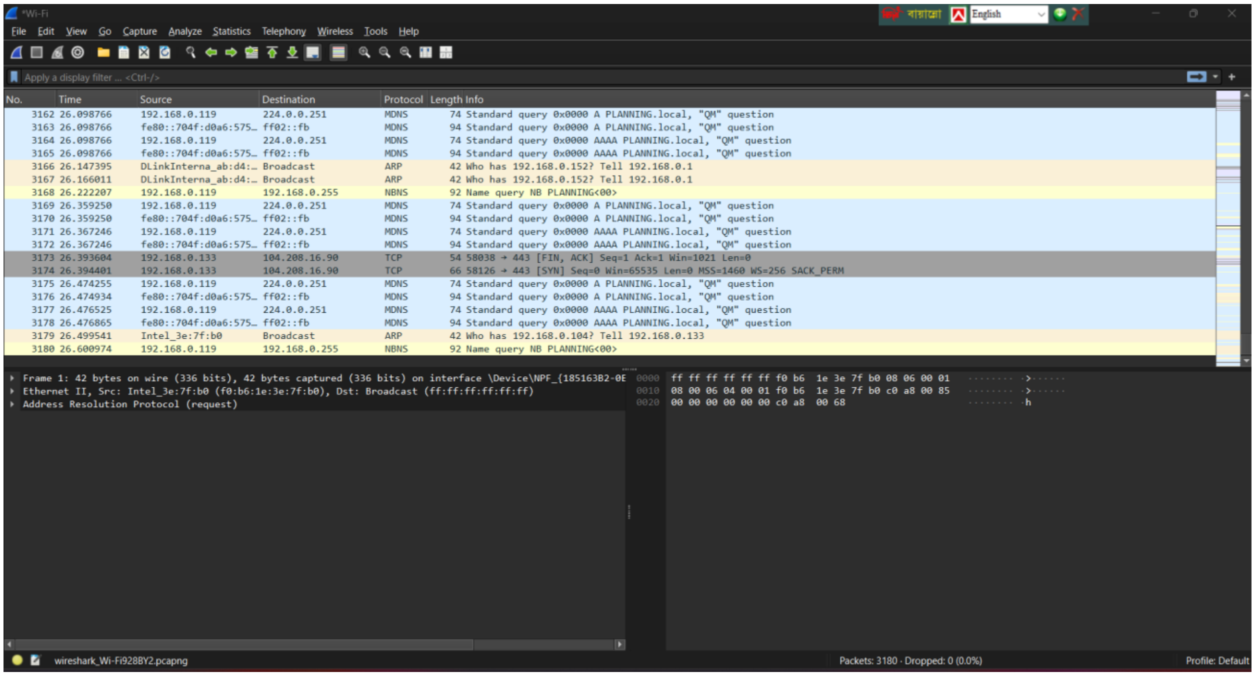
Capture network traffic using Wireshark


*Wi-Fi
বায়াম্লো
English
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

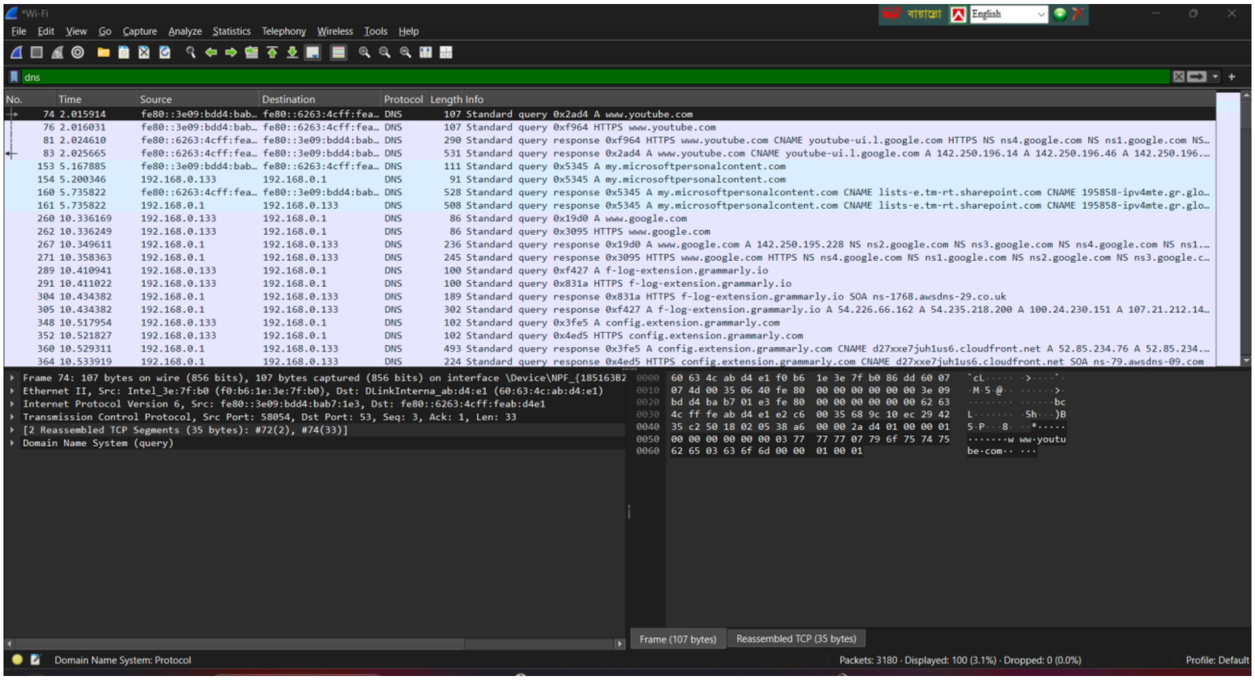
```
No.   Time       Source                 Destination     Protocol Length Info
 3162 26.098766  192.168.0.119          224.0.0.251     MDNS     74 Standard query 0x0000 A PLANNING.local, "QM" question
 3163 26.098766  fe80::704f:d0a6:575…   ff02::fb        MDNS     94 Standard query 0x0000 A PLANNING.local, "QM" question
 3164 26.098766  192.168.0.119          224.0.0.251     MDNS     74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
 3165 26.098766  fe80::704f:d0a6:575…   ff02::fb        MDNS     94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
 3166 26.147395  DLinkInterna_ab:d4:…   Broadcast       ARP      42 Who has 192.168.0.152? Tell 192.168.0.1
 3167 26.166011  DLinkInterna_ab:d4:…   Broadcast       ARP      42 Who has 192.168.0.152? Tell 192.168.0.1
 3168 26.222207  192.168.0.119          192.168.0.255   NBNS     92 Name query NB PLANNING<00>
 3169 26.359250  192.168.0.119          224.0.0.251     MDNS     74 Standard query 0x0000 A PLANNING.local, "QM" question
 3170 26.359250  fe80::704f:d0a6:575…   ff02::fb        MDNS     94 Standard query 0x0000 A PLANNING.local, "QM" question
 3171 26.367246  192.168.0.119          224.0.0.251     MDNS     74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
 3172 26.367246  fe80::704f:d0a6:575…   ff02::fb        MDNS     94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
 3173 26.393604  192.168.0.133          104.208.16.90   TCP      54 58038 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1021 Len=0
 3174 26.394401  192.168.0.133          104.208.16.90   TCP      66 58126 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 3175 26.474255  192.168.0.119          224.0.0.251     MDNS     74 Standard query 0x0000 A PLANNING.local, "QM" question
 3176 26.474934  fe80::704f:d0a6:575…   ff02::fb        MDNS     94 Standard query 0x0000 A PLANNING.local, "QM" question
 3177 26.476525  192.168.0.119          224.0.0.251     MDNS     74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
 3178 26.476865  fe80::704f:d0a6:575…   ff02::fb        MDNS     94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
 3179 26.499541  Intel_3e:7f:b0         Broadcast       ARP      42 Who has 192.168.0.104? Tell 192.168.0.133
 3180 26.600974  192.168.0.119          192.168.0.255   NBNS     92 Name query NB PLANNING<00>
```

```
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{185163B2-0E
Ethernet II, Src: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff f0 b6  1e 3e 7f b0 08 06 00 01   ········ ·>······
0010  08 00 06 04 00 01 f0 b6  1e 3e 7f b0 c0 a8 00 85   ········ ·>······
0020  00 00 00 00 00 00 c0 a8  00 68                     ········ ·h
```

wireshark_Wi-Fi928BY2.pcapng   Packets: 3180 · Dropped: 0 (0.0%)   Profile: Default

dns= 100


*Wi-Fi
বায়াম্লো
English
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Frame (107 bytes)
Reassembled TCP (35 bytes)

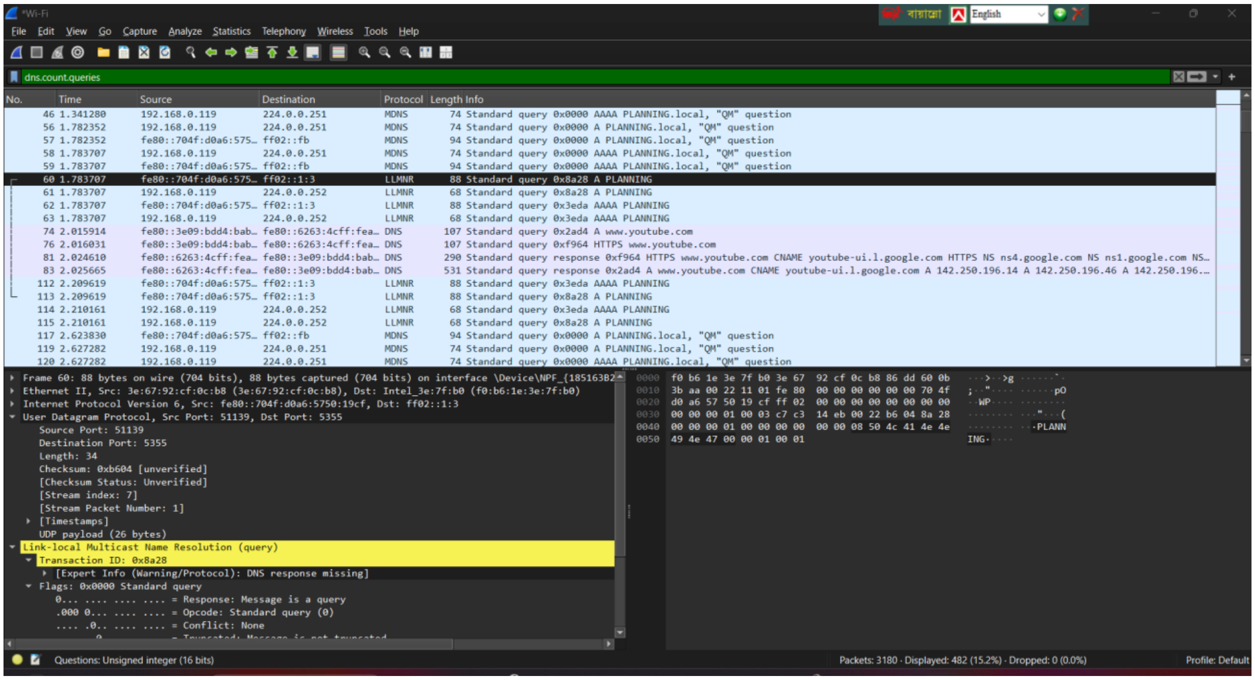
dns

```
No.  Time       Source                Destination           Protocol Length Info
  74 2.015914   fe80::3e09:bdd4:bab…  fe80::6263:4cff:fea…  DNS      107 Standard query 0x2ad4 A www.youtube.com
  76 2.016031   fe80::3e09:bdd4:bab…  fe80::6263:4cff:fea…  DNS      107 Standard query 0xf964 HTTPS www.youtube.com
  81 2.024610   fe80::6263:4cff:fea…  fe80::3e09:bdd4:bab…  DNS      290 Standard query response 0xf964 HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS NS ns4.google.com NS ns1.google.com NS…
  83 2.025665   fe80::6263:4cff:fea…  fe80::3e09:bdd4:bab…  DNS      531 Standard query response 0x2ad4 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.196.14 A 142.250.196.46 A 142.250.196.…
 153 5.167885   fe80::3e09:bdd4:bab…  fe80::6263:4cff:fea…  DNS      111 Standard query 0x5345 A my.microsoftpersonalcontent.com
 154 5.200346   192.168.0.133         192.168.0.1           DNS       91 Standard query 0x5345 A my.microsoftpersonalcontent.com
 160 5.735822   fe80::6263:4cff:fea…  fe80::3e09:bdd4:bab…  DNS      528 Standard query response 0x5345 A my.microsoftpersonalcontent.com CNAME lists-e.tm-rt.sharepoint.com CNAME 195858-ipv4mte.gr.glo…
 161 5.735822   192.168.0.1           192.168.0.133         DNS      508 Standard query response 0x5345 A my.microsoftpersonalcontent.com CNAME lists-e.tm-rt.sharepoint.com CNAME 195858-ipv4mte.gr.glo…
 260 10.336169  192.168.0.133         192.168.0.1           DNS       86 Standard query 0x19d0 A www.google.com
 262 10.336249  192.168.0.133         192.168.0.1           DNS       86 Standard query 0x3095 HTTPS www.google.com
 267 10.349611  192.168.0.1           192.168.0.133         DNS      236 Standard query response 0x19d0 A www.google.com A 142.250.195.228 NS ns2.google.com NS ns3.google.com NS ns4.google.com NS ns1.…
 271 10.358363  192.168.0.1           192.168.0.133         DNS      245 Standard query response 0x3095 HTTPS www.google.com HTTPS NS ns4.google.com NS ns1.google.com NS ns2.google.com NS ns3.google.c…
 289 10.410941  192.168.0.133         192.168.0.1           DNS      100 Standard query 0xf427 A f-log-extension.grammarly.io
 291 10.411022  192.168.0.133         192.168.0.1           DNS      100 Standard query 0x831a HTTPS f-log-extension.grammarly.io
 304 10.434382  192.168.0.1           192.168.0.133         DNS      189 Standard query response 0x831a HTTPS f-log-extension.grammarly.io SOA ns-1768.awsdns-29.co.uk
 305 10.434382  192.168.0.1           192.168.0.133         DNS      302 Standard query response 0xf427 A f-log-extension.grammarly.io A 54.226.66.162 A 54.235.218.200 A 100.24.230.151 A 107.21.212.14…
 348 10.517954  192.168.0.133         192.168.0.1           DNS      102 Standard query 0x3fe5 A config.extension.grammarly.com
 352 10.521827  192.168.0.133         192.168.0.1           DNS      102 Standard query 0x4ed5 HTTPS config.extension.grammarly.com
 360 10.529311  192.168.0.1           192.168.0.133         DNS      493 Standard query response 0x3fe5 A config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net A 52.85.234.76 A 52.85.234.…
 364 10.533919  192.168.0.1           192.168.0.133         DNS      224 Standard query response 0x4ed5 HTTPS config.extension.grammarly.com CNAME d27xxe7juh1us6.cloudfront.net SOA ns-79.awsdns-09.com
```

```
Frame 74: 107 bytes on wire (856 bits), 107 bytes captured (856 bits) on interface \Device\NPF_{185163B2
Ethernet II, Src: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0), Dst: DLinkInterna_ab:d4:e1 (60:63:4c:ab:d4:e1)
Internet Protocol Version 6, Src: fe80::3e09:bdd4:bab7:1e3, Dst: fe80::6263:4cff:feab:d4e1
Transmission Control Protocol, Src Port: 58054, Dst Port: 53, Seq: 3, Ack: 1, Len: 33
[2 Reassembled TCP Segments (35 bytes): #72(2), #74(33)]
Domain Name System (query)
```

```
0000  60 63 4c ab d4 e1 f0 b6  1e 3e 7f b0 86 dd 60 07   `cL····· ·>····`·
0010  07 4d 00 35 06 40 fe 80  00 00 00 00 00 00 3e 09   ·M·5·@·· ······>·
0020  bd d4 ba b7 01 e3 fe 80  00 00 00 00 00 00 62 63   ········ ······bc
0030  4c ff fe ab d4 e1 e2 c6  00 35 68 9c 10 ec 29 42   L······· ·5h···)B
0040  35 c2 50 18 02 05 38 a6  00 00 2a d4 01 00 00 01   5·P···8· ··*·····
0050  00 00 00 00 00 00 03 77  77 77 07 79 6f 75 74 75   ·······w ww·youtu
0060  62 65 03 63 6f 6d 00 00  01 00 01                  be·com·· ···
```

