COMPUTER NETWORK

LAB ASSIGNMENT 4

Submitted By:

Name: AKSHAT SAHU

Roll No: U22CS034

Branch: CSE

Semester: 4th Sem

Division : A

Department of Computer Science and Engineering

SV NATIONAL INSTITUTE OF TECHNOLOGY SURAT

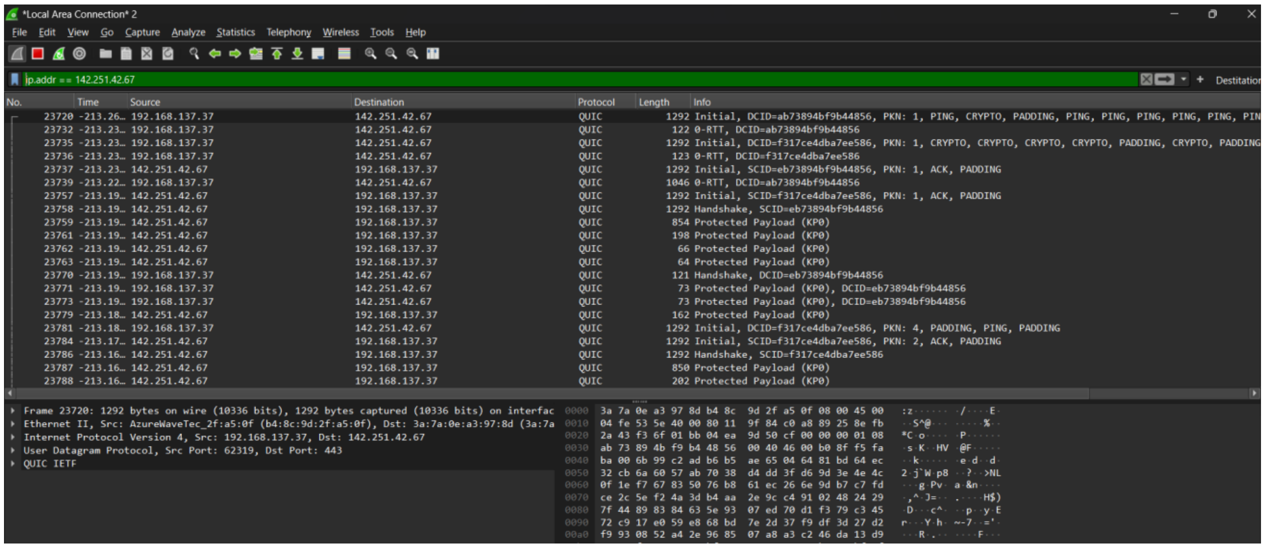
2024

Wireshark is a popular network protocol analyzer that allows you to capture and inspect data traveling back and forth on a network in real-time. Filters in Wireshark help you focus on specific packets of interest and analyze network traffic more effectively. Here are 20 Wireshark filters and their applications:

1. ip.addr == x.x.x.x

   - Application: Filters packets based on source or destination IP address.

