.217.19.202    192.168.100.14    QUIC      985 Protected Payload (KP0)
 1109 4.106981   172.217.19.202    192.168.100.14    QUIC      106 Protected Payload (KP0)
 1110 4.106981   172.217.19.202    192.168.100.14    QUIC       66 Protected Payload (KP0)
 1111 4.107438   192.168.100.14    172.217.19.202    QUIC     1292 Handshake, DCID=f118f55e00a2e303
 1112 4.107624   192.168.100.14    172.217.19.202    QUIC       73 Protected Payload (KP0), DCID=f118f55e00a2e303
 1113 4.108045   192.168.100.14    172.217.19.202    QUIC      682 Protected Payload (KP0), DCID=f118f55e00a2e303
 1117 4.149904   172.217.19.202    192.168.100.14    QUIC      162 Protected Payload (KP0)
 1118 4.150510   172.217.19.202    192.168.100.14    QUIC       71 Protected Payload (KP0)
 1119 4.150773   192.168.100.14    172.217.19.202    QUIC       74 Protected Payload (KP0), DCID=f118f55e00a2e303
 1125 4.321343   172.217.19.202    192.168.100.14    QUIC     1288 Protected Payload (KP0)
 1126 4.321791   172.217.19.202    192.168.100.14    QUIC     1292 Protected Payload (KP0)
 1127 4.321791   172.217.19.202    192.168.100.14    QUIC     1292 Protected Payload (KP0)
 1128 4.321945   172.217.19.202    192.168.100.14    QUIC     1227 Protected Payload (KP0)
 1129 4.321945   172.217.19.202    192.168.100.14    QUIC      171 Protected Payload (KP0)
 1130 4.322142   192.168.100.14    172.217.19.202    QUIC       77 Protected Payload (KP0), DCID=f118f55e00a2e303
 1131 4.322435   192.168.100.14    172.217.19.202    QUIC       73 Protected Payload (KP0), DCID=f118f55e00a2e303
 1132 4.322752   192.168.100.14    172.217.19.202    QUIC       73 Protected Payload (KP0), DCID=f118f55e00a2e303
 1150 4.398696   172.217.19.202    192.168.100.14    QUIC       66 Protected Payload (KP0)
 1649 5.886117   192.168.100.14    173.194.76.84     QUIC     1292 Initial, DCID=960586700c524ddd, PKN: 1, CRYPTO
 1650 5.886249   192.168.100.14    173.194.76.84     QUIC     1292 Initial, DCID=960586700c524ddd, PKN: 2, PADDING, CRYPTO, PADDING, CRYPTO, CRYPTO
 1651 5.889668   192.168.100.14    173.194.76.84     QUIC      121 0-RTT, DCID=960586700c524ddd
 1652 5.890963   192.168.100.14    173.194.76.84     QUIC     1288 0-RTT, DCID=960586700c524ddd
 1653 5.891563   192.168.100.14    173.194.76.84     QUIC     1292 0-RTT, DCID=960586700c524ddd
 1654 5.891955   192.168.100.14    173.194.76.84     QUIC     1147 0-RTT, DCID=960586700c524ddd
 1655 5.892075   192.168.100.14    173.194.76.84     QUIC      130 0-RTT, DCID=960586700c524ddd
 1709 6.041212   173.194.76.84     192.168.100.14    QUIC     1292 Initial, SCID=f60586700c524ddd, PKN: 1, ACK, PADDING
 1710 6.041838   173.194.76.84     192.168.100.14    QUIC     1292 Initial, SCID=f60586700c524ddd, PKN: 2, CRYPTO, PADDING
 1711 6.042578   173.194.76.84     192.168.100.14    QUIC      342 Protected Payload (KP0)
 1712 6.042578   173.194.76.84     192.168.100.14    QUIC      992 Protected Payload (KP0)
 1713 6.042578   173.194.76.84     192.168.100.14    QUIC       67 Protected Payload (KP0)
 1714 6.043007   192.168.100.14    173.194.76.84     QUIC      120 Handshake, DCID=f60586700c524ddd
 1715 6.043153   192.168.100.14    173.194.76.84     QUIC       73 Protected Payload (KP0), DCID=f60586700c524ddd
 1716 6.043760   173.194.76.84     192.168.100.14    QUIC       65 Protected Payload (KP0)
 1717 6.044076   173.194.76.84     192.168.100.14    QUIC       65 Protected Payload (KP0)
```

```
> Frame 1080: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF
> Ethernet II, Src: ChongqingFug_56:84:5f (ac:d5:64:56:84:5f), Dst: HuaweiTechno_6d:24:b5 (cc:20:8c:6d:2
> Internet Protocol Version 4, Src: 192.168.100.14, Dst: 172.217.19.202
```

```
0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   ···m$··· dV·_··E·
0010  04 fe 82 98 40 00 80 11  8d fc c0 a8 64 0e ac d9   ····@··· ····d···
```

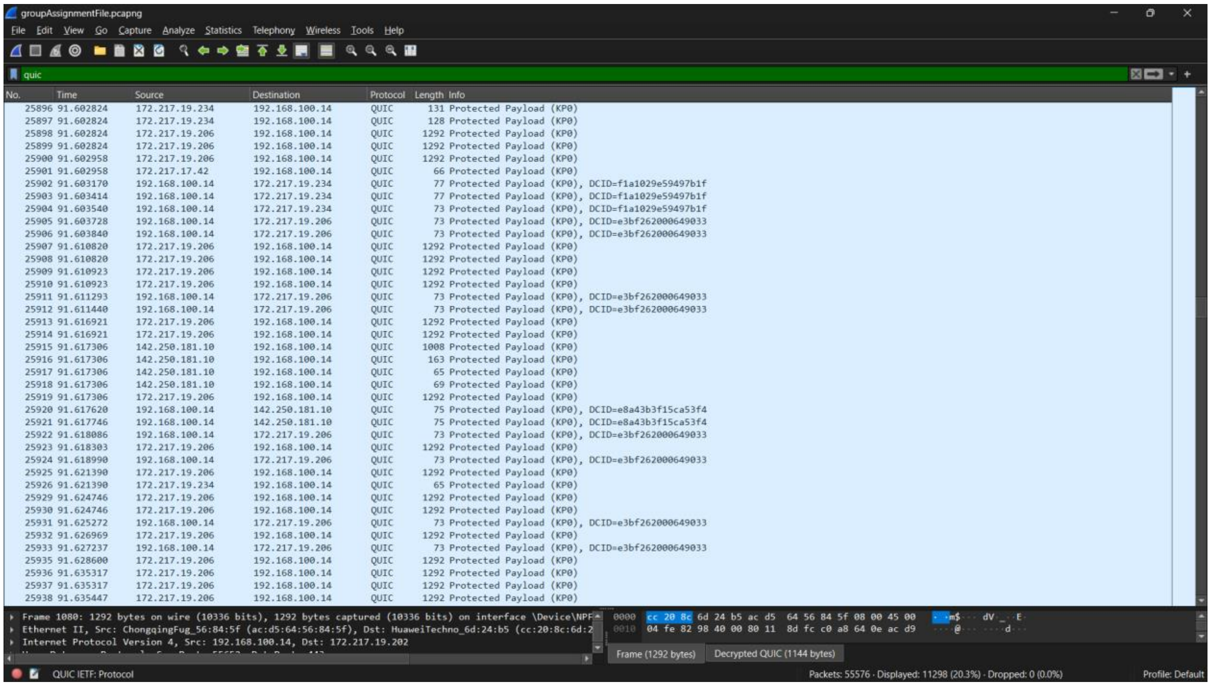
Packets: 55576 · Displayed: 11298 (20.3%) · Dropped: 0 (0.0%)


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