Domain Name System: Protocol   Packets: 3180 · Displayed: 100 (3.1%) · Dropped: 0 (0.0%)   Profile: Default dns.count.queries = 482



```
dns.count.queries
```

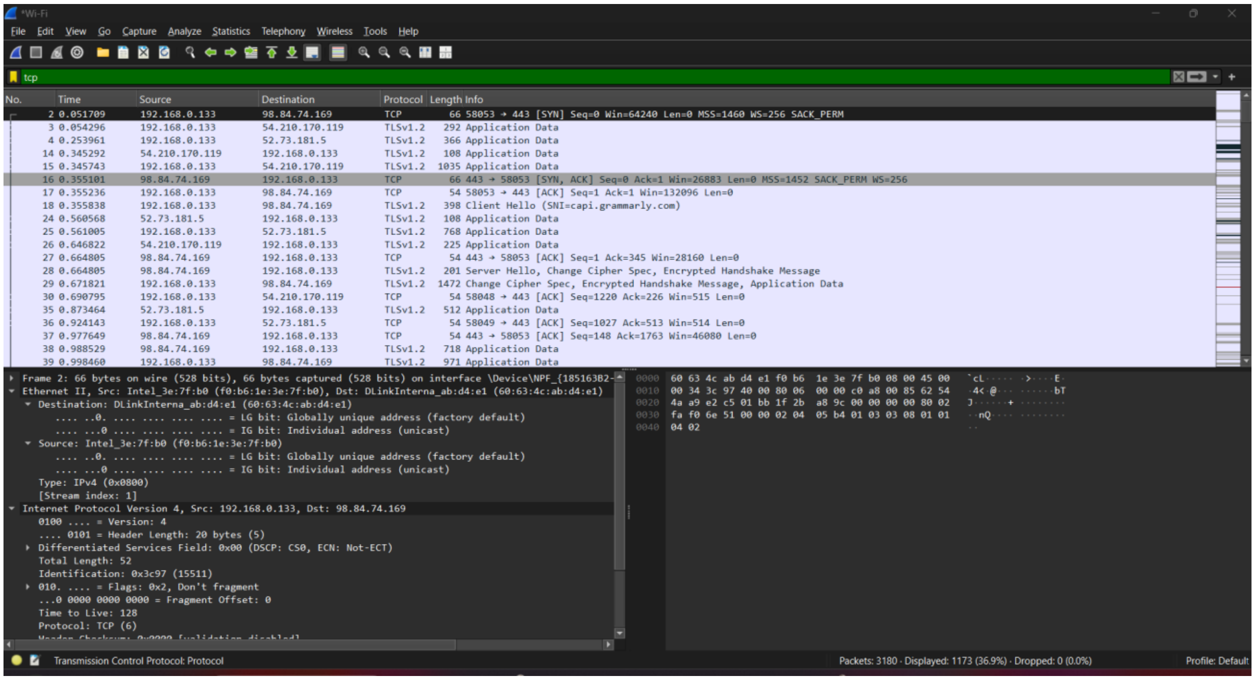
```
No.  Time       Source                   Destination              Protocol Length Info
  46 1.341280   192.168.0.119            224.0.0.251              MDNS      74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
  56 1.782352   192.168.0.119            224.0.0.251              MDNS      74 Standard query 0x0000 A PLANNING.local, "QM" question
  57 1.782352   fe80::704f:d0a6:575…     ff02::fb                 MDNS      94 Standard query 0x0000 A PLANNING.local, "QM" question
  58 1.783707   192.168.0.119            224.0.0.251              MDNS      74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
  59 1.783707   fe80::704f:d0a6:575…     ff02::fb                 MDNS      94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
  60 1.783707   fe80::704f:d0a6:575…     ff02::1:3                LLMNR     88 Standard query 0x8a28 A PLANNING
  61 1.783707   192.168.0.119            224.0.0.252              LLMNR     68 Standard query 0x8a28 A PLANNING
  62 1.783707   fe80::704f:d0a6:575…     ff02::1:3                LLMNR     88 Standard query 0x3eda AAAA PLANNING
  63 1.783707   192.168.0.119            224.0.0.252              LLMNR     68 Standard query 0x3eda AAAA PLANNING
  74 2.015914   fe80::3e09:bdd4:bab…     fe80::6263:4cff:fea…     DNS      107 Standard query 0x2ad4 A www.youtube.com
  76 2.016031   fe80::3e09:bdd4:bab…     fe80::6263:4cff:fea…     DNS      107 Standard query 0xf964 HTTPS www.youtube.com
  81 2.024610   fe80::6263:4cff:fea…     fe80::3e09:bdd4:bab…     DNS      290 Standard query response 0xf964 HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS NS ns4.google.com NS ns1.google.com NS…
  83 2.025665   fe80::6263:4cff:fea…     fe80::3e09:bdd4:bab…     DNS      531 Standard query response 0x2ad4 A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.196.14 A 142.250.196.46 A 142.250.196.…
 112 2.209619   fe80::704f:d0a6:575…     ff02::1:3                LLMNR     88 Standard query 0x3eda AAAA PLANNING
 113 2.209619   fe80::704f:d0a6:575…     ff02::1:3                LLMNR     88 Standard query 0x8a28 A PLANNING
 114 2.210161   192.168.0.119            224.0.0.252              LLMNR     68 Standard query 0x3eda AAAA PLANNING
 115 2.210161   192.168.0.119            224.0.0.252              LLMNR     68 Standard query 0x8a28 A PLANNING
 117 2.623830   fe80::704f:d0a6:575…     ff02::fb                 MDNS      94 Standard query 0x0000 A PLANNING.local, "QM" question
 119 2.627282   192.168.0.119            224.0.0.251              MDNS      74 Standard query 0x0000 A PLANNING.local, "QM" question
 120 2.627282   192.168.0.119            224.0.0.251              MDNS      74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
```

```
Frame 60: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \Device\NPF_{185163B2
Ethernet II, Src: 3e:67:92:cf:0c:b8 (3e:67:92:cf:0c:b8), Dst: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0)
Internet Protocol Version 6, Src: fe80::704f:d0a6:5750:19cf, Dst: ff02::1:3
User Datagram Protocol, Src Port: 51139, Dst Port: 5355
    Source Port: 51139
    Destination Port: 5355
    Length: 34
    Checksum: 0xb604 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
    [Stream Packet Number: 1]
  > [Timestamps]
    UDP payload (26 bytes)
Link-local Multicast Name Resolution (query)
    Transaction ID: 0x8a28
      > [Expert Info (Warning/Protocol): DNS response missing]
    Flags: 0x0000 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Conflict: None
        .... ..0. .... .... = Truncated: Message is not truncated
```

```
0000  f0 b6 1e 3e 7f b0 3e 67  92 cf 0c b8 86 dd 60 0b   ···>··>g ······`·
0010  3b aa 00 22 11 01 fe 80  00 00 00 00 00 00 70 4f   ;··"···· ······pO
0020  d0 a6 57 50 19 cf ff 02  00 00 00 00 00 00 00 00   ··WP···· ········
0030  00 00 00 01 00 03 c7 c3  14 eb 00 22 b6 04 8a 28   ········ ···"···(
0040  00 00 00 01 00 00 00 00  00 00 08 50 4c 41 4e 4e   ········ ···PLANN
0050  49 4e 47 00 00 01 00 01                            ING·····
```

```
Questions: Unsigned integer (16 bits)          Packets: 3180 · Displayed: 482 (15.2%) · Dropped: 0 (0.0%)          Profile: Default
```