   - Example: `ip.addr == 142.251.42.67`

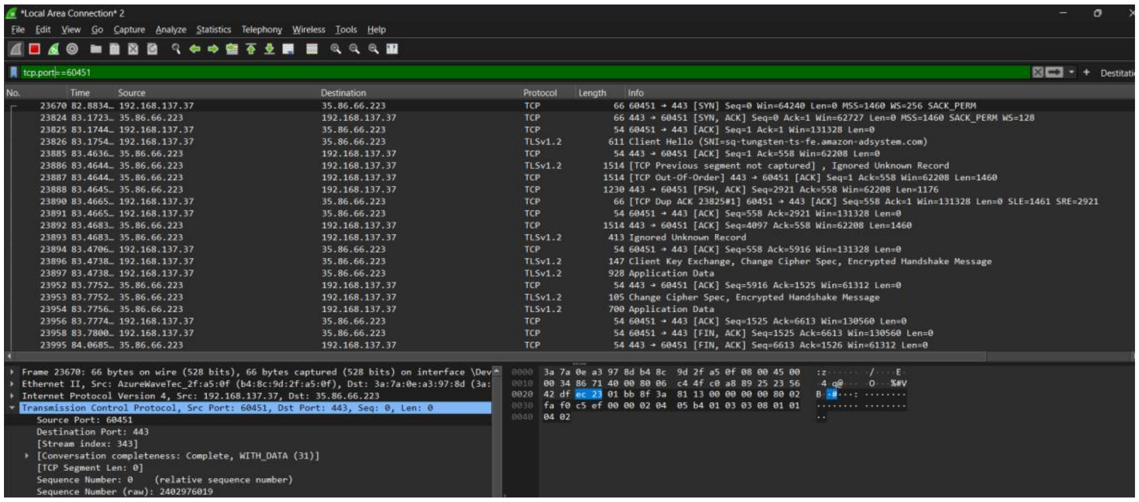

Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Destitation

```
ip.addr == 142.251.42.67

No.    Time       Source           Destination      Protocol  Length  Info
23720 -213.26…  192.168.137.37   142.251.42.67    QUIC      1292 Initial, DCID=ab73894bf9b44856, PKN: 1, PING, CRYPTO, PADDING, PING, PING, PING, PING, PING, PIN
23732 -213.23…  192.168.137.37   142.251.42.67    QUIC       122 0-RTT, DCID=ab73894bf9b44856
23735 -213.23…  192.168.137.37   142.251.42.67    QUIC      1292 Initial, DCID=f317ce4dba7ee586, PKN: 1, CRYPTO, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, PADDING
23736 -213.23…  192.168.137.37   142.251.42.67    QUIC       123 0-RTT, DCID=f317ce4dba7ee586
23737 -213.23…  142.251.42.67    192.168.137.37   QUIC      1292 Initial, SCID=eb73894bf9b44856, PKN: 1, ACK, PADDING
23739 -213.22…  192.168.137.37   142.251.42.67    QUIC      1046 0-RTT, DCID=ab73894bf9b44856
23757 -213.19…  142.251.42.67    192.168.137.37   QUIC      1292 Initial, SCID=f317ce4dba7ee586, PKN: 1, ACK, PADDING
23758 -213.19…  142.251.42.67    192.168.137.37   QUIC      1292 Handshake, SCID=eb73894bf9b44856
23759 -213.19…  142.251.42.67    192.168.137.37   QUIC       854 Protected Payload (KP0)
23761 -213.19…  142.251.42.67    192.168.137.37   QUIC       198 Protected Payload (KP0)
23762 -213.19…  142.251.42.67    192.168.137.37   QUIC        66 Protected Payload (KP0)
23763 -213.19…  142.251.42.67    192.168.137.37   QUIC        64 Protected Payload (KP0)
23770 -213.19…  192.168.137.37   142.251.42.67    QUIC       121 Handshake, DCID=eb73894bf9b44856
23771 -213.19…  192.168.137.37   142.251.42.67    QUIC        73 Protected Payload (KP0), DCID=eb73894bf9b44856