```
No.   Time      Source          Destination     Protocol Length Info
25455 91.092597 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25456 91.092597 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25457 91.092597 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25458 91.092597 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25459 91.092597 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25460 91.092597 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25461 91.092738 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25462 91.092738 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25463 91.092738 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25464 91.092738 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25465 91.092738 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25466 91.092738 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25467 91.098774 192.168.100.14  172.217.19.195  QUIC       75 Protected Payload (KP0), DCID=e01dfc516a42e9ac
25468 91.099123 192.168.100.14  172.217.19.195  QUIC       75 Protected Payload (KP0), DCID=e01dfc516a42e9ac
25469 91.099382 192.168.100.14  172.217.19.195  QUIC       75 Protected Payload (KP0), DCID=e01dfc516a42e9ac
25470 91.099600 192.168.100.14  172.217.19.195  QUIC       75 Protected Payload (KP0), DCID=e01dfc516a42e9ac
25471 91.099996 192.168.100.14  142.250.181.72  QUIC       77 Protected Payload (KP0), DCID=e46f737e81de6f15
25472 91.100236 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25473 91.100236 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25474 91.100345 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25475 91.100345 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25476 91.100345 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25477 91.100345 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25478 91.100345 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25479 91.100345 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25480 91.100345 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25481 91.100478 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25482 91.100478 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25483 91.100478 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25484 91.100478 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25485 91.100478 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25486 91.100478 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25487 91.100478 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25488 91.100593 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25489 91.100593 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25490 91.100593 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25491 91.100593 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25492 91.100593 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25493 91.100593 172.217.19.195  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25494 91.101066 192.168.100.14  142.250.181.72  QUIC       73 Protected Payload (KP0), DCID=e46f737e81de6f15
```

```
> Frame 1080: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF
> Ethernet II, Src: ChongqingFug_56:84:5f (ac:d5:64:56:84:5f), Dst: HuaweiTechno_6d:24:b5 (cc:20:8c:6d:2
> Internet Protocol Version 4, Src: 192.168.100.14, Dst: 172.217.19.202

0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   ···m$···dV·_··E·
0010  04 fe 82 98 40 00 80 11  8d fc c0 a8 64 0e ac d9   ····@·······d···
```

Frame (1292 bytes)
Decrypted QUIC (1144 bytes)
QUIC IETF: Protocol
Packets: 55576 · Displayed: 11298 (20.3%) · Dropped: 0 (0.0%)
Profile: Default


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

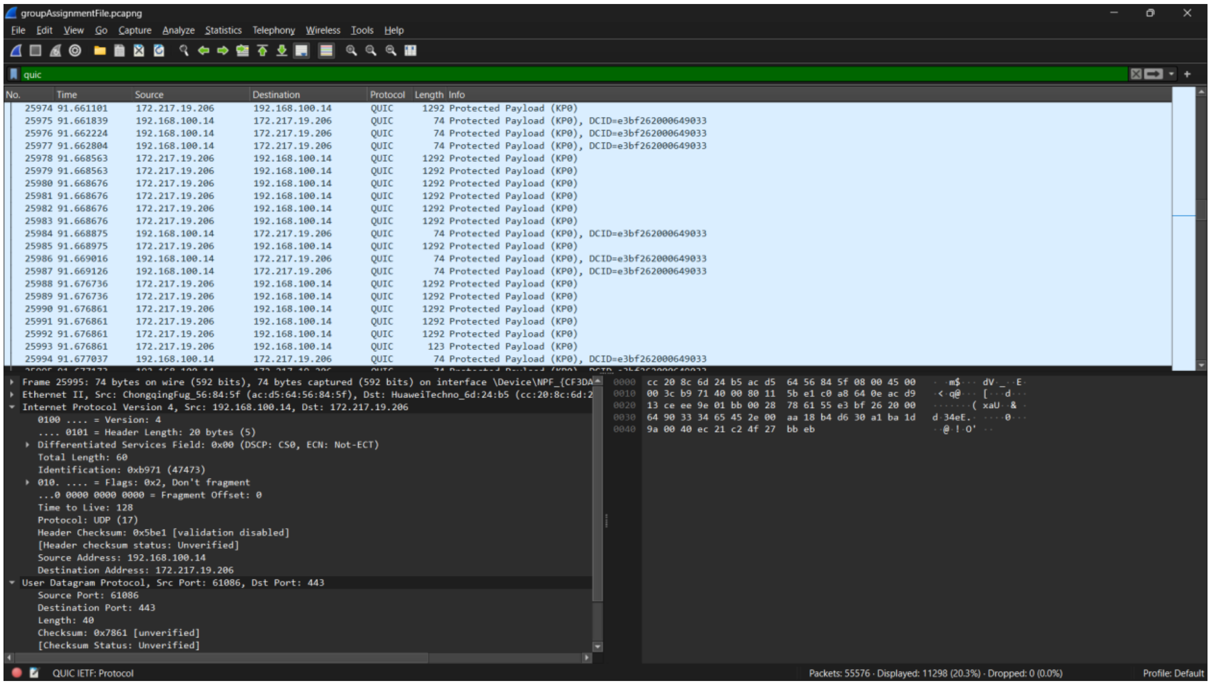
```
No.   Time      Source          Destination     Protocol Length Info
25896 91.602824 172.217.19.234  192.168.100.14  QUIC      131 Protected Payload (KP0)
25897 91.602824 172.217.19.234  192.168.100.14  QUIC      128 Protected Payload (KP0)
25898 91.602824 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25899 91.602824 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25900 91.602958 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25901 91.602958 172.217.17.42   192.168.100.14  QUIC       66 Protected Payload (KP0)
25902 91.603170 192.168.100.14  172.217.19.234  QUIC       77 Protected Payload (KP0), DCID=f1a1029e59497b1f
25903 91.603414 192.168.100.14  172.217.19.234  QUIC       77 Protected Payload (KP0), DCID=f1a1029e59497b1f
25904 91.603540 192.168.100.14  172.217.19.234  QUIC       73 Protected Payload (KP0), DCID=f1a1029e59497b1f
25905 91.603728 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25906 91.603840 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25907 91.610820 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25908 91.610820 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25909 91.610923 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25910 91.610923 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25911 91.611293 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25912 91.611440 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25913 91.616921 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25914 91.616921 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25915 91.617306 142.250.181.10  192.168.100.14  QUIC     1008 Protected Payload (KP0)
25916 91.617306 142.250.181.10  192.168.100.14  QUIC      163 Protected Payload (KP0)
25917 91.617306 142.250.181.10  192.168.100.14  QUIC       65 Protected Payload (KP0)
25918 91.617306 142.250.181.10  192.168.100.14  QUIC       69 Protected Payload (KP0)
25919 91.617306 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25920 91.617620 192.168.100.14  142.250.181.10  QUIC       75 Protected Payload (KP0), DCID=e8a43b3f15ca53f4
25921 91.617746 192.168.100.14  142.250.181.10  QUIC       75 Protected Payload (KP0), DCID=e8a43b3f15ca53f4
25922 91.618086 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25923 91.618303 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25924 91.618990 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25925 91.621390 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25926 91.621390 172.217.19.234  192.168.100.14  QUIC       65 Protected Payload (KP0)
25929 91.624746 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25930 91.624746 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25931 91.625272 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25932 91.626969 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25933 91.627237 192.168.100.14  172.217.19.206  QUIC       73 Protected Payload (KP0), DCID=e3bf262000649033
25935 91.628600 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25936 91.635317 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25937 91.635317 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25938 91.635447 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
```

```
> Frame 1080: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interface \Device\NPF
> Ethernet II, Src: ChongqingFug_56:84:5f (ac:d5:64:56:84:5f), Dst: HuaweiTechno_6d:24:b5 (cc:20:8c:6d:2
> Internet Protocol Version 4, Src: 192.168.100.14, Dst: 172.217.19.202