tcp – 1173



```
tcp
```

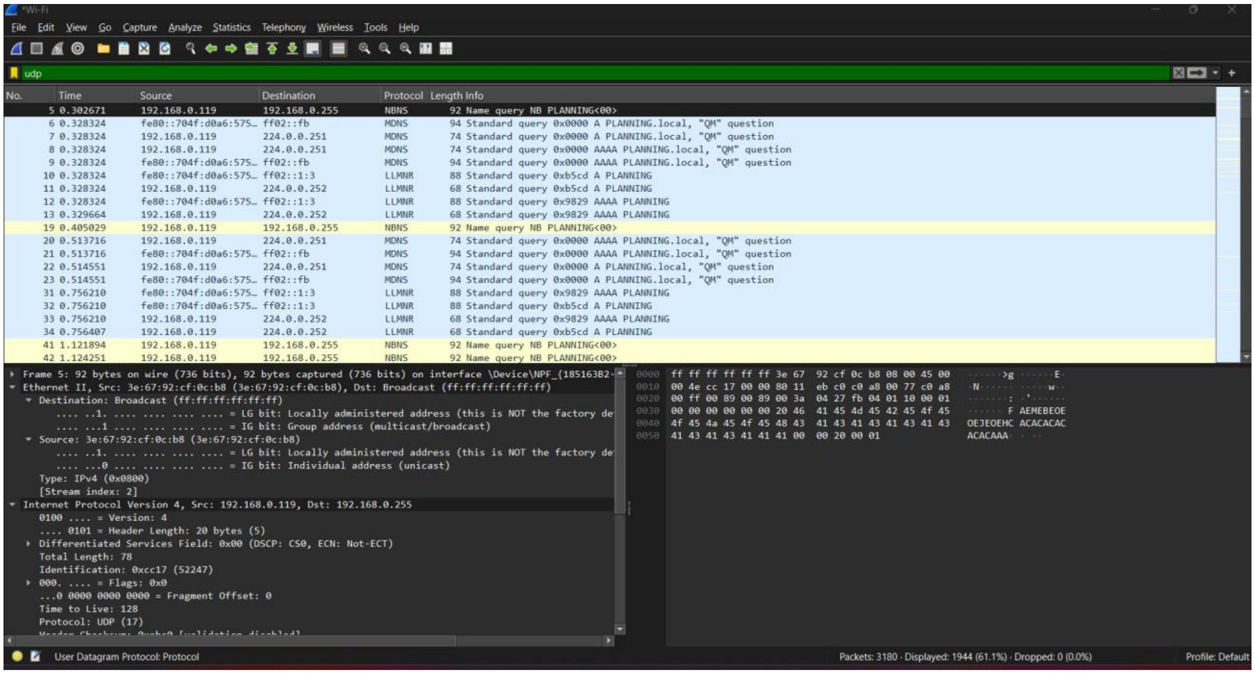
```
No.  Time       Source            Destination       Protocol Length Info
   2 0.051709   192.168.0.133     98.84.74.169      TCP       66 58053 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   3 0.054296   192.168.0.133     54.210.170.119    TLSv1.2  292 Application Data
   4 0.253961   192.168.0.133     52.73.181.5       TLSv1.2  366 Application Data
  14 0.345292   54.210.170.119    192.168.0.133     TLSv1.2  108 Application Data
  15 0.345743   192.168.0.133     54.210.170.119    TLSv1.2 1035 Application Data
  16 0.355101   98.84.74.169      192.168.0.133     TCP       66 443 → 58053 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1452 SACK_PERM WS=256
  17 0.355236   192.168.0.133     98.84.74.169      TCP       54 58053 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
  18 0.355838   192.168.0.133     98.84.74.169      TLSv1.2  398 Client Hello (SNI=capi.grammarly.com)
  24 0.560568   52.73.181.5       192.168.0.133     TLSv1.2  108 Application Data
  25 0.561005   192.168.0.133     52.73.181.5       TLSv1.2  768 Application Data
  26 0.646822   54.210.170.119    192.168.0.133     TLSv1.2  225 Application Data
  27 0.664805   98.84.74.169      192.168.0.133     TCP       54 443 → 58053 [ACK] Seq=1 Ack=345 Win=28160 Len=0
  28 0.664805   98.84.74.169      192.168.0.133     TLSv1.2  201 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  29 0.671821   192.168.0.133     98.84.74.169      TLSv1.2 1472 Change Cipher Spec, Encrypted Handshake Message, Application Data
  30 0.690795   192.168.0.133     54.210.170.119    TCP       54 58048 → 443 [ACK] Seq=1220 Ack=226 Win=515 Len=0
  35 0.873464   52.73.181.5       192.168.0.133     TLSv1.2  512 Application Data
  36 0.924143   192.168.0.133     52.73.181.5       TCP       54 58049 → 443 [ACK] Seq=1027 Ack=513 Win=514 Len=0
  37 0.977649   98.84.74.169      192.168.0.133     TCP       54 443 → 58053 [ACK] Seq=148 Ack=1763 Win=46080 Len=0
  38 0.988529   98.84.74.169      192.168.0.133     TLSv1.2  718 Application Data
  39 0.998460   192.168.0.133     98.84.74.169      TLSv1.2  971 Application Data
```

```
Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{185163B2-
Ethernet II, Src: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0), Dst: DLinkInterna_ab:d4:e1 (60:63:4c:ab:d4:e1)
    Destination: DLinkInterna_ab:d4:e1 (60:63:4c:ab:d4:e1)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
Internet Protocol Version 4, Src: 192.168.0.133, Dst: 98.84.74.169
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x3c97 (15511)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
```

```
0000  60 63 4c ab d4 e1 f0 b6  1e 3e 7f b0 08 00 45 00   `cL····· ·>····E·
0010  00 34 3c 97 40 00 80 06  00 00 c0 a8 00 85 62 54   ·4<·@··· ······bT
0020  4a a9 e2 c5 01 bb 1f 2b  a8 9c 00 00 00 00 80 02   J······+ ········
0030  fa f0 6e 51 00 00 02 04  05 b4 01 03 03 08 01 01   ··nQ···· ········
0040  04 02                                              ··
```

```
Transmission Control Protocol: Protocol          Packets: 3180 · Displayed: 1173 (36.9%) · Dropped: 0 (0.0%)          Profile: Default
```

udp – 1944



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

udp

```
No.   Time       Source                 Destination      Protocol Length Info
    5 0.302671   192.168.0.119          192.168.0.255    NBNS      92 Name query NB PLANNING<00>
    6 0.328324   fe80::704f:d0a6:575…   ff02::fb         MDNS      94 Standard query 0x0000 A PLANNING.local, "QM" question
    7 0.328324   192.168.0.119          224.0.0.251      MDNS      74 Standard query 0x0000 A PLANNING.local, "QM" question
    8 0.328324   192.168.0.119          224.0.0.251      MDNS      74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
    9 0.328324   fe80::704f:d0a6:575…   ff02::fb         MDNS      94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
   10 0.328324   fe80::704f:d0a6:575…   ff02::1:3        LLMNR     88 Standard query 0xb5cd A PLANNING
   11 0.328324   192.168.0.119          224.0.0.252      LLMNR     68 Standard query 0xb5cd A PLANNING
   12 0.328324   fe80::704f:d0a6:575…   ff02::1:3        LLMNR     88 Standard query 0x9829 AAAA PLANNING
   13 0.329664   192.168.0.119          224.0.0.252      LLMNR     68 Standard query 0x9829 AAAA PLANNING
   19 0.405029   192.168.0.119          192.168.0.255    NBNS      92 Name query NB PLANNING<00>
   20 0.513716   192.168.0.119          224.0.0.251      MDNS      74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
   21 0.513716   fe80::704f:d0a6:575…   ff02::fb         MDNS      94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
   22 0.514551   192.168.0.119          224.0.0.251      MDNS      74 Standard query 0x0000 A PLANNING.local, "QM" question
   23 0.514551   fe80::704f:d0a6:575…   ff02::fb         MDNS      94 Standard query 0x0000 A PLANNING.local, "QM" question
   31 0.756210   fe80::704f:d0a6:575…   ff02::1:3        LLMNR     88 Standard query 0x9829 AAAA PLANNING
   32 0.756210   fe80::704f:d0a6:575…   ff02::1:3        LLMNR     88 Standard query 0xb5cd A PLANNING
   33 0.756210   192.168.0.119          224.0.0.252      LLMNR     68 Standard query 0x9829 AAAA PLANNING
   34 0.756407   192.168.0.119          224.0.0.252      LLMNR     68 Standard query 0xb5cd A PLANNING
   41 1.121894   192.168.0.119          192.168.0.255    NBNS      92 Name query NB PLANNING<00>
   42 1.124251   192.168.0.119          192.168.0.255    NBNS      92 Name query NB PLANNING<00>
```

```
▸ Frame 5: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{185163B2-
▾ Ethernet II, Src: 3e:67:92:cf:0c:b8 (3e:67:92:cf:0c:b8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: 3e:67:92:cf:0c:b8 (3e:67:92:cf:0c:b8)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 2]
▾ Internet Protocol Version 4, Src: 192.168.0.119, Dst: 192.168.0.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 78
    Identification: 0xcc17 (52247)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xebc0 [validation disabled]
```

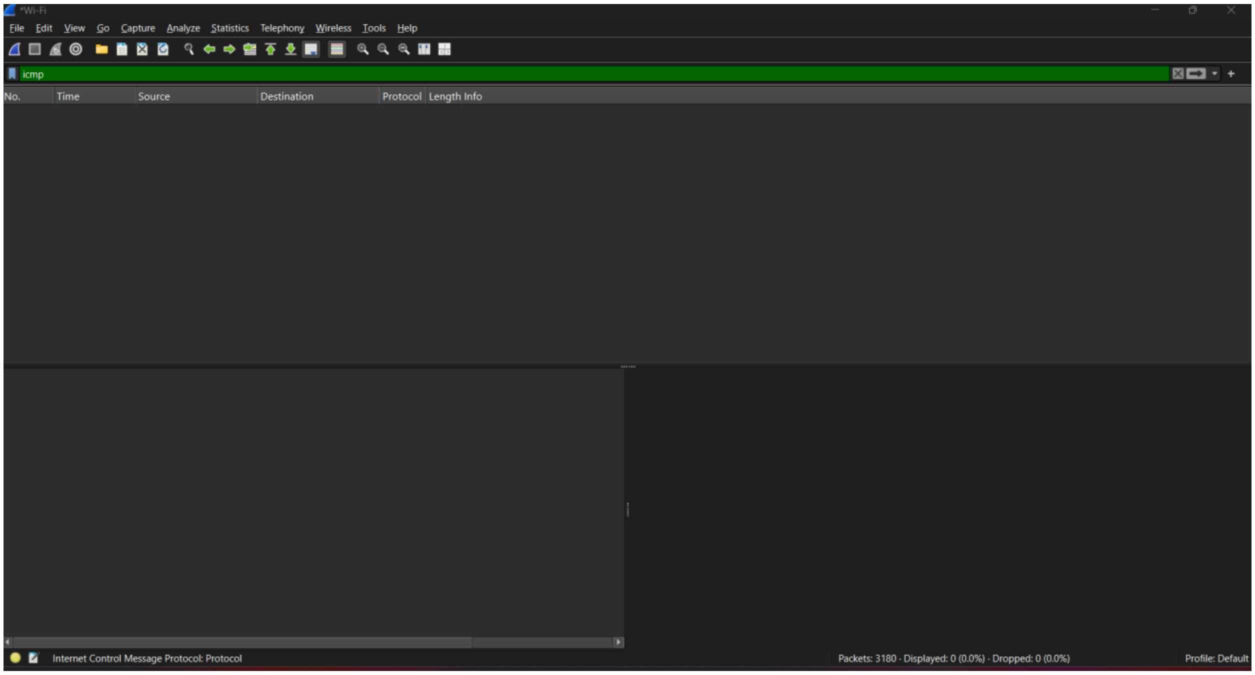
```
0000  ff ff ff ff ff ff 3e 67  92 cf 0c b8 08 00 45 00   ······>g ······E·
0010  00 4e cc 17 00 00 80 11  eb c0 c0 a8 00 77 c0 a8   ·N······ ·····w··
0020  00 ff 00 89 00 89 00 3a  04 27 fb 04 01 10 00 01   ·······: ·'······
0030  00 00 00 00 00 00 20 46  41 45 4d 45 42 45 4f 45   ······ F AEMEBEOE
0040  4f 45 4a 45 4f 45 48 43  41 43 41 43 41 43 41 43   OEJEOEHC ACACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA· · ··
```

User Datagram Protocol: Protocol

Packets: 3180 · Displayed: 1944 (61.1%) · Dropped: 0 (0.0%)

Profile: Default

icmp – 0



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

icmp

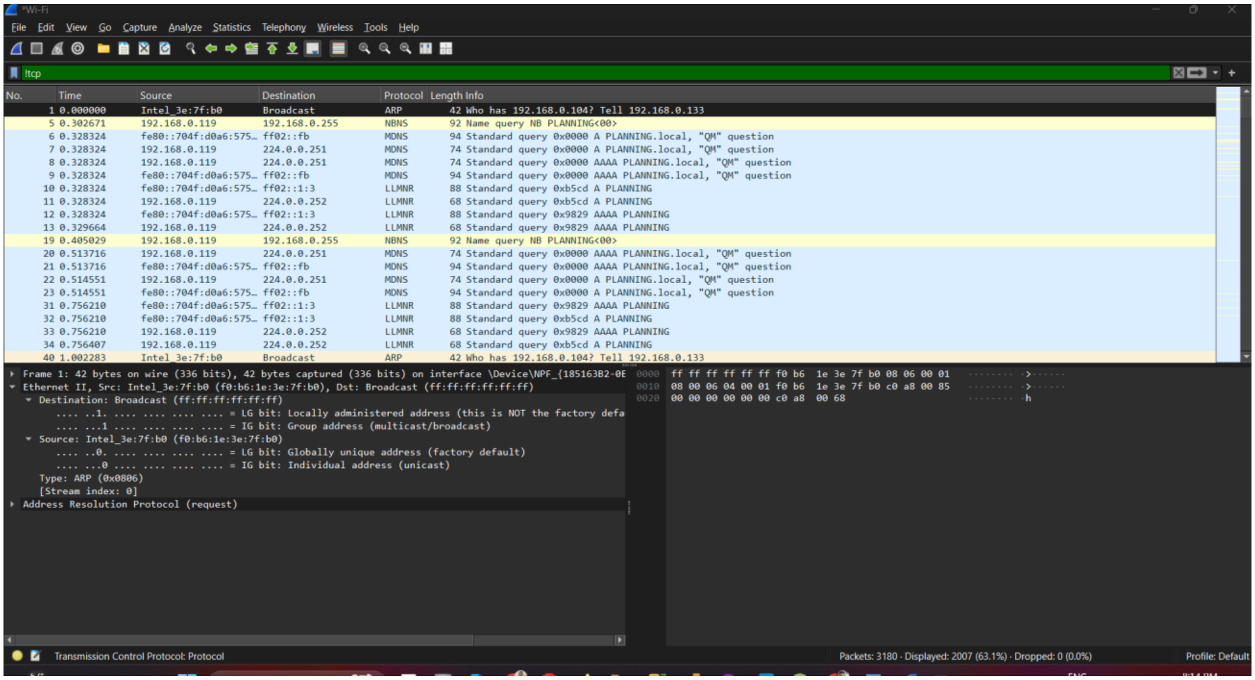
```
No.   Time       Source                 Destination      Protocol Length Info
```

Internet Control Message Protocol: Protocol

Packets: 3180 · Displayed: 0 (0.0%) · Dropped: 0 (0.0%)