23773 -213.19…  192.168.137.37   142.251.42.67    QUIC        73 Protected Payload (KP0), DCID=eb73894bf9b44856
23779 -213.18…  142.251.42.67    192.168.137.37   QUIC       162 Protected Payload (KP0)
23781 -213.18…  192.168.137.37   142.251.42.67    QUIC      1292 Initial, DCID=f317ce4dba7ee586, PKN: 4, PADDING, PING, PADDING
23784 -213.17…  142.251.42.67    192.168.137.37   QUIC      1292 Initial, SCID=f317ce4dba7ee586, PKN: 2, ACK, PADDING
23786 -213.16…  142.251.42.67    192.168.137.37   QUIC      1292 Handshake, SCID=f317ce4dba7ee586
23787 -213.16…  142.251.42.67    192.168.137.37   QUIC       850 Protected Payload (KP0)
23788 -213.16…  142.251.42.67    192.168.137.37   QUIC       202 Protected Payload (KP0)

▸ Frame 23720: 1292 bytes on wire (10336 bits), 1292 bytes captured (10336 bits) on interfac
▸ Ethernet II, Src: AzureWaveTec_2f:a5:0f (b4:8c:9d:2f:a5:0f), Dst: 3a:7a:0e:a3:97:8d (3a:7a
▸ Internet Protocol Version 4, Src: 192.168.137.37, Dst: 142.251.42.67
▸ User Datagram Protocol, Src Port: 62319, Dst Port: 443
▸ QUIC IETF

0000  3a 7a 0e a3 97 8d b4 8c  9d 2f a5 0f 08 00 45 00   :z······ ·/····E·
0010  04 fe 53 5e 40 00 80 11  9f 84 c0 a8 89 25 8e fb   ··S^@··· ·····%··
0020  2a 43 f3 6f 01 bb 04 ea  9d 50 cf 00 00 00 01 08   *C·o···· ·P······
0030  ab 73 89 4b f9 b4 48 56  00 40 46 00 b0 8f f5 fa   ·s·K··HV ·@F·····
0040  ba 00 6b 99 c2 ad b6 b5  ae 65 04 64 81 bd 64 ec   ··k····· ·e·d··d·
0050  32 cb 6a 60 57 ab 70 38  d4 dd 3f d6 9d 3e 4e 4c   2·j`W·p8 ··?··>NL
0060  0f 1e f7 67 83 50 76 b8  61 ec 26 6e 9d b7 c7 fd   ···g·Pv· a·&n····
0070  ce 2c 5e f2 4a 3d b4 aa  2e 9c c4 91 02 48 24 29   ·,^·J=·· .····H$)
0080  7f 44 89 83 84 63 5e 93  07 ed 70 d1 f3 79 c3 45   ·D···c^· ··p··y·E
0090  72 c9 17 e0 59 e8 68 bd  7e 2d 37 f9 df 3d 27 d2   r···Y·h· ~-7··='·
00a0  f9 93 08 52 a4 2e 96 85  07 a8 a3 c2 46 da 13 d9   ···R·.·· ····F···
```