0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   ···m$···dV·_··E·
0010  04 fe 82 98 40 00 80 11  8d fc c0 a8 64 0e ac d9   ····@·······d···
```

Frame (1292 bytes)
Decrypted QUIC (1144 bytes)
QUIC IETF: Protocol
Packets: 55576 · Displayed: 11298 (20.3%) · Dropped: 0 (0.0%)
Profile: Default

Analyzing QUIC:

Analyzing packet length, source, and destination related to QUIC protocol reveals insights into network efficiency and security. Studying these aspects helps understand data transmission patterns, origin, and destination, crucial for optimizing QUIC performance and ensuring secure communication, enhancing overall browsing experiences.


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

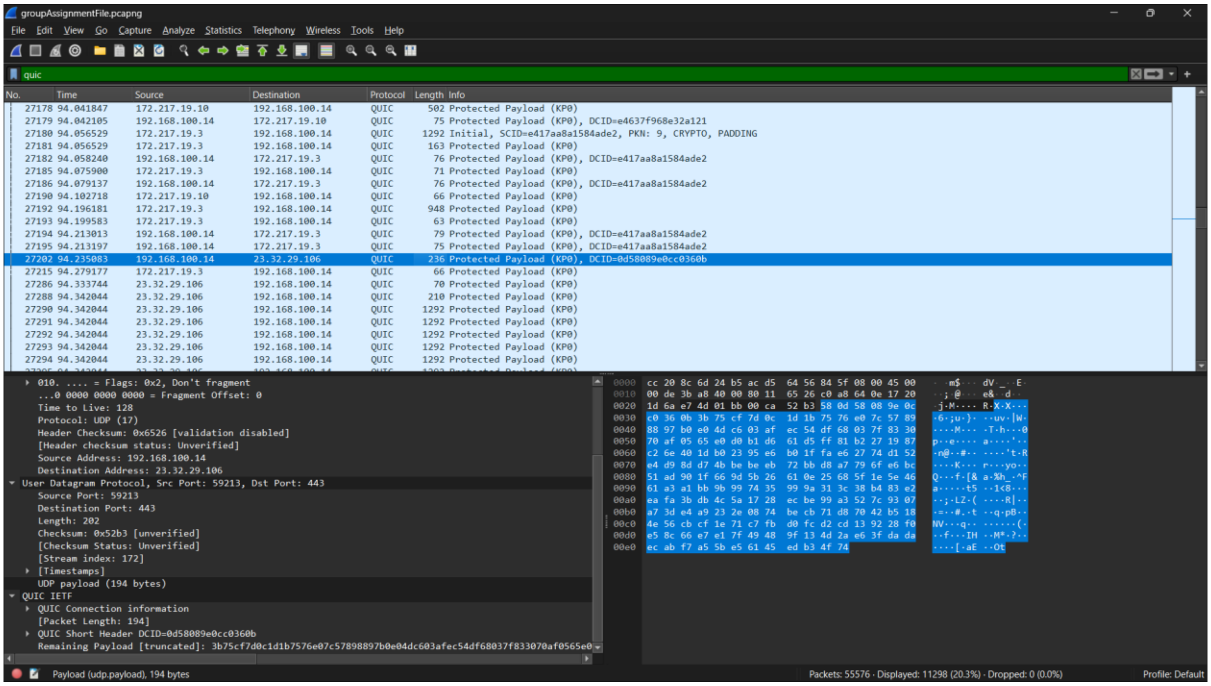
```
No.   Time      Source          Destination     Protocol Length Info
25974 91.661101 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25975 91.661839 192.168.100.14  172.217.19.206  QUIC       74 Protected Payload (KP0), DCID=e3bf262000649033
25976 91.662224 192.168.100.14  172.217.19.206  QUIC       74 Protected Payload (KP0), DCID=e3bf262000649033
25977 91.662804 192.168.100.14  172.217.19.206  QUIC       74 Protected Payload (KP0), DCID=e3bf262000649033
25978 91.668563 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25979 91.668563 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25980 91.668676 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25981 91.668676 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25982 91.668676 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25983 91.668676 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25984 91.668875 192.168.100.14  172.217.19.206  QUIC       74 Protected Payload (KP0), DCID=e3bf262000649033
25985 91.668975 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25986 91.669016 192.168.100.14  172.217.19.206  QUIC       74 Protected Payload (KP0), DCID=e3bf262000649033
25987 91.669126 192.168.100.14  172.217.19.206  QUIC       74 Protected Payload (KP0), DCID=e3bf262000649033
25988 91.676736 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25989 91.676736 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25990 91.676861 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25991 91.676861 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25992 91.676861 172.217.19.206  192.168.100.14  QUIC     1292 Protected Payload (KP0)
25993 91.676861 172.217.19.206  192.168.100.14  QUIC      123 Protected Payload (KP0)
25994 91.677037 192.168.100.14  172.217.19.206  QUIC       74 Protected Payload (KP0), DCID=e3bf262000649033
```

```
> Frame 25995: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CF3DA
> Ethernet II, Src: ChongqingFug_56:84:5f (ac:d5:64:56:84:5f), Dst: HuaweiTechno_6d:24:b5 (cc:20:8c:6d:2
v Internet Protocol Version 4, Src: 192.168.100.14, Dst: 172.217.19.206
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0xb971 (47473)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x5be1 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.100.14
    Destination Address: 172.217.19.206
v User Datagram Protocol, Src Port: 61086, Dst Port: 443
    Source Port: 61086
    Destination Port: 443
    Length: 40
    Checksum: 0x7861 [unverified]
    [Checksum Status: Unverified]
```

```
0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   ···m$··· dV·_··E·
0010  00 3c b9 71 40 00 80 11  5b e1 c0 a8 64 0e ac d9   ·<·q@··· [···d···
0020  13 ce ee 9e 01 bb 00 28  78 61 55 e3 bf 26 20 00   ·······( xaU··& ·
0030  64 90 33 34 65 45 2e 00  aa 18 b4 d6 30 a1 ba 1d   d·34eE.· ····0···
0040  9a 00 40 ec 21 c2 4f 27  bb eb                     ··@·!·O' ··
```

QUIC IETF: Protocol

Packets: 55576 · Displayed: 11298 (20.3%) · Dropped: 0 (0.0%)   Profile: Default


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

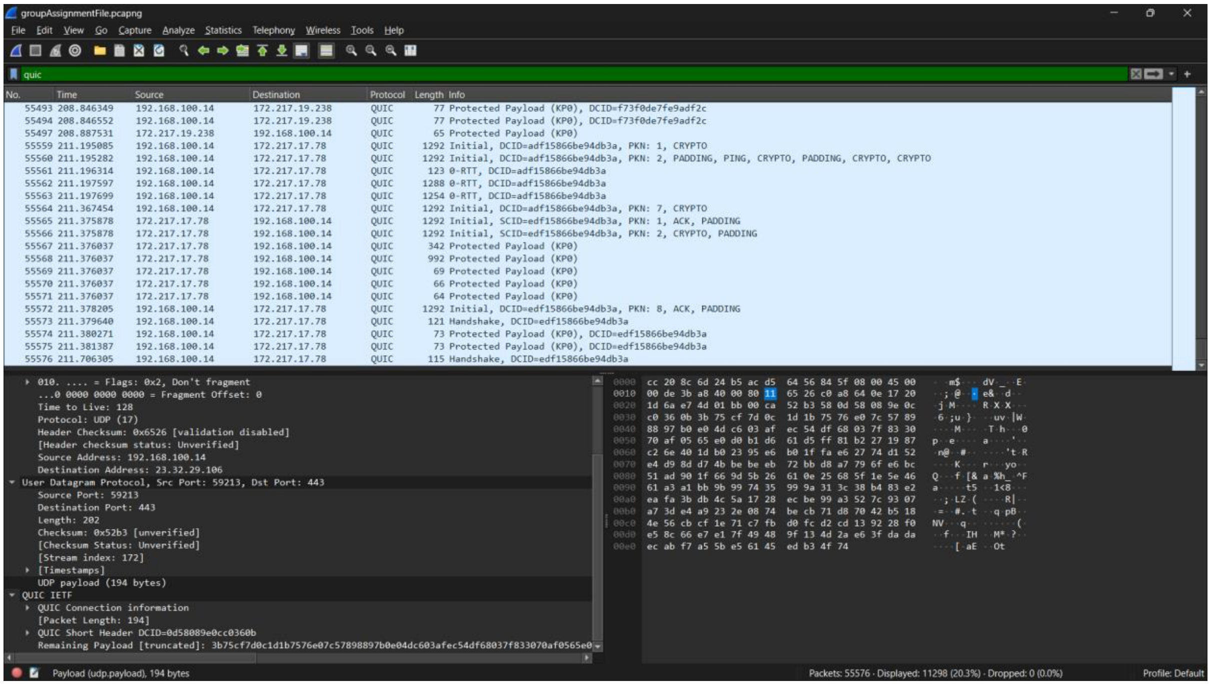
```
No.   Time      Source          Destination     Protocol Length Info
27178 94.041847 172.217.19.10   192.168.100.14  QUIC      502 Protected Payload (KP0)
27179 94.042105 192.168.100.14  172.217.19.10   QUIC       75 Protected Payload (KP0), DCID=e4637f968e32a121
27180 94.056529 172.217.19.3    192.168.100.14  QUIC     1292 Initial, SCID=e417aa8a1584ade2, PKN: 9, CRYPTO, PADDING
27181 94.056529 172.217.19.3    192.168.100.14  QUIC      163 Protected Payload (KP0)
27182 94.058240 192.168.100.14  172.217.19.3    QUIC       76 Protected Payload (KP0), DCID=e417aa8a1584ade2
27185 94.075900 172.217.19.3    192.168.100.14  QUIC       71 Protected Payload (KP0)
27186 94.079137 192.168.100.14  172.217.19.3    QUIC       76 Protected Payload (KP0), DCID=e417aa8a1584ade2
27190 94.102718 172.217.19.10   192.168.100.14  QUIC       66 Protected Payload (KP0)
27192 94.196181 172.217.19.3    192.168.100.14  QUIC      948 Protected Payload (KP0)
27193 94.199583 172.217.19.3    192.168.100.14  QUIC       63 Protected Payload (KP0)
27194 94.213013 192.168.100.14  172.217.19.3    QUIC       79 Protected Payload (KP0), DCID=e417aa8a1584ade2
27195 94.213197 192.168.100.14  172.217.19.3    QUIC       75 Protected Payload (KP0), DCID=e417aa8a1584ade2
27202 94.235083 192.168.100.14  23.32.29.106    QUIC      236 Protected Payload (KP0), DCID=0d58089e0cc0360b
27215 94.279177 172.217.19.3    192.168.100.14  QUIC       66 Protected Payload (KP0)
27286 94.333744 23.32.29.106    192.168.100.14  QUIC       70 Protected Payload (KP0)
27288 94.342044 23.32.29.106    192.168.100.14  QUIC      210 Protected Payload (KP0)
27290 94.342044 23.32.29.106    192.168.100.14  QUIC     1292 Protected Payload (KP0)
27291 94.342044 23.32.29.106    192.168.100.14  QUIC     1292 Protected Payload (KP0)
27292 94.342044 23.32.29.106    192.168.100.14  QUIC     1292 Protected Payload (KP0)
27293 94.342044 23.32.29.106    192.168.100.14  QUIC     1292 Protected Payload (KP0)
27294 94.342044 23.32.29.106    192.168.100.14  QUIC     1292 Protected Payload (KP0)
```