Profile: Default

!tcp – 2007


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

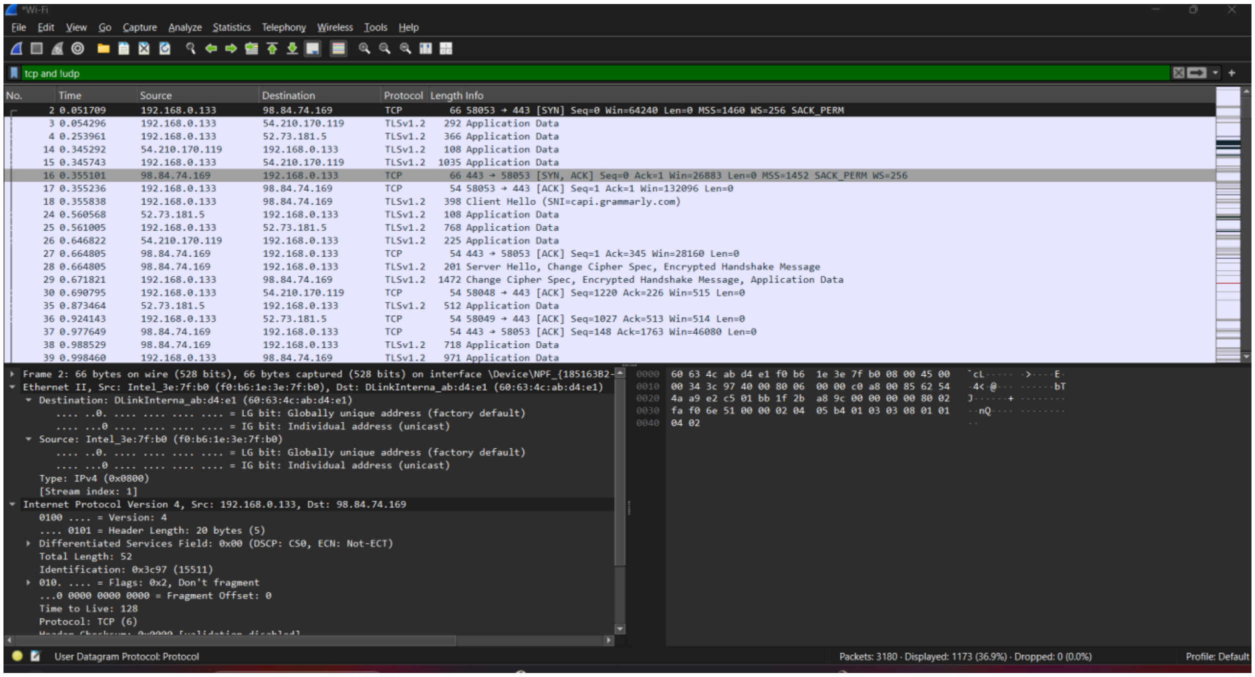
```
!tcp

No.  Time      Source                Destination    Protocol Length Info
   1 0.000000  Intel_3e:7f:b0        Broadcast      ARP      42 Who has 192.168.0.104? Tell 192.168.0.133
   5 0.302671  192.168.0.119         192.168.0.255  NBNS     92 Name query NB PLANNING<00>
   6 0.328324  fe80::704f:d0a6:575…  ff02::fb       MDNS     94 Standard query 0x0000 A PLANNING.local, "QM" question
   7 0.328324  192.168.0.119         224.0.0.251    MDNS     74 Standard query 0x0000 A PLANNING.local, "QM" question
   8 0.328324  192.168.0.119         224.0.0.251    MDNS     74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
   9 0.328324  fe80::704f:d0a6:575…  ff02::fb       MDNS     94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
  10 0.328324  fe80::704f:d0a6:575…  ff02::1:3      LLMNR    88 Standard query 0xb5cd A PLANNING
  11 0.328324  192.168.0.119         224.0.0.252    LLMNR    68 Standard query 0xb5cd A PLANNING
  12 0.328324  fe80::704f:d0a6:575…  ff02::1:3      LLMNR    88 Standard query 0x9829 AAAA PLANNING
  13 0.329664  192.168.0.119         224.0.0.252    LLMNR    68 Standard query 0x9829 AAAA PLANNING
  19 0.405029  192.168.0.119         192.168.0.255  NBNS     92 Name query NB PLANNING<00>
  20 0.513716  192.168.0.119         224.0.0.251    MDNS     74 Standard query 0x0000 AAAA PLANNING.local, "QM" question
  21 0.513716  fe80::704f:d0a6:575…  ff02::fb       MDNS     94 Standard query 0x0000 AAAA PLANNING.local, "QM" question
  22 0.514551  192.168.0.119         224.0.0.251    MDNS     74 Standard query 0x0000 A PLANNING.local, "QM" question
  23 0.514551  fe80::704f:d0a6:575…  ff02::fb       MDNS     94 Standard query 0x0000 A PLANNING.local, "QM" question
  31 0.756210  fe80::704f:d0a6:575…  ff02::1:3      LLMNR    88 Standard query 0x9829 AAAA PLANNING
  32 0.756210  fe80::704f:d0a6:575…  ff02::1:3      LLMNR    88 Standard query 0xb5cd A PLANNING
  33 0.756210  192.168.0.119         224.0.0.252    LLMNR    68 Standard query 0x9829 AAAA PLANNING
  34 0.756407  192.168.0.119         224.0.0.252    LLMNR    68 Standard query 0xb5cd A PLANNING
  40 1.002283  Intel_3e:7f:b0        Broadcast      ARP      42 Who has 192.168.0.104? Tell 192.168.0.133
```

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{185163B2-0E
▾ Ethernet II, Src: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory defa
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  ▾ Source: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
▸ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff f0 b6  1e 3e 7f b0 08 06 00 01   ········ ·>······
0010  08 00 06 04 00 01 f0 b6  1e 3e 7f b0 c0 a8 00 85   ········ ·>······
0020  00 00 00 00 00 00 c0 a8  00 68                     ········ ·h
```

```
Transmission Control Protocol: Protocol        Packets: 3180 · Displayed: 2007 (63.1%) · Dropped: 0 (0.0%)        Profile: Default
```

tcp and !udp – 1173


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

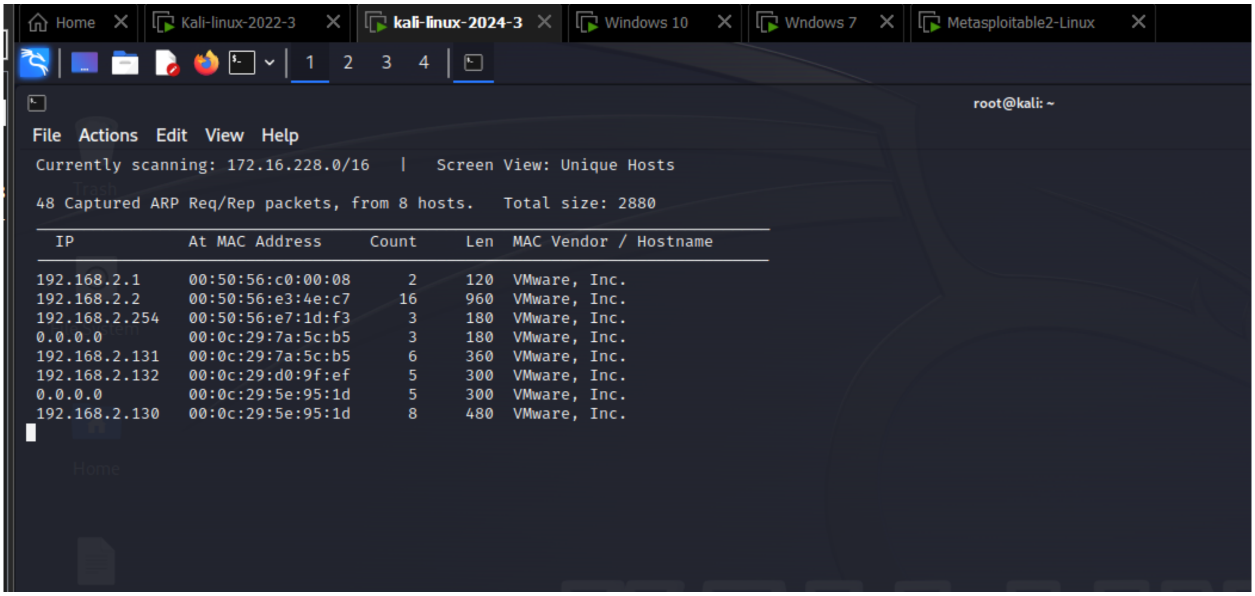
```
tcp and !udp

No.  Time      Source          Destination     Protocol Length Info
   2 0.051709  192.168.0.133   98.84.74.169    TCP        66 58053 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   3 0.054296  192.168.0.133   54.210.170.119  TLSv1.2   292 Application Data
   4 0.253961  192.168.0.133   52.73.181.5     TLSv1.2   366 Application Data
  14 0.345292  54.210.170.119  192.168.0.133   TLSv1.2   108 Application Data
  15 0.345743  192.168.0.133   54.210.170.119  TLSv1.2  1035 Application Data
  16 0.355101  98.84.74.169    192.168.0.133   TCP        66 443 → 58053 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1452 SACK_PERM WS=256
  17 0.355236  192.168.0.133   98.84.74.169    TCP        54 58053 → 443 [ACK] Seq=1 Ack=1 Win=132096 Len=0
  18 0.355838  192.168.0.133   98.84.74.169    TLSv1.2   398 Client Hello (SNI=capi.grammarly.com)
  24 0.560568  52.73.181.5     192.168.0.133   TLSv1.2   108 Application Data
  25 0.561005  192.168.0.133   52.73.181.5     TLSv1.2   768 Application Data
  26 0.646822  54.210.170.119  192.168.0.133   TLSv1.2   225 Application Data
  27 0.664805  98.84.74.169    192.168.0.133   TCP        54 443 → 58053 [ACK] Seq=1 Ack=345 Win=28160 Len=0
  28 0.664805  98.84.74.169    192.168.0.133   TLSv1.2   201 Server Hello, Change Cipher Spec, Encrypted Handshake Message
  29 0.671821  192.168.0.133   98.84.74.169    TLSv1.2  1472 Change Cipher Spec, Encrypted Handshake Message, Application Data
  30 0.690795  192.168.0.133   54.210.170.119  TCP        54 58048 → 443 [ACK] Seq=1220 Ack=226 Win=515 Len=0
  35 0.873464  52.73.181.5     192.168.0.133   TLSv1.2   512 Application Data
  36 0.924143  192.168.0.133   52.73.181.5     TCP        54 58049 → 443 [ACK] Seq=1027 Ack=513 Win=514 Len=0
  37 0.977649  98.84.74.169    192.168.0.133   TCP        54 443 → 58053 [ACK] Seq=148 Ack=1763 Win=46080 Len=0
  38 0.988529  98.84.74.169    192.168.0.133   TLSv1.2   718 Application Data
  39 0.998460  192.168.0.133   98.84.74.169    TLSv1.2   971 Application Data
```

```
▸ Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{185163B2-
▾ Ethernet II, Src: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0), Dst: DLinkInterna_ab:d4:e1 (60:63:4c:ab:d4:e1)
  ▾ Destination: DLinkInterna_ab:d4:e1 (60:63:4c:ab:d4:e1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
▾ Internet Protocol Version 4, Src: 192.168.0.133, Dst: 98.84.74.169
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x3c97 (15511)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
```