```
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x6526 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.100.14
    Destination Address: 23.32.29.106
v User Datagram Protocol, Src Port: 59213, Dst Port: 443
    Source Port: 59213
    Destination Port: 443
    Length: 202
    Checksum: 0x52b3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 172]
  > [Timestamps]
    UDP payload (194 bytes)
v QUIC IETF
  > QUIC Connection information
    [Packet Length: 194]
  > QUIC Short Header DCID=0d58089e0cc0360b
    Remaining Payload [truncated]: 3b75cf7d0c1d1b7576e07c57898897b0e04dc603afec54df68037f833070af0565e0
```

```
0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   ···m$··· dV·_··E·
0010  00 de 3b a8 40 00 80 11  65 26 c0 a8 64 0e 17 20   ··;·@··· e&··d··
0020  1d 6a e7 4d 01 bb 00 ca  52 b3 58 0d 58 08 9e 0c   ·j·M···· R·X·X···
0030  c0 36 0b 3b 75 cf 7d 0c  1d 1b 75 76 e0 7c 57 89   ·6·;u·}· ··uv·|W·
0040  88 97 b0 e0 4d c6 03 af  ec 54 df 68 03 7f 83 30   ····M··· ·T·h···0
0050  70 af 05 65 e0 d0 b1 d6  61 d5 ff 81 b2 27 19 87   p··e···· a····'··
0060  c2 6e 40 1d b0 23 95 e6  b0 1f fa e6 27 74 d1 52   ·n@··#·· ····'t·R
0070  e4 d9 8d d7 4b be be eb  72 bb d8 a7 79 6f e6 bc   ····K··· r···yo··
0080  51 ad 90 1f 66 9d 5b 26  61 0e 25 68 5f 1e 5e 46   Q···f·[& a·%h_·^F
0090  61 a3 a1 bb 9b 99 74 35  99 9a 31 3c 38 b4 83 e2   a·····t5 ··1<8···
00a0  ea fa 3b db 4c 5a 17 28  ec be 99 a3 52 7c 93 07   ··;·LZ·( ····R|··
00b0  a7 3d e4 a9 23 2e 08 74  be cb 71 d8 70 42 b5 18   ·=··#.·t ··q·pB··
00c0  4e 56 cb cf 1e 71 c7 fb  d0 fc d2 cd 13 92 28 f0   NV···q·· ······(·
00d0  e5 8c 66 e7 e1 7f 49 48  9f 13 4d 2a e6 3f da da   ··f···IH ··M*·?··
00e0  ec ab f7 a5 5b e5 61 45  ed b3 4f 74               ····[·aE ··Ot
```

Payload (udp.payload), 194 bytes

Packets: 55576 · Displayed: 11298 (20.3%) · Dropped: 0 (0.0%)   Profile: Default



groupAssignmentFile.pcapng

quic

```
No.   Time       Source          Destination     Protocol Length Info
55493 208.846349 192.168.100.14  172.217.19.238  QUIC       77 Protected Payload (KP0), DCID=f73f0de7fe9adf2c
55494 208.846552 192.168.100.14  172.217.19.238  QUIC       77 Protected Payload (KP0), DCID=f73f0de7fe9adf2c
55497 208.887531 172.217.19.238  192.168.100.14  QUIC       65 Protected Payload (KP0)
55559 211.195085 192.168.100.14  172.217.17.78   QUIC     1292 Initial, DCID=adf15866be94db3a, PKN: 1, CRYPTO
55560 211.195282 192.168.100.14  172.217.17.78   QUIC     1292 Initial, DCID=adf15866be94db3a, PKN: 2, PADDING, PING, CRYPTO, PADDING, CRYPTO, CRYPTO
55561 211.196314 192.168.100.14  172.217.17.78   QUIC      123 0-RTT, DCID=adf15866be94db3a
55562 211.197597 192.168.100.14  172.217.17.78   QUIC     1288 0-RTT, DCID=adf15866be94db3a
55563 211.197699 192.168.100.14  172.217.17.78   QUIC     1254 0-RTT, DCID=adf15866be94db3a
55564 211.367454 192.168.100.14  172.217.17.78   QUIC     1292 Initial, DCID=adf15866be94db3a, PKN: 7, CRYPTO
55565 211.375878 172.217.17.78   192.168.100.14  QUIC     1292 Initial, SCID=edf15866be94db3a, PKN: 1, ACK, PADDING
55566 211.375878 172.217.17.78   192.168.100.14  QUIC     1292 Initial, SCID=edf15866be94db3a, PKN: 2, CRYPTO, PADDING
55567 211.376037 172.217.17.78   192.168.100.14  QUIC      342 Protected Payload (KP0)
55568 211.376037 172.217.17.78   192.168.100.14  QUIC      992 Protected Payload (KP0)
55569 211.376037 172.217.17.78   192.168.100.14  QUIC       69 Protected Payload (KP0)
55570 211.376037 172.217.17.78   192.168.100.14  QUIC       66 Protected Payload (KP0)
55571 211.376037 172.217.17.78   192.168.100.14  QUIC       64 Protected Payload (KP0)
55572 211.378205 192.168.100.14  172.217.17.78   QUIC     1292 Initial, DCID=edf15866be94db3a, PKN: 8, ACK, PADDING
55573 211.379640 192.168.100.14  172.217.17.78   QUIC      121 Handshake, DCID=edf15866be94db3a
55574 211.380271 192.168.100.14  172.217.17.78   QUIC       73 Protected Payload (KP0), DCID=edf15866be94db3a
55575 211.381387 192.168.100.14  172.217.17.78   QUIC       73 Protected Payload (KP0), DCID=edf15866be94db3a
55576 211.706305 192.168.100.14  172.217.17.78   QUIC      115 Handshake, DCID=edf15866be94db3a
```

```
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x6526 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.100.14
    Destination Address: 23.32.29.106
v User Datagram Protocol, Src Port: 59213, Dst Port: 443
    Source Port: 59213
    Destination Port: 443
    Length: 202
    Checksum: 0x52b3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 172]
  > [Timestamps]
    UDP payload (194 bytes)
v QUIC IETF
  > QUIC Connection information
    [Packet Length: 194]
  > QUIC Short Header DCID=0d58089e0cc0360b
    Remaining Payload [truncated]: 3b75cf7d0c1d1b7576e07c57898897b0e04dc603afec54df68037f833070af0565e0
```