```
0000  60 63 4c ab d4 e1 f0 b6  1e 3e 7f b0 08 00 45 00   `cL····· ·>····E·
0010  00 34 3c 97 40 00 80 06  00 00 c0 a8 00 85 62 54   ·4<·@··· ······bT
0020  4a a9 e2 c5 01 bb 1f 2b  a8 9c 00 00 00 00 80 02   J······+ ········
0030  fa f0 6e 51 00 00 02 04  05 b4 01 03 03 08 01 01   ··nQ···· ········
0040  04 02                                              ··
```

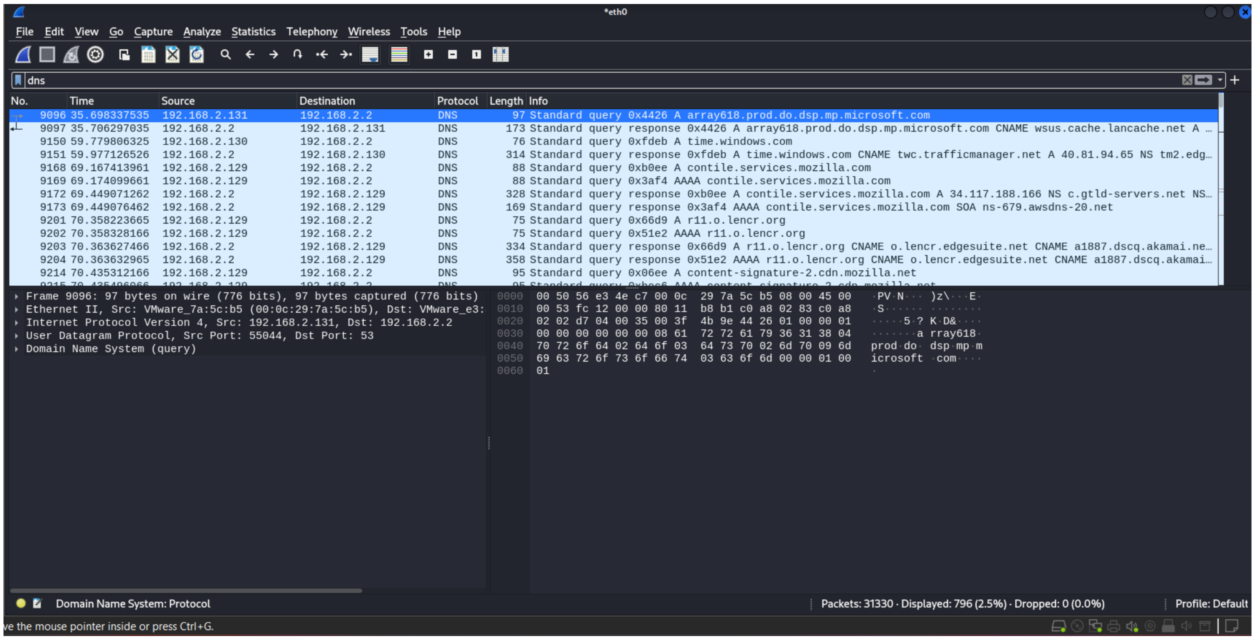
```
User Datagram Protocol: Protocol        Packets: 3180 · Displayed: 1173 (36.9%) · Dropped: 0 (0.0%)        Profile: Default
```

netdiscover



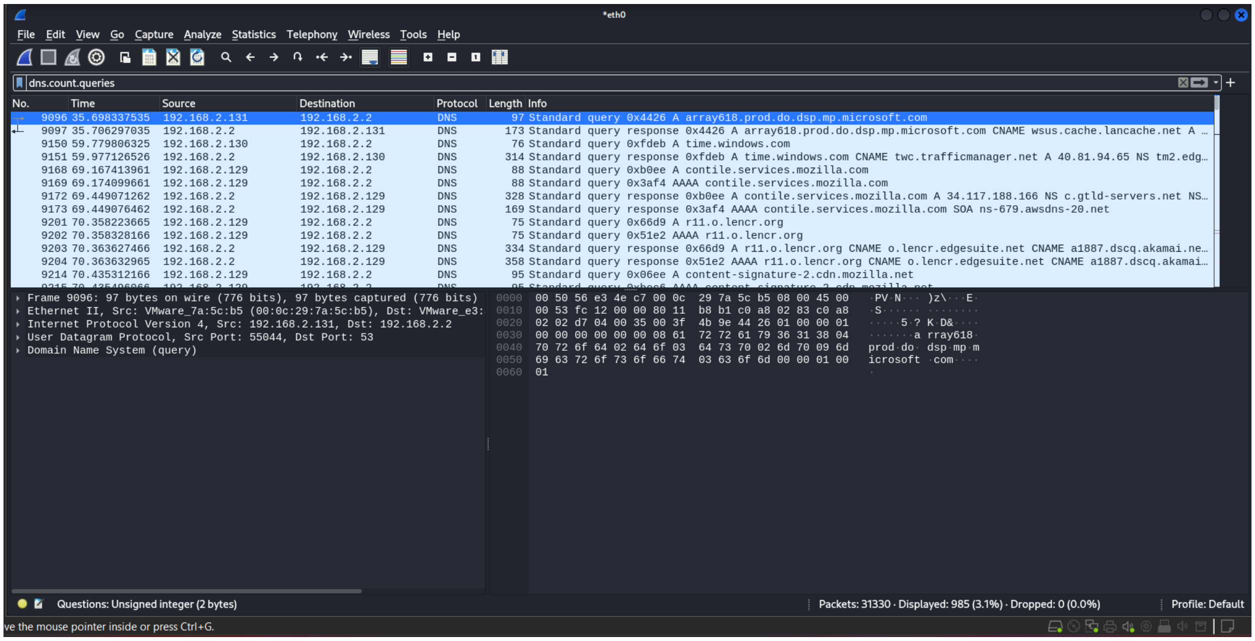
```
Currently scanning: 172.16.228.0/16   |   Screen View: Unique Hosts

48 Captured ARP Req/Rep packets, from 8 hosts.   Total size: 2880
_____________________________________________________________________________
  IP              At MAC Address      Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------

192.168.2.1     00:50:56:c0:00:08       2     120  VMware, Inc.
192.168.2.2     00:50:56:e3:4e:c7      16     960  VMware, Inc.
192.168.2.254   00:50:56:e7:1d:f3       3     180  VMware, Inc.
0.0.0.0         00:0c:29:7a:5c:b5       3     180  VMware, Inc.
192.168.2.131   00:0c:29:7a:5c:b5       6     360  VMware, Inc.
192.168.2.132   00:0c:29:d0:9f:ef       5     300  VMware, Inc.
0.0.0.0         00:0c:29:5e:95:1d       5     300  VMware, Inc.
192.168.2.130   00:0c:29:5e:95:1d       8     480  VMware, Inc.
```

dns= 796



```
dns

No.  Time          Source         Destination    Protocol Length Info
9096 35.698337535  192.168.2.131  192.168.2.2    DNS       97 Standard query 0x4426 A array618.prod.do.dsp.mp.microsoft.com
9097 35.706297035  192.168.2.2    192.168.2.131  DNS      173 Standard query response 0x4426 A array618.prod.do.dsp.mp.microsoft.com CNAME wsus.cache.lancache.net A …
9150 59.779806325  192.168.2.130  192.168.2.2    DNS       76 Standard query 0xfdeb A time.windows.com
9151 59.977126526  192.168.2.2    192.168.2.130  DNS      314 Standard query response 0xfdeb A time.windows.com CNAME twc.trafficmanager.net A 40.81.94.65 NS tm2.edg…
9168 69.167413961  192.168.2.129  192.168.2.2    DNS       88 Standard query 0xb0ee A contile.services.mozilla.com
9169 69.174099661  192.168.2.129  192.168.2.2    DNS       88 Standard query 0x3af4 AAAA contile.services.mozilla.com
9172 69.449071262  192.168.2.2    192.168.2.129  DNS      328 Standard query response 0xb0ee A contile.services.mozilla.com A 34.117.188.166 NS c.gtld-servers.net NS…
9173 69.449076462  192.168.2.2    192.168.2.129  DNS      169 Standard query response 0x3af4 AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net
9201 70.358223665  192.168.2.129  192.168.2.2    DNS       75 Standard query 0x66d9 A r11.o.lencr.org
9202 70.358328166  192.168.2.129  192.168.2.2    DNS       75 Standard query 0x51e2 AAAA r11.o.lencr.org
9203 70.363627466  192.168.2.2    192.168.2.129  DNS      334 Standard query response 0x66d9 A r11.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.ne…
9204 70.363632965  192.168.2.2    192.168.2.129  DNS      358 Standard query response 0x51e2 AAAA r11.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai…
9214 70.435312166  192.168.2.129  192.168.2.2    DNS       95 Standard query 0x06ee A content-signature-2.cdn.mozilla.net
9215 70.435496066  192.168.2.129  192.168.2.2    DNS       95 Standard query 0xbec6 AAAA content-signature-2.cdn.mozilla.net

› Frame 9096: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
› Ethernet II, Src: VMware_7a:5c:b5 (00:0c:29:7a:5c:b5), Dst: VMware_e3:
› Internet Protocol Version 4, Src: 192.168.2.131, Dst: 192.168.2.2
› User Datagram Protocol, Src Port: 55044, Dst Port: 53
› Domain Name System (query)

0000  00 50 56 e3 4e c7 00 0c  29 7a 5c b5 08 00 45 00   ·PV·N··· )z\···E·
0010  00 53 fc 12 00 00 80 11  b8 b1 c0 a8 02 83 c0 a8   ·S······ ········
0020  02 02 d7 04 00 35 00 3f  4b 9e 44 26 01 00 00 01   ·····5·? K·D&····
0030  00 00 00 00 00 00 08 61  72 72 61 79 36 31 38 04   ·······a rray618·
0040  70 72 6f 64 02 64 6f 03  64 73 70 02 6d 70 09 6d   prod·do· dsp·mp·m
0050  69 63 72 6f 73 6f 66 74  03 63 6f 6d 00 00 01 00   icrosoft ·com····
0060  01                                                 ·

Domain Name System: Protocol      Packets: 31330 · Displayed: 796 (2.5%) · Dropped: 0 (0.0%)      Profile: Default
ve the mouse pointer inside or press Ctrl+G.
```

dns.count.queries = 985



```
dns.count.queries
```

```
No.   Time          Source          Destination     Protocol Length Info
 9096 35.698337535  192.168.2.131   192.168.2.2     DNS        97 Standard query 0x4426 A array618.prod.do.dsp.mp.microsoft.com
 9097 35.706297035  192.168.2.2     192.168.2.131   DNS       173 Standard query response 0x4426 A array618.prod.do.dsp.mp.microsoft.com CNAME wsus.cache.lancache.net A …
 9150 59.779806325  192.168.2.130   192.168.2.2     DNS        76 Standard query 0xfdeb A time.windows.com
 9151 59.977126526  192.168.2.2     192.168.2.130   DNS       314 Standard query response 0xfdeb A time.windows.com CNAME twc.trafficmanager.net A 40.81.94.65 NS tm2.edg…
 9168 69.167413961  192.168.2.129   192.168.2.2     DNS        88 Standard query 0xb0ee A contile.services.mozilla.com
 9169 69.174099661  192.168.2.129   192.168.2.2     DNS        88 Standard query 0x3af4 AAAA contile.services.mozilla.com
 9172 69.449071262  192.168.2.2     192.168.2.129   DNS       328 Standard query response 0xb0ee A contile.services.mozilla.com A 34.117.188.166 NS c.gtld-servers.net NS…
 9173 69.449076462  192.168.2.2     192.168.2.129   DNS       169 Standard query response 0x3af4 AAAA contile.services.mozilla.com SOA ns-679.awsdns-20.net
 9201 70.358223665  192.168.2.129   192.168.2.2     DNS        75 Standard query 0x66d9 A r11.o.lencr.org
 9202 70.358328166  192.168.2.129   192.168.2.2     DNS        75 Standard query 0x51e2 AAAA r11.o.lencr.org
 9203 70.363627466  192.168.2.2     192.168.2.129   DNS       334 Standard query response 0x66d9 A r11.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai.ne…
 9204 70.363632965  192.168.2.2     192.168.2.129   DNS       358 Standard query response 0x51e2 AAAA r11.o.lencr.org CNAME o.lencr.edgesuite.net CNAME a1887.dscq.akamai…
 9214 70.435312166  192.168.2.129   192.168.2.2     DNS        95 Standard query 0x06ee A content-signature-2.cdn.mozilla.net
```

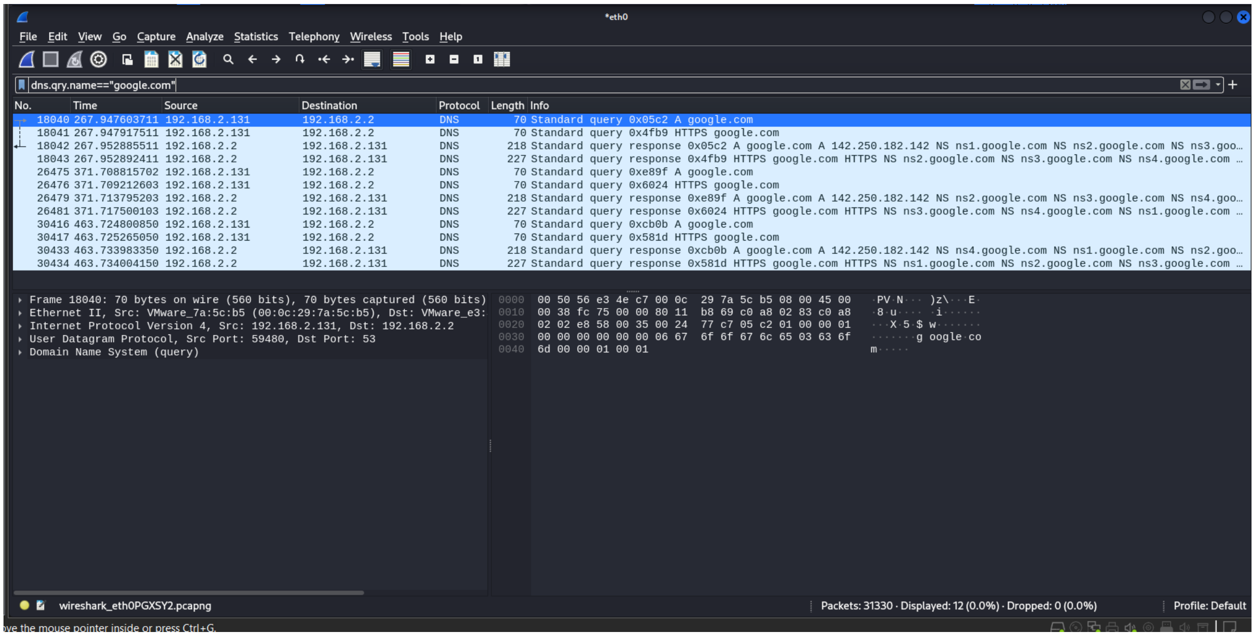
```
› Frame 9096: 97 bytes on wire (776 bits), 97 bytes captured (776 bits)
› Ethernet II, Src: VMware_7a:5c:b5 (00:0c:29:7a:5c:b5), Dst: VMware_e3:
› Internet Protocol Version 4, Src: 192.168.2.131, Dst: 192.168.2.2
› User Datagram Protocol, Src Port: 55044, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 50 56 e3 4e c7 00 0c  29 7a 5c b5 08 00 45 00   ·PV·N··· )z\···E·
0010  00 53 fc 12 00 00 80 11  b8 b1 c0 a8 02 83 c0 a8   ·S······ ········
0020  02 02 d7 04 00 35 00 3f  4b 9e 44 26 01 00 00 01   ·····5·? K·D&····
0030  00 00 00 00 00 00 08 61  72 72 61 79 36 31 38 04   ·······a rray618·
0040  70 72 6f 64 02 64 6f 03  64 73 70 02 6d 70 09 6d   prod·do· dsp·mp·m
0050  69 63 72 6f 73 6f 66 74  03 63 6f 6d 00 00 01 00   icrosoft ·com····
0060  01                                                 ·
```

Questions: Unsigned integer (2 bytes) | Packets: 31330 · Displayed: 985 (3.1%) · Dropped: 0 (0.0%) | Profile: Default

ve the mouse pointer inside or press Ctrl+G.

dns.qry.name == “google.com” – 12



```
dns.qry.name=="google.com"
```

```
No.   Time           Source          Destination     Protocol Length Info
18040 267.947603711  192.168.2.131   192.168.2.2     DNS        70 Standard query 0x05c2 A google.com
18041 267.947917511  192.168.2.131   192.168.2.2     DNS        70 Standard query 0x4fb9 HTTPS google.com
18042 267.952885511  192.168.2.2     192.168.2.131   DNS       218 Standard query response 0x05c2 A google.com A 142.250.182.142 NS ns1.google.com NS ns2.google.com NS ns3.goo…
18043 267.952892411  192.168.2.2     192.168.2.131   DNS       227 Standard query response 0x4fb9 HTTPS google.com HTTPS NS ns2.google.com NS ns3.google.com NS ns4.google.com …
26475 371.708815702  192.168.2.131   192.168.2.2     DNS        70 Standard query 0xe89f A google.com
26476 371.709212603  192.168.2.131   192.168.2.2     DNS        70 Standard query 0x6024 HTTPS google.com
26479 371.713795203  192.168.2.2     192.168.2.131   DNS       218 Standard query response 0xe89f A google.com A 142.250.182.142 NS ns2.google.com NS ns3.google.com NS ns4.goo…
26481 371.717500103  192.168.2.2     192.168.2.131   DNS       227 Standard query response 0x6024 HTTPS google.com HTTPS NS ns3.google.com NS ns4.google.com NS ns1.google.com …
30416 463.724800850  192.168.2.131   192.168.2.2     DNS        70 Standard query 0xcb0b A google.com
30417 463.725265050  192.168.2.131   192.168.2.2     DNS        70 Standard query 0x581d HTTPS google.com
30433 463.733983350  192.168.2.2     192.168.2.131   DNS       218 Standard query response 0xcb0b A google.com A 142.250.182.142 NS ns4.google.com NS ns1.google.com NS ns2.goo…
30434 463.734004150  192.168.2.2     192.168.2.131   DNS       227 Standard query response 0x581d HTTPS google.com HTTPS NS ns1.google.com NS ns2.google.com NS ns3.google.com …
```

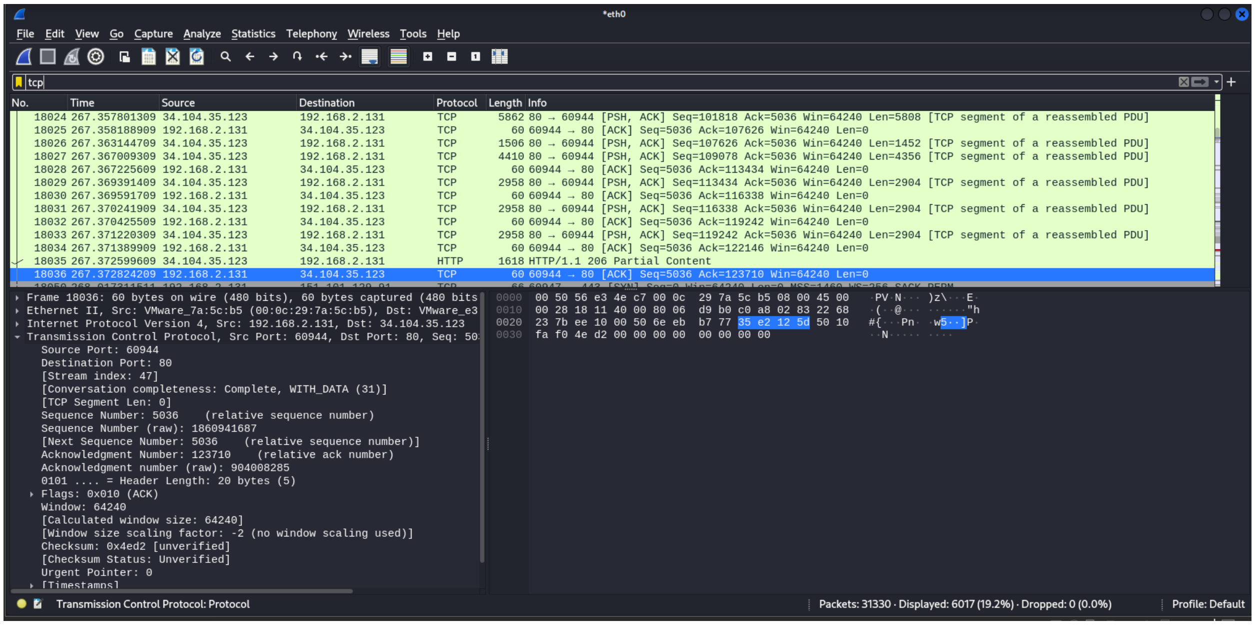
```
› Frame 18040: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
› Ethernet II, Src: VMware_7a:5c:b5 (00:0c:29:7a:5c:b5), Dst: VMware_e3:
› Internet Protocol Version 4, Src: 192.168.2.131, Dst: 192.168.2.2
› User Datagram Protocol, Src Port: 59480, Dst Port: 53
› Domain Name System (query)
```

```
0000  00 50 56 e3 4e c7 00 0c  29 7a 5c b5 08 00 45 00   ·PV·N··· )z\···E·
0010  00 38 fc 75 00 00 80 11  b8 69 c0 a8 02 83 c0 a8   ·8·u···· ·i······
0020  02 02 e8 58 00 35 00 24  77 c7 05 c2 01 00 00 01   ···X·5·$ w·······
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f   ·······g oogle·co
0040  6d 00 00 01 00 01                                  m·····
```

wireshark_eth0PGXSY2.pcapng | Packets: 31330 · Displayed: 12 (0.0%) · Dropped: 0 (0.0%) | Profile: Default

ve the mouse pointer inside or press Ctrl+G.

tcp – 6017


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp
```

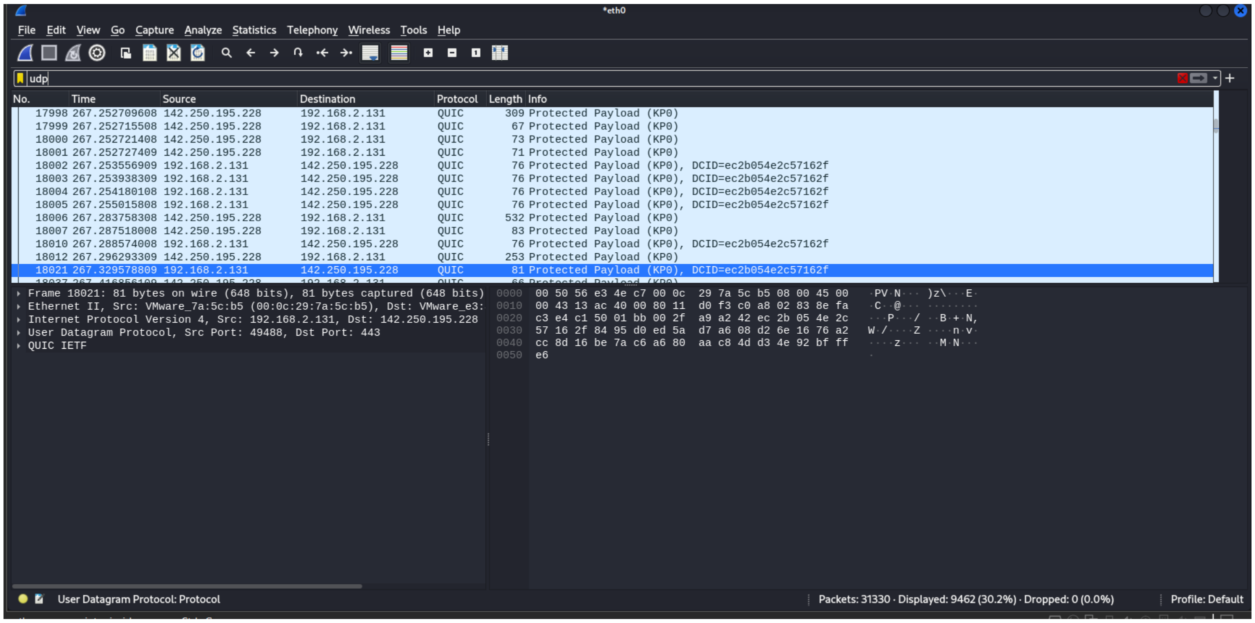
```
No.   Time          Source          Destination     Protocol Length Info
18024 267.357801309 34.104.35.123   192.168.2.131   TCP      5862 80 → 60944 [PSH, ACK] Seq=101818 Ack=5036 Win=64240 Len=5808 [TCP segment of a reassembled PDU]
18025 267.358188909 192.168.2.131   34.104.35.123   TCP        60 60944 → 80 [ACK] Seq=5036 Ack=107626 Win=64240 Len=0
18026 267.363144709 34.104.35.123   192.168.2.131   TCP      1506 80 → 60944 [PSH, ACK] Seq=107626 Ack=5036 Win=64240 Len=1452 [TCP segment of a reassembled PDU]
18027 267.367009309 34.104.35.123   192.168.2.131   TCP      4410 80 → 60944 [PSH, ACK] Seq=109078 Ack=5036 Win=64240 Len=4356 [TCP segment of a reassembled PDU]
18028 267.367225609 192.168.2.131   34.104.35.123   TCP        60 60944 → 80 [ACK] Seq=5036 Ack=113434 Win=64240 Len=0
18029 267.369391409 34.104.35.123   192.168.2.131   TCP      2958 80 → 60944 [PSH, ACK] Seq=113434 Ack=5036 Win=64240 Len=2904 [TCP segment of a reassembled PDU]
18030 267.369591709 192.168.2.131   34.104.35.123   TCP        60 60944 → 80 [ACK] Seq=5036 Ack=116338 Win=64240 Len=0
18031 267.370241909 34.104.35.123   192.168.2.131   TCP      2958 80 → 60944 [PSH, ACK] Seq=116338 Ack=5036 Win=64240 Len=2904 [TCP segment of a reassembled PDU]
18032 267.370425509 192.168.2.131   34.104.35.123   TCP        60 60944 → 80 [ACK] Seq=5036 Ack=119242 Win=64240 Len=0
18033 267.371220309 34.104.35.123   192.168.2.131   TCP      2958 80 → 60944 [PSH, ACK] Seq=119242 Ack=5036 Win=64240 Len=2904 [TCP segment of a reassembled PDU]
18034 267.371389909 192.168.2.131   34.104.35.123   TCP        60 60944 → 80 [ACK] Seq=5036 Ack=122146 Win=64240 Len=0
18035 267.372599609 34.104.35.123   192.168.2.131   HTTP     1618 HTTP/1.1 206 Partial Content
18036 267.372824209 192.168.2.131   34.104.35.123   TCP        60 60944 → 80 [ACK] Seq=5036 Ack=123710 Win=64240 Len=0
```

```
› Frame 18036: 60 bytes on wire (480 bits), 60 bytes captured (480 bits
› Ethernet II, Src: VMware_7a:5c:b5 (00:0c:29:7a:5c:b5), Dst: VMware_e3
› Internet Protocol Version 4, Src: 192.168.2.131, Dst: 34.104.35.123
⌄ Transmission Control Protocol, Src Port: 60944, Dst Port: 80, Seq: 50
    Source Port: 60944
    Destination Port: 80
    [Stream index: 47]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 5036    (relative sequence number)
    Sequence Number (raw): 1860941687
    [Next Sequence Number: 5036    (relative sequence number)]
    Acknowledgment Number: 123710    (relative ack number)
    Acknowledgment number (raw): 904008285
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x010 (ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x4ed2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
```

```
0000  00 50 56 e3 4e c7 00 0c  29 7a 5c b5 08 00 45 00   ·PV·N···)z\···E·
0010  00 28 18 11 40 00 80 06  d9 b0 c0 a8 02 83 22 68   ·(··@·········"h
0020  23 7b ee 10 00 50 6e eb  b7 77 35 e2 12 5d 50 10   #{···Pn··w5··]P·
0030  fa f0 4e d2 00 00 00 00  00 00 00 00               ··N·········
```

```
Transmission Control Protocol: Protocol          Packets: 31330 · Displayed: 6017 (19.2%) · Dropped: 0 (0.0%)          Profile: Default
```