```
0000  cc 20 8c 6d 24 b5 ac d5  64 56 84 5f 08 00 45 00   · ·m$···dV·_··E·
0010  00 de 3b a8 40 00 80 11  65 26 c0 a8 64 0e 17 20   ··;·@···e&··d··
0020  1d 6a e7 4d 01 bb 00 ca  52 b3 58 0d 58 08 9e 0c   ·j·M····R·X·X···
0030  c0 36 0b 3b 75 cf 7d 0c  1d 1b 75 76 e0 7c 57 89   ·6·;u·}···uv·|W·
0040  88 97 b0 e0 4d c6 03 af  ec 54 df 68 03 7f 83 30   ····M····T·h···0
0050  70 af 05 65 e0 d0 b1 d6  61 d5 ff 81 b2 27 19 87   p··e····a····'··
0060  c2 6e 40 1d b0 23 95 e6  b0 1f fa e6 27 74 d1 52   ·n@··#······'t·R
0070  e4 d9 8d d7 4b be be eb  72 bb d8 a7 79 6f e6 bc   ····K···r···yo··
0080  51 ad 90 1f 66 9d 5b 26  61 0e 25 68 5f 1e 5e 46   Q···f·[&a·%h_·^F
0090  61 a3 a1 bb 9b 99 74 35  99 9a 31 3c 38 b4 83 e2   a·····t5··1<8···
00a0  ea fa 3b db 4c 5a 17 28  ec be 99 a3 52 7c 93 07   ··;·LZ·(····R|··
00b0  a7 3d e4 a9 23 2e 08 74  be cb 71 d8 70 42 b5 18   ·=··#.·t··q·pB··
00c0  4e 56 cb cf 1e 71 c7 fb  d0 fc d2 cd 13 92 28 f0   NV···q········(·
00d0  e5 8c 66 e7 e1 7f 49 48  9f 13 4d 2a e6 3f da da   ··f···IH··M*·?··
00e0  ec ab f7 a5 5b e5 61 45  ed b3 4f 74               ····[·aE··Ot
```

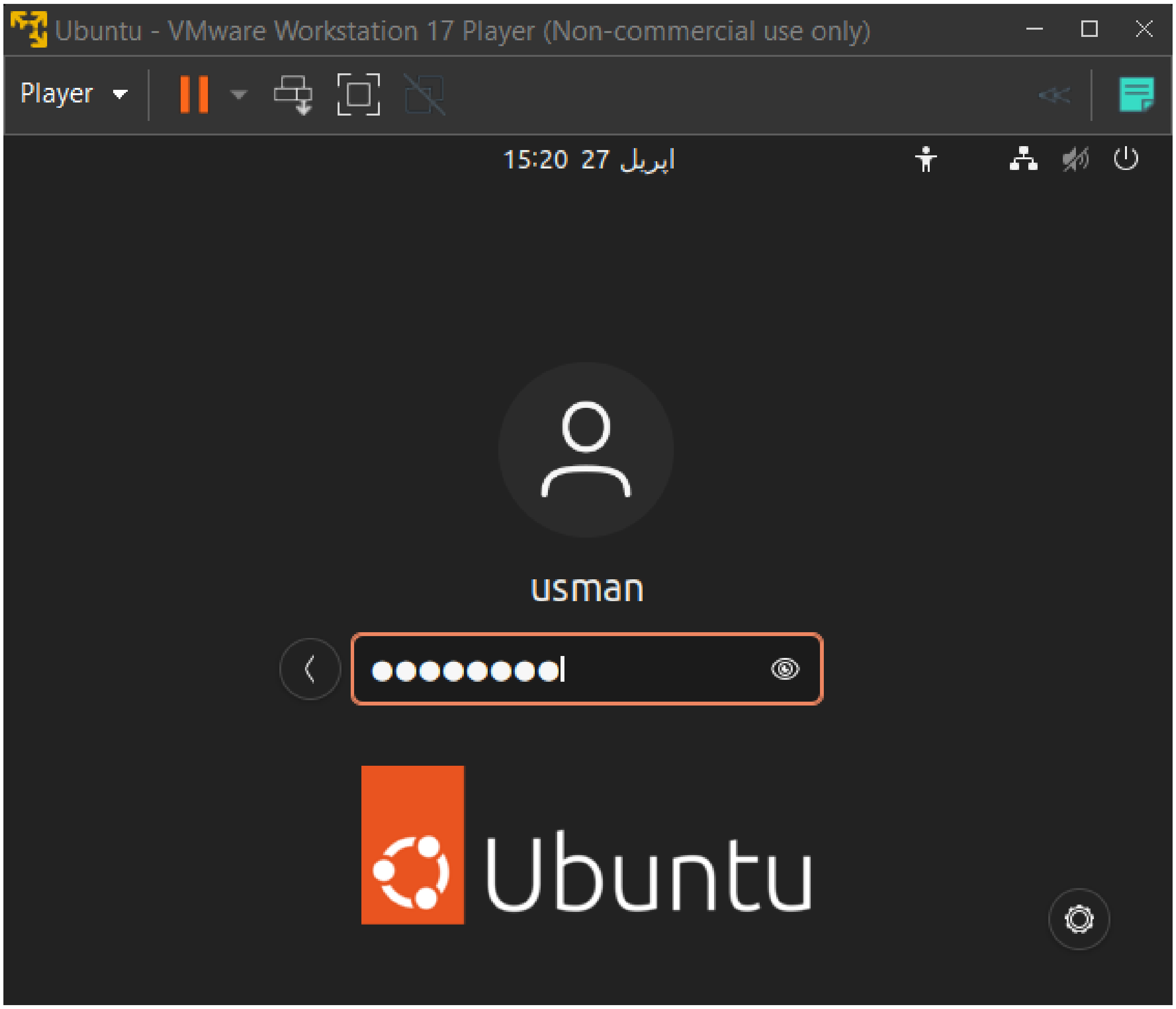
Payload (udp.payload), 194 bytes

Packets: 55576 · Displayed: 11298 (20.3%) · Dropped: 0 (0.0%)

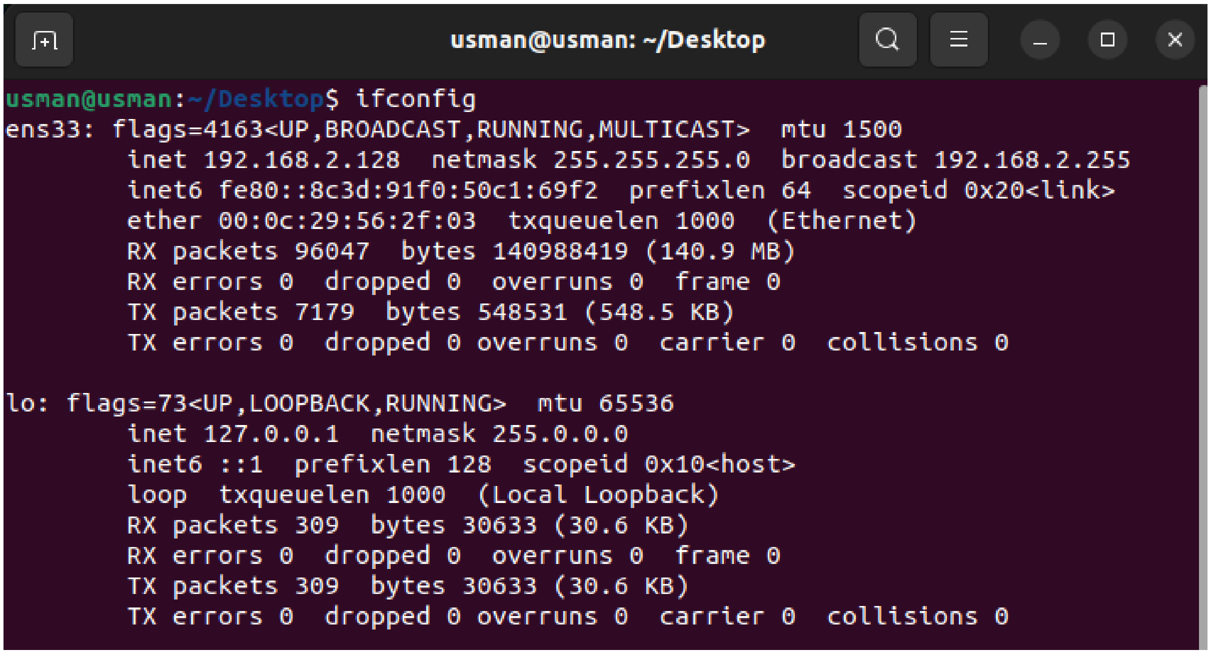
Profile: Default

Activity 3: Ethical Hacking ARP Poisoning

Step 1-2: Install Linux Based System On VMware And Sign-In

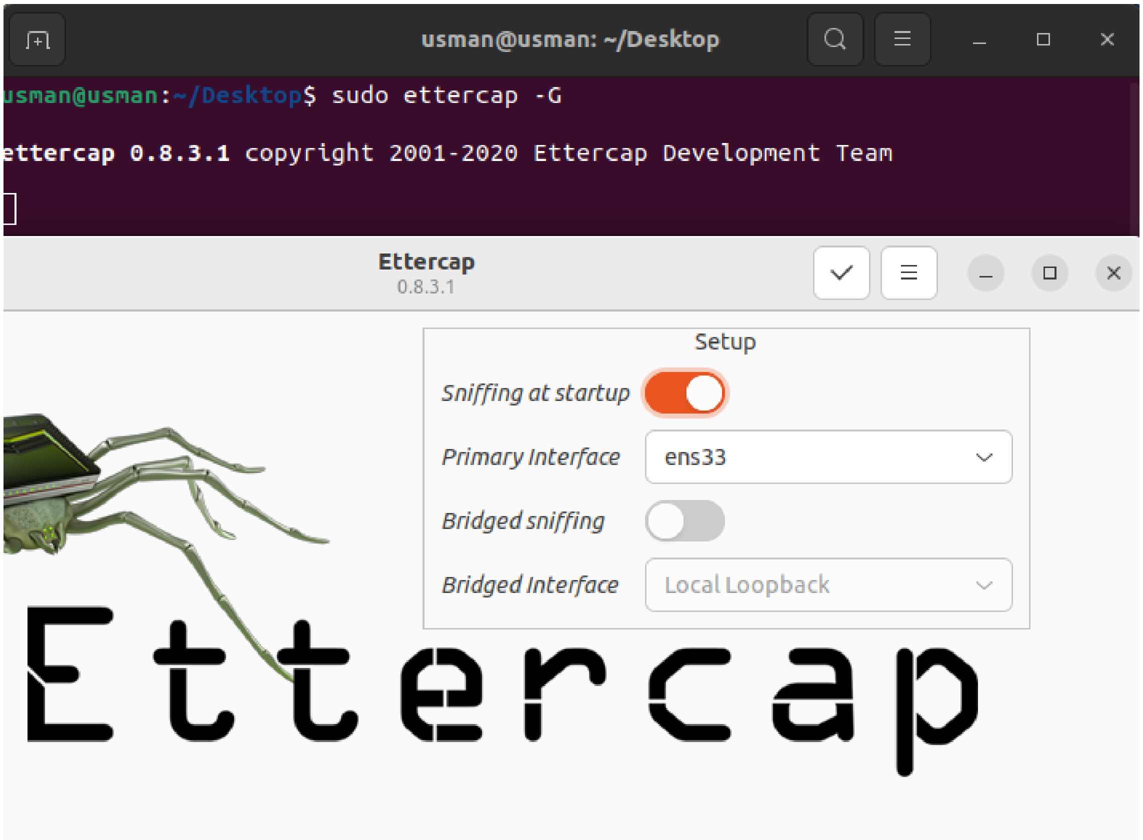

Ubuntu - VMware Workstation 17 Player (Non-commercial use only)
Player
15:20 27 ابریل
usman
●●●●●●●●
Ubuntu

Step 3: Checking the IP address by typing the command ifconfig in the terminal



```
usman@usman:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.2.128  netmask 255.255.255.0  broadcast 192.168.2.255
        inet6 fe80::8c3d:91f0:50c1:69f2  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:56:2f:03  txqueuelen 1000  (Ethernet)
        RX packets 96047  bytes 140988419 (140.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7179  bytes 548531 (548.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 309  bytes 30633 (30.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 309  bytes 30633 (30.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Step 4: Starting the graphical version of Ettercap



```
usman@usman:~/Desktop$ sudo ettercap -G

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team
```

Setup

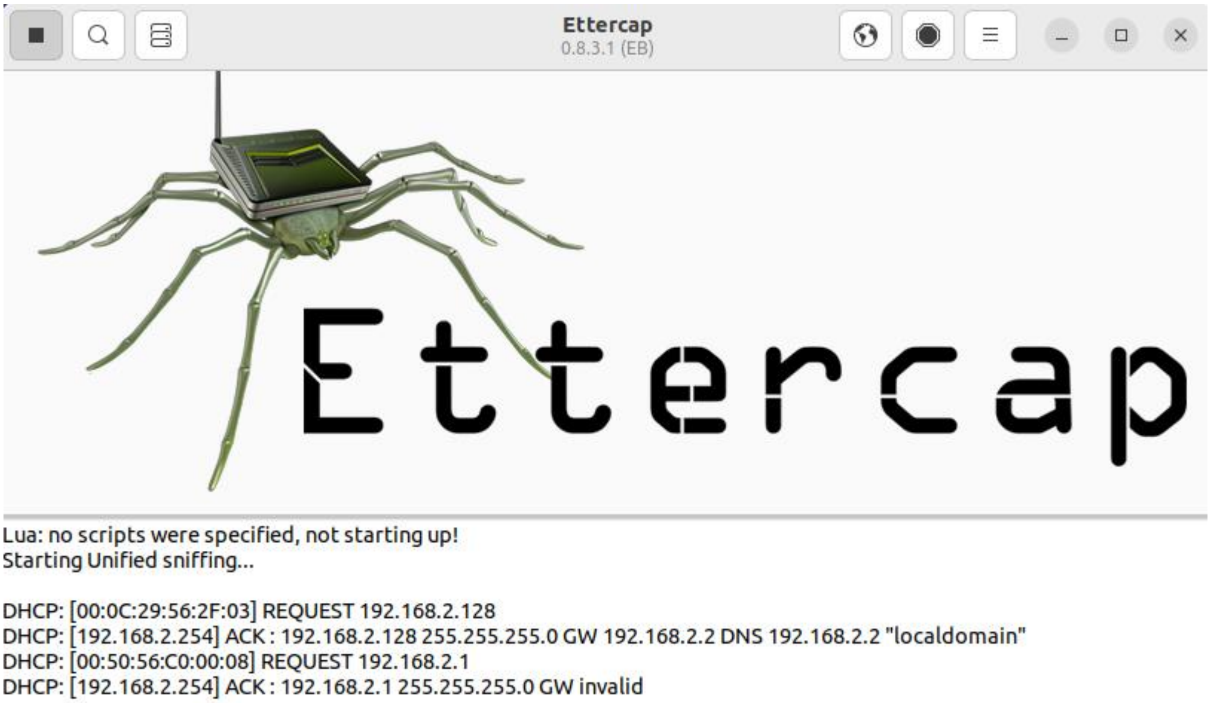
Sniffing at startup ●

Primary Interface ens33

Bridged sniffing ○

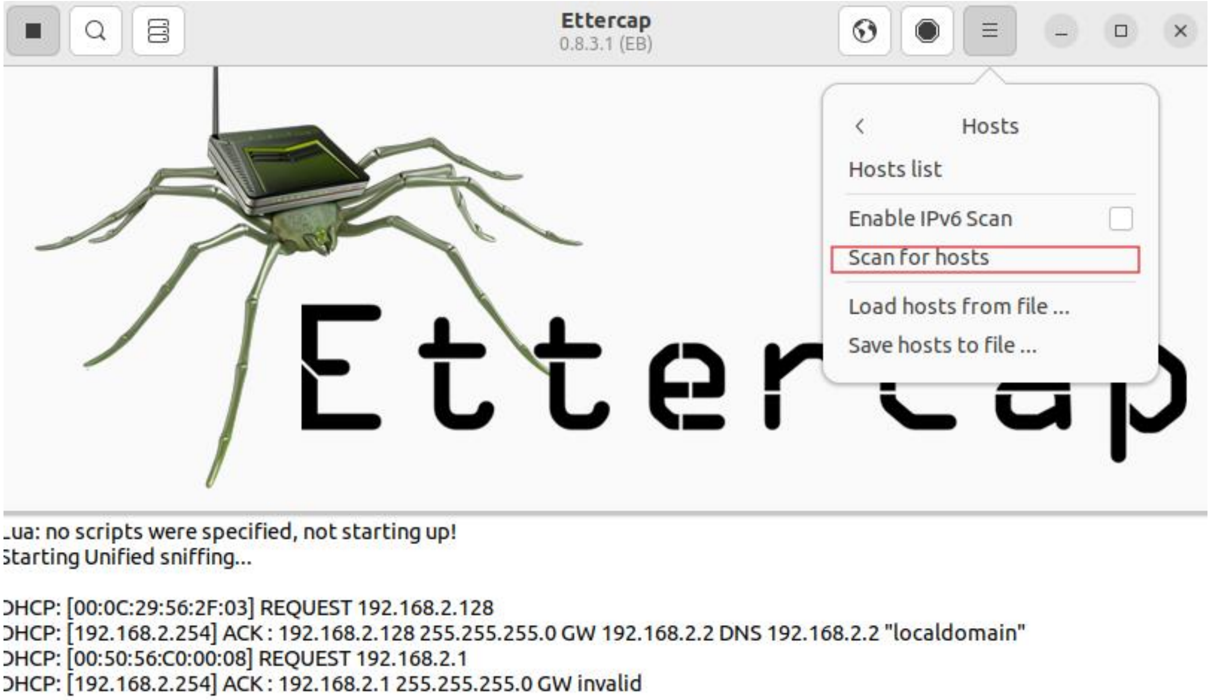
Bridged Interface Local Loopback

Step 5: Initiating Unified Sniffing



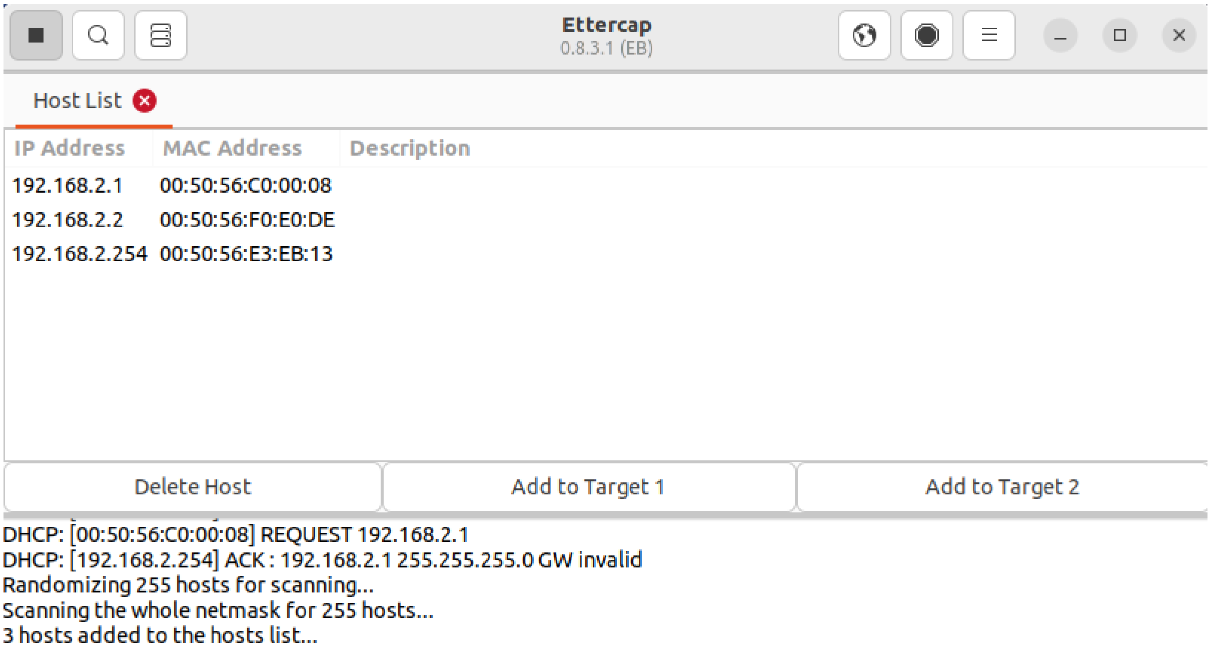
```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
```

Step 6: Scanning for Hosts



```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
```