udp – 9462


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp
```

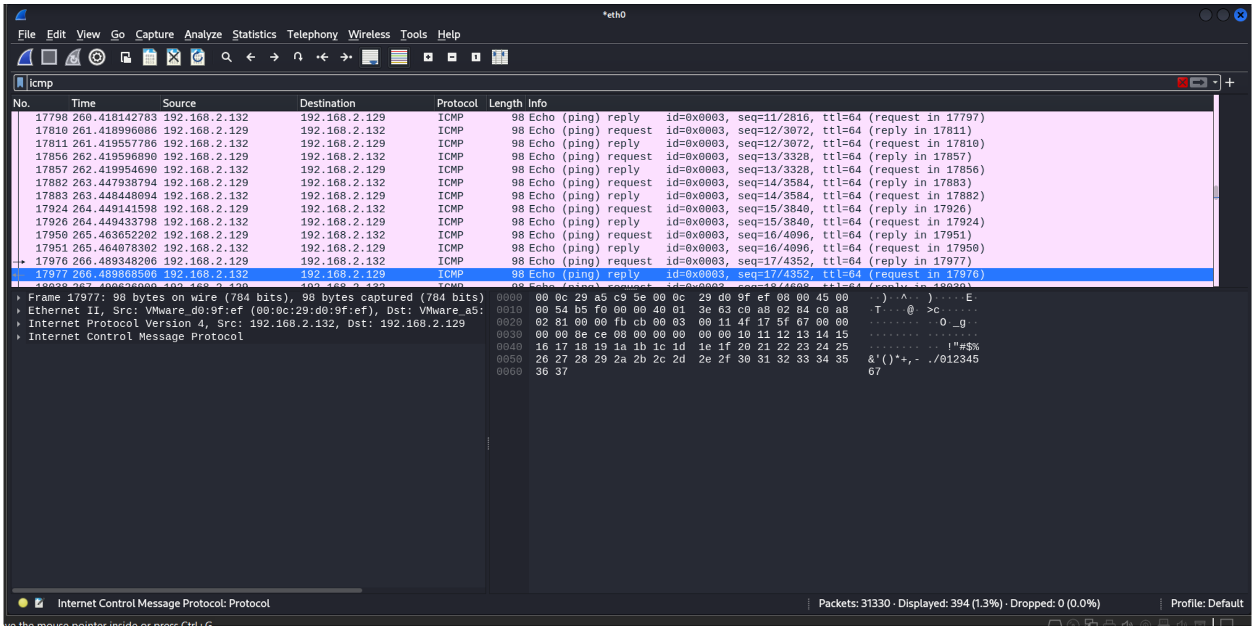
```
No.   Time          Source          Destination     Protocol Length Info
17998 267.252709608 142.250.195.228 192.168.2.131   QUIC      309 Protected Payload (KP0)
17999 267.252715508 142.250.195.228 192.168.2.131   QUIC       67 Protected Payload (KP0)
18000 267.252721408 142.250.195.228 192.168.2.131   QUIC       73 Protected Payload (KP0)
18001 267.252727409 142.250.195.228 192.168.2.131   QUIC       71 Protected Payload (KP0)
18002 267.253556909 192.168.2.131   142.250.195.228 QUIC       76 Protected Payload (KP0), DCID=ec2b054e2c57162f
18003 267.253938309 192.168.2.131   142.250.195.228 QUIC       76 Protected Payload (KP0), DCID=ec2b054e2c57162f
18004 267.254180108 192.168.2.131   142.250.195.228 QUIC       76 Protected Payload (KP0), DCID=ec2b054e2c57162f
18005 267.255015808 192.168.2.131   142.250.195.228 QUIC       76 Protected Payload (KP0), DCID=ec2b054e2c57162f
18006 267.283758308 142.250.195.228 192.168.2.131   QUIC      532 Protected Payload (KP0)
18007 267.287518008 142.250.195.228 192.168.2.131   QUIC       83 Protected Payload (KP0)
18010 267.288574008 192.168.2.131   142.250.195.228 QUIC       76 Protected Payload (KP0), DCID=ec2b054e2c57162f
18012 267.296293309 142.250.195.228 192.168.2.131   QUIC      253 Protected Payload (KP0)
18021 267.329578809 192.168.2.131   142.250.195.228 QUIC       81 Protected Payload (KP0), DCID=ec2b054e2c57162f
```

```
› Frame 18021: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
› Ethernet II, Src: VMware_7a:5c:b5 (00:0c:29:7a:5c:b5), Dst: VMware_e3:
› Internet Protocol Version 4, Src: 192.168.2.131, Dst: 142.250.195.228
› User Datagram Protocol, Src Port: 49488, Dst Port: 443
› QUIC IETF
```

```
0000  00 50 56 e3 4e c7 00 0c  29 7a 5c b5 08 00 45 00   ·PV·N···)z\···E·
0010  00 43 13 ac 40 00 80 11  d0 f3 c0 a8 02 83 8e fa   ·C··@···········
0020  c3 e4 c1 50 01 bb 00 2f  a9 a2 42 ec 2b 05 4e 2c   ···P···/··B·+·N,
0030  57 16 2f 84 95 d0 ed 5a  d7 a6 08 d2 6e 16 76 a2   W·/····Z····n·v·
0040  cc 8d 16 be 7a c6 a6 80  aa c8 4d d3 4e 92 bf ff   ····z·····M·N···
0050  e6                                                 ·
```

```
User Datagram Protocol: Protocol          Packets: 31330 · Displayed: 9462 (30.2%) · Dropped: 0 (0.0%)          Profile: Default
```

icmp – 394


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

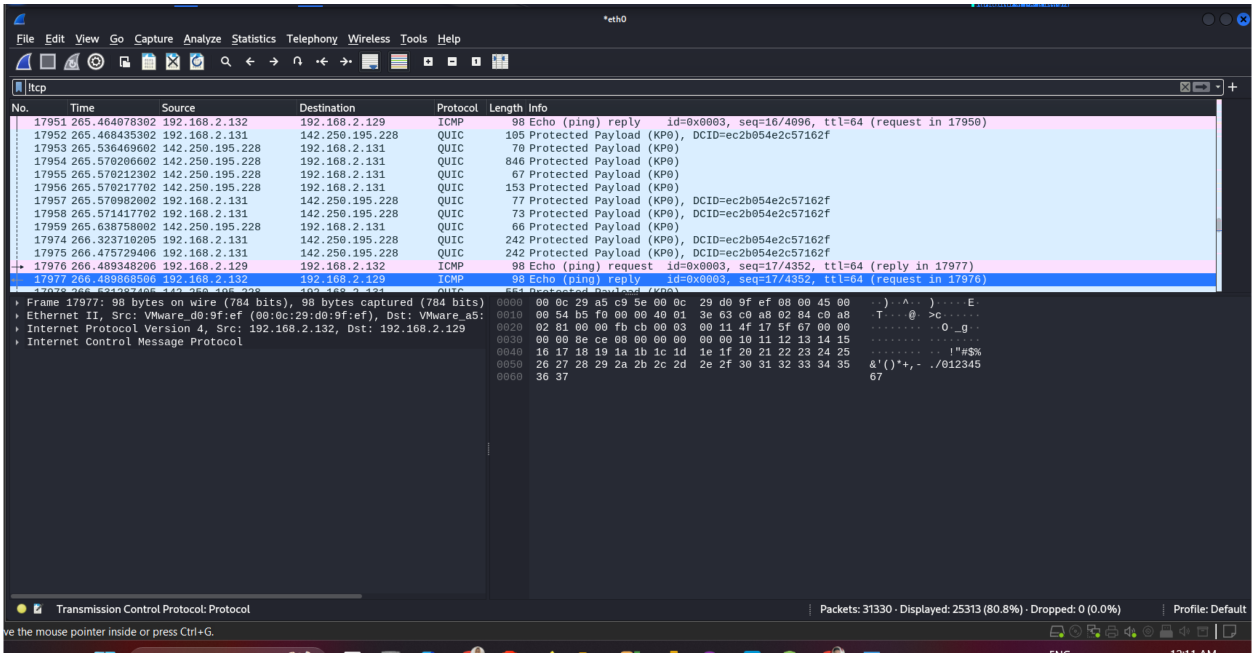
```
No.   Time          Source         Destination    Protocol Length Info
17798 260.418142783 192.168.2.132  192.168.2.129  ICMP     98 Echo (ping) reply    id=0x0003, seq=11/2816, ttl=64 (request in 17797)
17810 261.418996086 192.168.2.129  192.168.2.132  ICMP     98 Echo (ping) request  id=0x0003, seq=12/3072, ttl=64 (reply in 17811)
17811 261.419557786 192.168.2.132  192.168.2.129  ICMP     98 Echo (ping) reply    id=0x0003, seq=12/3072, ttl=64 (request in 17810)
17856 262.419596890 192.168.2.129  192.168.2.132  ICMP     98 Echo (ping) request  id=0x0003, seq=13/3328, ttl=64 (reply in 17857)
17857 262.419954690 192.168.2.132  192.168.2.129  ICMP     98 Echo (ping) reply    id=0x0003, seq=13/3328, ttl=64 (request in 17856)
17882 263.447938794 192.168.2.129  192.168.2.132  ICMP     98 Echo (ping) request  id=0x0003, seq=14/3584, ttl=64 (reply in 17883)
17883 263.448448094 192.168.2.132  192.168.2.129  ICMP     98 Echo (ping) reply    id=0x0003, seq=14/3584, ttl=64 (request in 17882)
17924 264.449141598 192.168.2.129  192.168.2.132  ICMP     98 Echo (ping) request  id=0x0003, seq=15/3840, ttl=64 (reply in 17926)
17926 264.449433798 192.168.2.132  192.168.2.129  ICMP     98 Echo (ping) reply    id=0x0003, seq=15/3840, ttl=64 (request in 17924)
17950 265.463652202 192.168.2.129  192.168.2.132  ICMP     98 Echo (ping) request  id=0x0003, seq=16/4096, ttl=64 (reply in 17951)
17951 265.464078302 192.168.2.132  192.168.2.129  ICMP     98 Echo (ping) reply    id=0x0003, seq=16/4096, ttl=64 (request in 17950)
17976 266.489348206 192.168.2.129  192.168.2.132  ICMP     98 Echo (ping) request  id=0x0003, seq=17/4352, ttl=64 (reply in 17977)
17977 266.489868506 192.168.2.132  192.168.2.129  ICMP     98 Echo (ping) reply    id=0x0003, seq=17/4352, ttl=64 (request in 17976)
```

```
› Frame 17977: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
› Ethernet II, Src: VMware_d0:9f:ef (00:0c:29:d0:9f:ef), Dst: VMware_a5:
› Internet Protocol Version 4, Src: 192.168.2.132, Dst: 192.168.2.129
› Internet Control Message Protocol
```

```
0000  00 0c 29 a5 c9 5e 00 0c  29 d0 9f ef 08 00 45 00   ··)··^·· )·····E·
0010  00 54 b5 f0 00 00 40 01  3e 63 c0 a8 02 84 c0 a8   ·T····@· >c······
0020  02 81 00 00 fb cb 00 03  00 11 4f 17 5f 67 00 00   ········ ··O·_g··
0030  00 00 8e ce 08 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Internet Control Message Protocol: Protocol | Packets: 31330 · Displayed: 394 (1.3%) · Dropped: 0 (0.0%) | Profile: Default

!tcp – 25313


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

!tcp

```
No.   Time          Source          Destination     Protocol Length Info
17951 265.464078302 192.168.2.132   192.168.2.129   ICMP     98 Echo (ping) reply    id=0x0003, seq=16/4096, ttl=64 (request in 17950)
17952 265.468435302 192.168.2.131   142.250.195.228 QUIC    105 Protected Payload (KP0), DCID=ec2b054e2c57162f
17953 265.536469602 142.250.195.228 192.168.2.131   QUIC     70 Protected Payload (KP0)
17954 265.570206602 142.250.195.228 192.168.2.131   QUIC    846 Protected Payload (KP0)
17955 265.570212302 142.250.195.228 192.168.2.131   QUIC     67 Protected Payload (KP0)
17956 265.570217702 142.250.195.228 192.168.2.131   QUIC    153 Protected Payload (KP0)
17957 265.570982002 192.168.2.131   142.250.195.228 QUIC     77 Protected Payload (KP0), DCID=ec2b054e2c57162f
17958 265.571417702 192.168.2.131   142.250.195.228 QUIC     73 Protected Payload (KP0), DCID=ec2b054e2c57162f
17959 265.638758002 142.250.195.228 192.168.2.131   QUIC     66 Protected Payload (KP0)
17974 266.323710205 192.168.2.131   142.250.195.228 QUIC    242 Protected Payload (KP0), DCID=ec2b054e2c57162f
17975 266.475729406 192.168.2.131   142.250.195.228 QUIC    242 Protected Payload (KP0), DCID=ec2b054e2c57162f
17976 266.489348206 192.168.2.129   192.168.2.132   ICMP     98 Echo (ping) request  id=0x0003, seq=17/4352, ttl=64 (reply in 17977)
17977 266.489868506 192.168.2.132   192.168.2.129   ICMP     98 Echo (ping) reply    id=0x0003, seq=17/4352, ttl=64 (request in 17976)
```