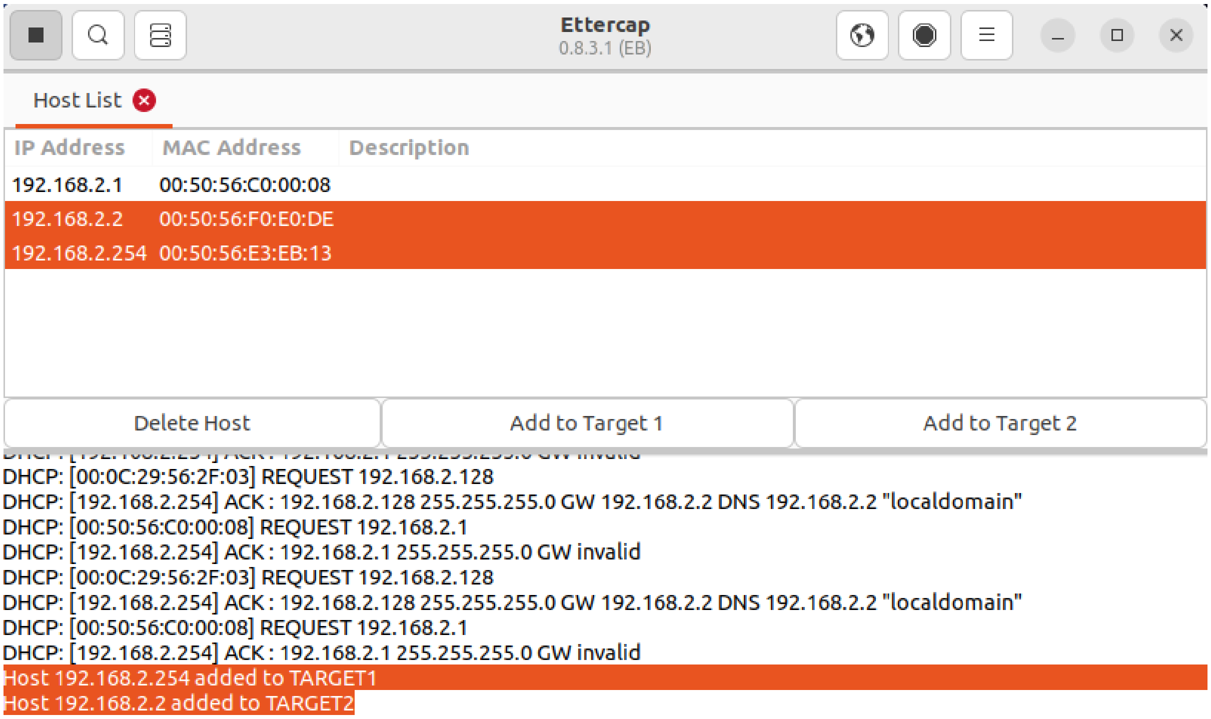
Step 7: Hosts List



IP Address	MAC Address	Description
192.168.2.1	00:50:56:C0:00:08	
192.168.2.2	00:50:56:F0:E0:DE	
192.168.2.254	00:50:56:E3:EB:13	

```
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```

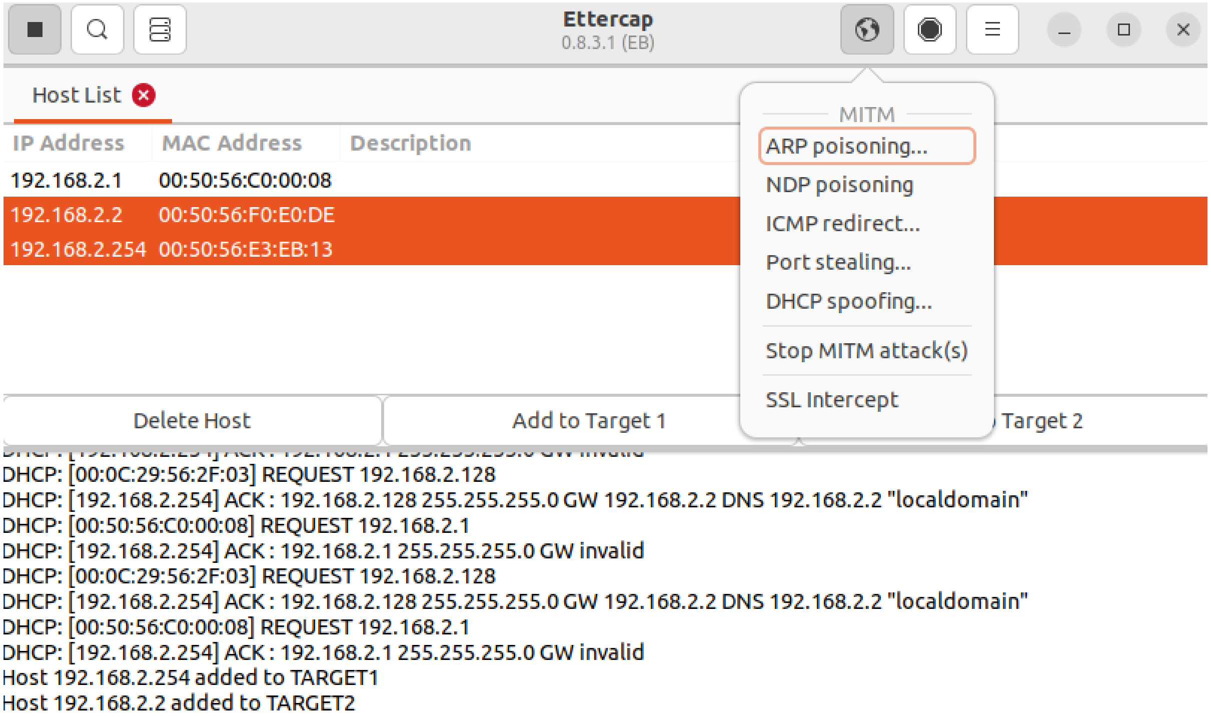
Step 8-9: Selecting Targets



IP Address	MAC Address	Description
192.168.2.1	00:50:56:C0:00:08	
192.168.2.2	00:50:56:F0:E0:DE	
192.168.2.254	00:50:56:E3:EB:13	

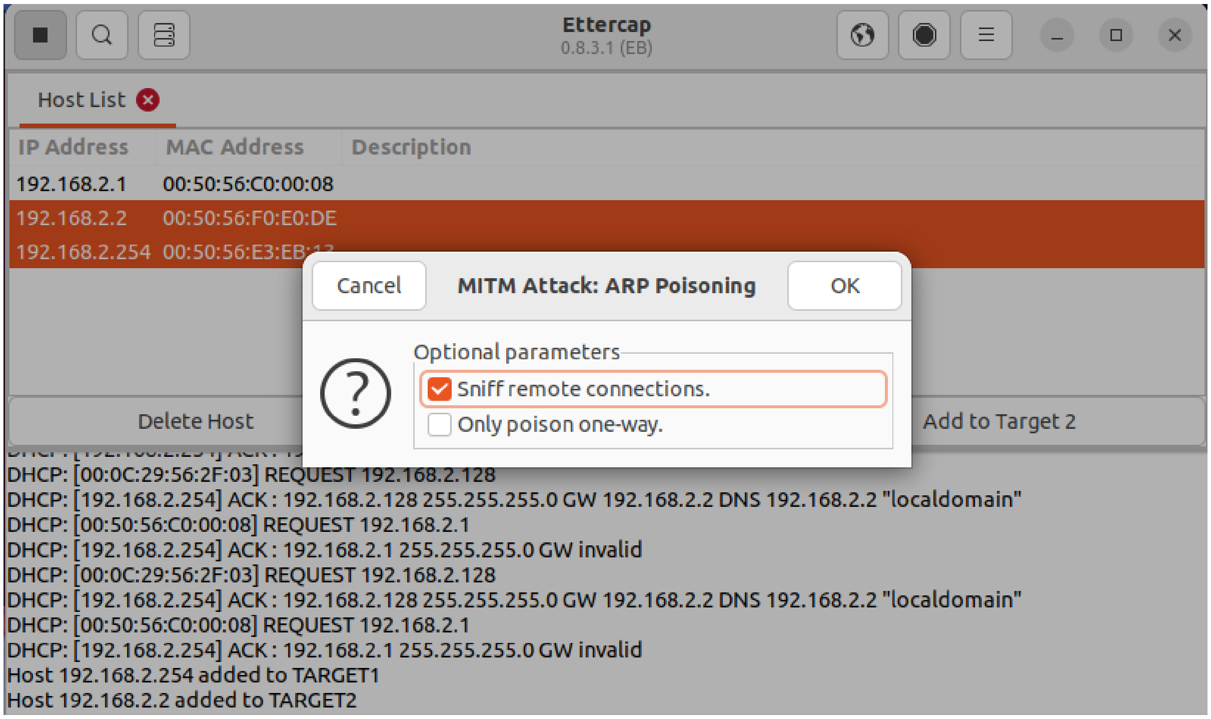
```
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
Host 192.168.2.254 added to TARGET1
Host 192.168.2.2 added to TARGET2
```

Step 10: ARP Poisoning and Sniffing remote connections



IP Address	MAC Address	Description
192.168.2.1	00:50:56:C0:00:08	
192.168.2.2	00:50:56:F0:E0:DE	
192.168.2.254	00:50:56:E3:EB:13	

```
DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
Host 192.168.2.254 added to TARGET1
Host 192.168.2.2 added to TARGET2
```



IP Address	MAC Address	Description
192.168.2.1	00:50:56:C0:00:08	
192.168.2.2	00:50:56:F0:E0:DE	
192.168.2.254	00:50:56:E3:EB:13	

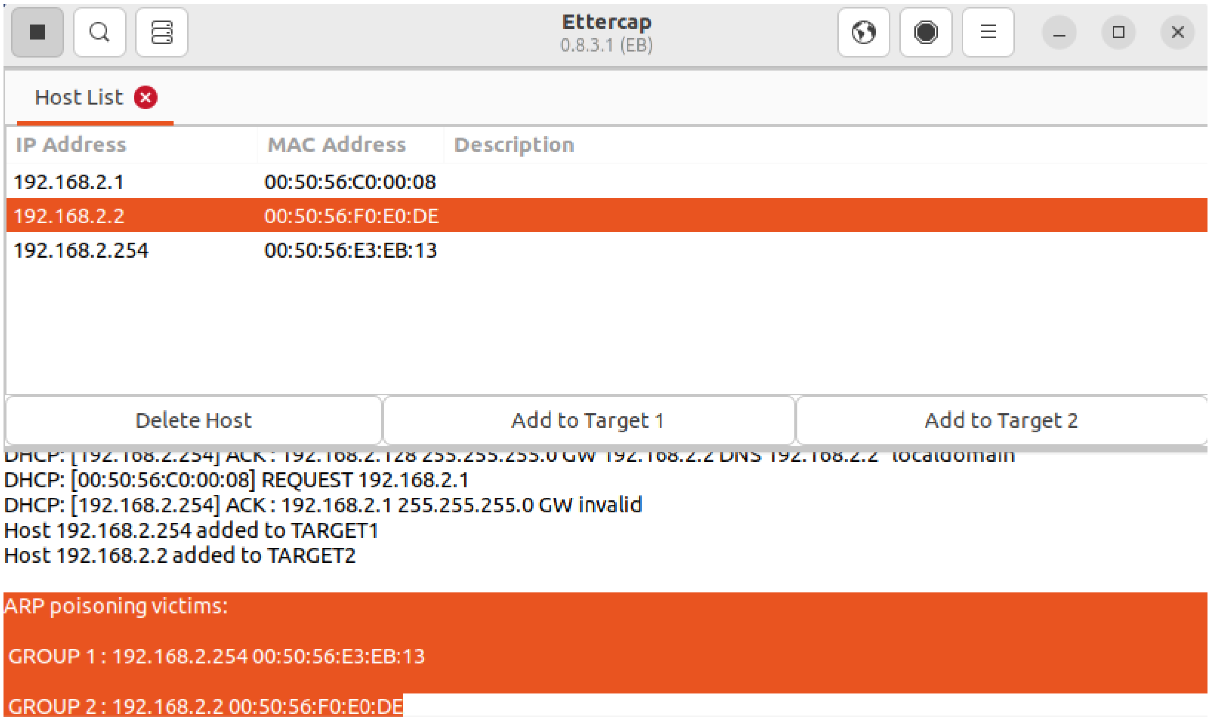
Optional parameters

☑ Sniff remote connections.

□ Only poison one-way.

```
DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
DHCP: [00:0C:29:56:2F:03] REQUEST 192.168.2.128
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
Host 192.168.2.254 added to TARGET1
Host 192.168.2.2 added to TARGET2
```

Step 11-12: Start Sniffing and Check Results



IP Address	MAC Address	Description
192.168.2.1	00:50:56:C0:00:08	
192.168.2.2	00:50:56:F0:E0:DE	
192.168.2.254	00:50:56:E3:EB:13	

```
DHCP: [192.168.2.254] ACK : 192.168.2.128 255.255.255.0 GW 192.168.2.2 DNS 192.168.2.2 "localdomain"
DHCP: [00:50:56:C0:00:08] REQUEST 192.168.2.1
DHCP: [192.168.2.254] ACK : 192.168.2.1 255.255.255.0 GW invalid
Host 192.168.2.254 added to TARGET1
Host 192.168.2.2 added to TARGET2

ARP poisoning victims:

 GROUP 1 : 192.168.2.254 00:50:56:E3:EB:13

 GROUP 2 : 192.168.2.2 00:50:56:F0:E0:DE
```