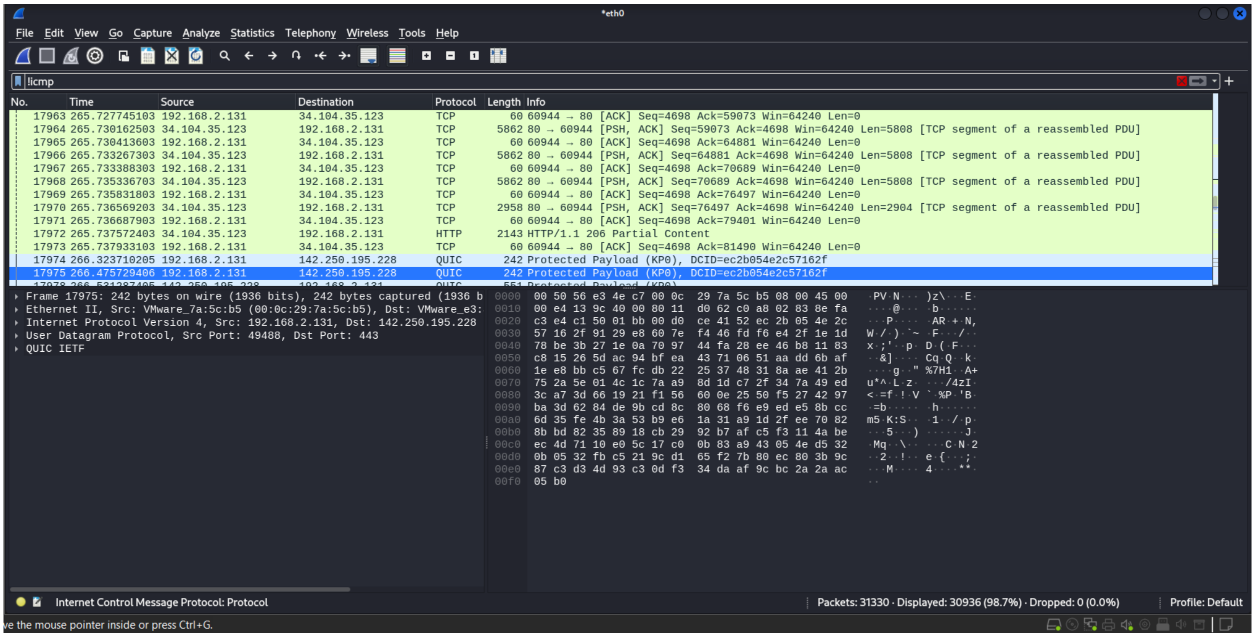
```
› Frame 17977: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
› Ethernet II, Src: VMware_d0:9f:ef (00:0c:29:d0:9f:ef), Dst: VMware_a5:
› Internet Protocol Version 4, Src: 192.168.2.132, Dst: 192.168.2.129
› Internet Control Message Protocol
```

```
0000  00 0c 29 a5 c9 5e 00 0c  29 d0 9f ef 08 00 45 00   ··)··^·· )·····E·
0010  00 54 b5 f0 00 00 40 01  3e 63 c0 a8 02 84 c0 a8   ·T····@· >c······
0020  02 81 00 00 fb cb 00 03  00 11 4f 17 5f 67 00 00   ········ ··O·_g··
0030  00 00 8e ce 08 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Transmission Control Protocol: Protocol | Packets: 31330 · Displayed: 25313 (80.8%) · Dropped: 0 (0.0%) | Profile: Default

ve the mouse pointer inside or press Ctrl+G.

!icmp – 30936



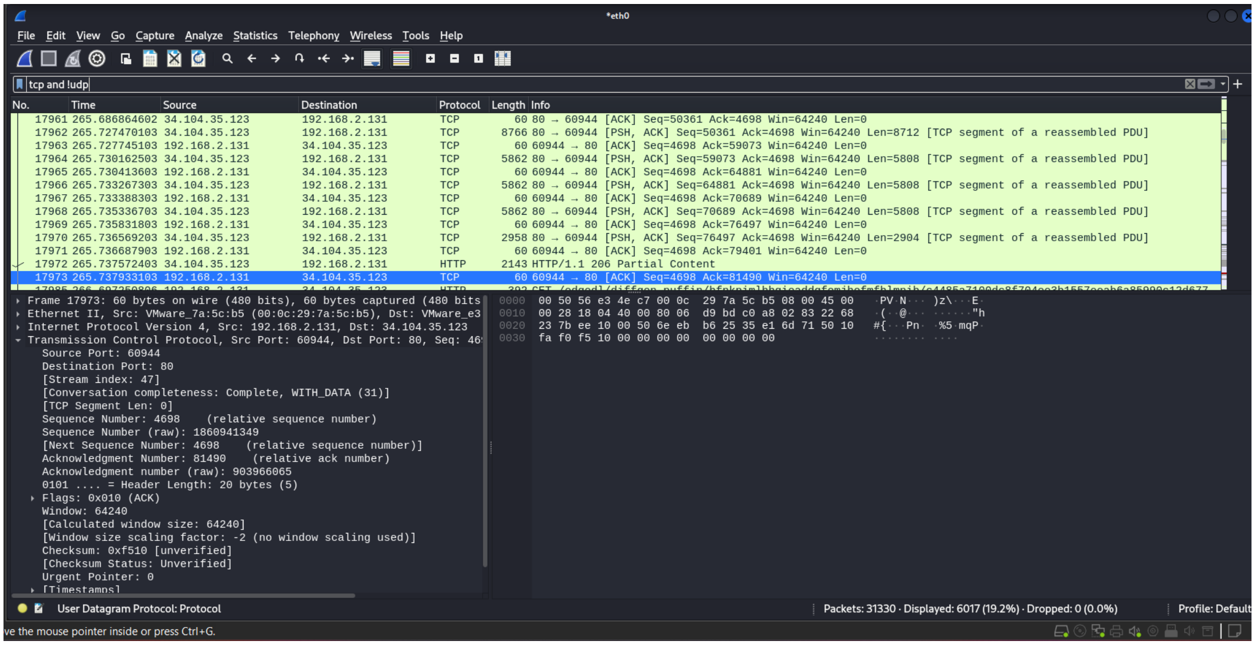
```
!icmp

No.   Time           Source          Destination      Protocol Length Info
17963 265.727745103 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=59073 Win=64240 Len=0
17964 265.730162503 34.104.35.123   192.168.2.131    TCP      5862 80 → 60944 [PSH, ACK] Seq=59073 Ack=4698 Win=64240 Len=5808 [TCP segment of a reassembled PDU]
17965 265.730413603 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=64881 Win=64240 Len=0
17966 265.733267303 34.104.35.123   192.168.2.131    TCP      5862 80 → 60944 [PSH, ACK] Seq=64881 Ack=4698 Win=64240 Len=5808 [TCP segment of a reassembled PDU]
17967 265.733388303 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=70689 Win=64240 Len=0
17968 265.735336703 34.104.35.123   192.168.2.131    TCP      5862 80 → 60944 [PSH, ACK] Seq=70689 Ack=4698 Win=64240 Len=5808 [TCP segment of a reassembled PDU]
17969 265.735831803 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=76497 Win=64240 Len=0
17970 265.736569203 34.104.35.123   192.168.2.131    TCP      2958 80 → 60944 [PSH, ACK] Seq=76497 Ack=4698 Win=64240 Len=2904 [TCP segment of a reassembled PDU]
17971 265.736687903 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=79401 Win=64240 Len=0
17972 265.737572403 34.104.35.123   192.168.2.131    HTTP     2143 HTTP/1.1 206 Partial Content
17973 265.737933103 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=81490 Win=64240 Len=0
17974 266.323710205 192.168.2.131   142.250.195.228  QUIC      242 Protected Payload (KP0), DCID=ec2b054e2c57162f
17975 266.475729406 192.168.2.131   142.250.195.228  QUIC      242 Protected Payload (KP0), DCID=ec2b054e2c57162f
```

```
› Frame 17975: 242 bytes on wire (1936 bits), 242 bytes captured (1936 b
› Ethernet II, Src: VMware_7a:5c:b5 (00:0c:29:7a:5c:b5), Dst: VMware_e3:
› Internet Protocol Version 4, Src: 192.168.2.131, Dst: 142.250.195.228
› User Datagram Protocol, Src Port: 49488, Dst Port: 443
› QUIC IETF
```

```
0000  00 50 56 e3 4e c7 00 0c  29 7a 5c b5 08 00 45 00   ·PV·N···)z\···E·
0010  00 e4 13 9c 40 00 80 11  d0 62 c0 a8 02 83 8e fa   ····@····b······
0020  c3 e4 c1 50 01 bb 00 d0  ce 41 52 ec 2b 05 4e 2c   ···P·····AR·+·N,
0030  57 16 2f 91 29 e8 60 7e  f4 46 fd f6 e4 2f 1e 1d   W·/·)·`~·F···/··
0040  78 be 3b 27 1e 0a 70 97  44 fa 28 ee 46 b8 11 83   x·;'··p·D·(·F···
0050  c8 15 26 5d ac 94 bf ea  43 71 06 51 aa dd 6b af   ··&]····Cq·Q··k·
0060  1e e8 bb c5 67 fc db 22  25 37 48 31 8a ae 41 2b   ····g··"%7H1··A+
0070  75 2a 5e 01 4c 1c 7a a9  8d 1d c7 2f 34 7a 49 ed   u*^·L·z····/4zI·
0080  3c a7 3d 66 19 21 f1 56  60 0e 25 50 f5 27 42 97   <·=f·!·V`·%P·'B·
0090  ba 3d 62 84 de 9b cd 8c  80 68 f6 e9 ed e5 8b cc   ·=b······h······
00a0  6d 35 fe 4b 3a 53 b9 e6  1a 31 a9 1d 2f ee 70 82   m5·K:S···1··/·p·
00b0  8b bd 82 35 89 18 cb 29  92 b7 af c5 f3 11 4a be   ···5···)······J·
00c0  ec 4d 71 10 e0 5c 17 c0  0b 83 a9 43 05 4e d5 32   ·Mq··\·····C·N·2
00d0  0b 05 32 fb c5 21 9c d1  65 f2 7b 80 ec 80 3b 9c   ··2··!··e·{···;·
00e0  87 c3 d3 4d 93 c3 0d f3  34 da af 9c bc 2a 2a ac   ···M····4····**·
00f0  05 b0                                              ··
```

```
Internet Control Message Protocol: Protocol    Packets: 31330 · Displayed: 30936 (98.7%) · Dropped: 0 (0.0%)    Profile: Default
ve the mouse pointer inside or press Ctrl+G.
```

tcp and !udp – 6017



```
tcp and !udp

No.   Time           Source          Destination      Protocol Length Info
17961 265.686864602 34.104.35.123   192.168.2.131    TCP        60 80 → 60944 [ACK] Seq=50361 Ack=4698 Win=64240 Len=0
17962 265.727470103 34.104.35.123   192.168.2.131    TCP      8766 80 → 60944 [PSH, ACK] Seq=50361 Ack=4698 Win=64240 Len=8712 [TCP segment of a reassembled PDU]
17963 265.727745103 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=59073 Win=64240 Len=0
17964 265.730162503 34.104.35.123   192.168.2.131    TCP      5862 80 → 60944 [PSH, ACK] Seq=59073 Ack=4698 Win=64240 Len=5808 [TCP segment of a reassembled PDU]
17965 265.730413603 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=64881 Win=64240 Len=0
17966 265.733267303 34.104.35.123   192.168.2.131    TCP      5862 80 → 60944 [PSH, ACK] Seq=64881 Ack=4698 Win=64240 Len=5808 [TCP segment of a reassembled PDU]
17967 265.733388303 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=70689 Win=64240 Len=0
17968 265.735336703 34.104.35.123   192.168.2.131    TCP      5862 80 → 60944 [PSH, ACK] Seq=70689 Ack=4698 Win=64240 Len=5808 [TCP segment of a reassembled PDU]
17969 265.735831803 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=76497 Win=64240 Len=0
17970 265.736569203 34.104.35.123   192.168.2.131    TCP      2958 80 → 60944 [PSH, ACK] Seq=76497 Ack=4698 Win=64240 Len=2904 [TCP segment of a reassembled PDU]
17971 265.736687903 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=79401 Win=64240 Len=0
17972 265.737572403 34.104.35.123   192.168.2.131    HTTP     2143 HTTP/1.1 206 Partial Content
17973 265.737933103 192.168.2.131   34.104.35.123    TCP        60 60944 → 80 [ACK] Seq=4698 Ack=81490 Win=64240 Len=0
```

```
› Frame 17973: 60 bytes on wire (480 bits), 60 bytes captured (480 bits
› Ethernet II, Src: VMware_7a:5c:b5 (00:0c:29:7a:5c:b5), Dst: VMware_e3
› Internet Protocol Version 4, Src: 192.168.2.131, Dst: 34.104.35.123
⌄ Transmission Control Protocol, Src Port: 60944, Dst Port: 80, Seq: 46
    Source Port: 60944
    Destination Port: 80
    [Stream index: 47]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 4698    (relative sequence number)
    Sequence Number (raw): 1860941349
    [Next Sequence Number: 4698    (relative sequence number)]
    Acknowledgment Number: 81490    (relative ack number)
    Acknowledgment number (raw): 903966065
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x010 (ACK)
    Window: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xf510 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
```

```
0000  00 50 56 e3 4e c7 00 0c  29 7a 5c b5 08 00 45 00   ·PV·N···)z\···E·
0010  00 28 18 04 40 00 80 06  d9 bd c0 a8 02 83 22 68   ·(··@·········"h
0020  23 7b ee 10 00 50 6e eb  b6 25 35 e1 6d 71 50 10   #{···Pn··%5·mqP·
0030  fa f0 f5 10 00 00 00 00  00 00 00 00               ········ ····
```

```
User Datagram Protocol: Protocol    Packets: 31330 · Displayed: 6017 (19.2%) · Dropped: 0 (0.0%)    Profile: Default
ve the mouse pointer inside or press Ctrl+G.
```