2. tcp.port == xx

   - Application: Filters TCP packets based on source or destination port number.

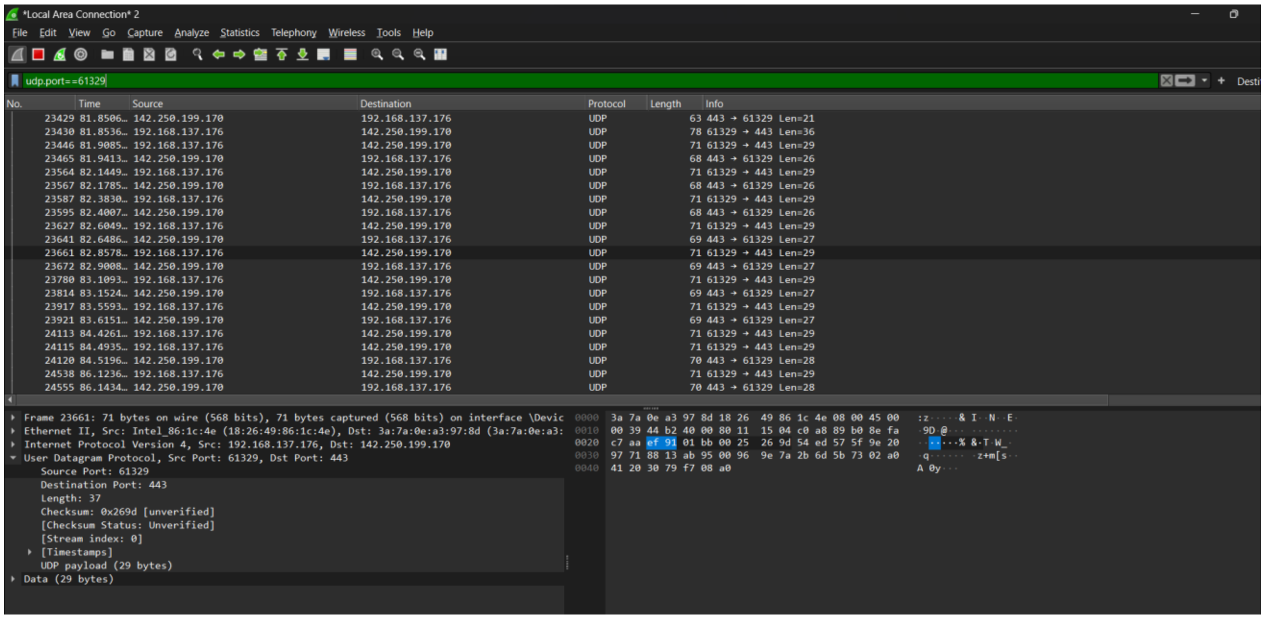
   - Example: `tcp.port == 80`


Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Destitati

```
tcp.port==60451

No.    Time       Source           Destination      Protocol  Length  Info
23670 82.8834…  192.168.137.37   35.86.66.223     TCP         66 60451 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
23824 83.1723…  35.86.66.223     192.168.137.37   TCP         66 443 → 60451 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SACK_PERM WS=128
23825 83.1744…  192.168.137.37   35.86.66.223     TCP         54 60451 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
23826 83.1754…  192.168.137.37   35.86.66.223     TLSv1.2    611 Client Hello (SNI=sq-tungsten-ts-fe.amazon-adsystem.com)
23885 83.4636…  35.86.66.223     192.168.137.37   TCP         54 443 → 60451 [ACK] Seq=1 Ack=558 Win=62208 Len=0
23886 83.4644…  35.86.66.223     192.168.137.37   TLSv1.2   1514 [TCP Previous segment not captured] , Ignored Unknown Record
23887 83.4644…  35.86.66.223     192.168.137.37   TCP       1514 [TCP Out-Of-Order] 443 → 60451 [ACK] Seq=1 Ack=558 Win=62208 Len=1460
23888 83.4645…  35.86.66.223     192.168.137.37   TCP       1230 443 → 60451 [PSH, ACK] Seq=2921 Ack=558 Win=62208 Len=1176
23890 83.4665…  192.168.137.37   35.86.66.223     TCP         66 [TCP Dup ACK 23825#1] 60451 → 443 [ACK] Seq=558 Ack=1 Win=131328 Len=0 SLE=1461 SRE=2921
23891 83.4665…  192.168.137.37   35.86.66.223     TCP         54 60451 → 443 [ACK] Seq=558 Ack=2921 Win=131328 Len=0
23892 83.4683…  35.86.66.223     192.168.137.37   TCP       1514 443 → 60451 [ACK] Seq=4097 Ack=558 Win=62208 Len=1460
23893 83.4683…  35.86.66.223     192.168.137.37   TLSv1.2    413 Ignored Unknown Record
23894 83.4706…  192.168.137.37   35.86.66.223     TCP         54 60451 → 443 [ACK] Seq=558 Ack=5916 Win=131328 Len=0
23896 83.4738…  192.168.137.37   35.86.66.223     TLSv1.2    147 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
23897 83.4738…  192.168.137.37   35.86.66.223     TLSv1.2    928 Application Data
23952 83.7752…  35.86.66.223     192.168.137.37   TCP         54 443 → 60451 [ACK] Seq=5916 Ack=1525 Win=61312 Len=0
23953 83.7752…  35.86.66.223     192.168.137.37   TLSv1.2    105 Change Cipher Spec, Encrypted Handshake Message
23954 83.7756…  35.86.66.223     192.168.137.37   TLSv1.2    700 Application Data
23956 83.7774…  192.168.137.37   35.86.66.223     TCP         54 60451 → 443 [ACK] Seq=1525 Ack=6613 Win=130560 Len=0
23958 83.7800…  192.168.137.37   35.86.66.223     TCP         54 60451 → 443 [FIN, ACK] Seq=1525 Ack=6613 Win=130560 Len=0
23995 84.0685…  35.86.66.223     192.168.137.37   TCP         54 443 → 60451 [FIN, ACK] Seq=6613 Ack=1526 Win=61312 Len=0

▸ Frame 23670: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Dev
▸ Ethernet II, Src: AzureWaveTec_2f:a5:0f (b4:8c:9d:2f:a5:0f), Dst: 3a:7a:0e:a3:97:8d (3a:
▸ Internet Protocol Version 4, Src: 192.168.137.37, Dst: 35.86.66.223
▾ Transmission Control Protocol, Src Port: 60451, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 60451
    Destination Port: 443
    [Stream index: 343]
  ▸ [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 2402976019

0000  3a 7a 0e a3 97 8d b4 8c  9d 2f a5 0f 08 00 45 00   :z······ ·/····E·
0010  00 34 86 71 40 00 80 06  c4 4f c0 a8 89 25 23 56   ·4·q@··· ·O···%#V
0020  42 df ec 23 01 bb 8f 3a  81 13 00 00 00 00 80 02   B··#···: ········
0030  fa f0 c5 ef 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

3. udp.port == xx

- Application: Filters UDP packets based on source or destination port number.
- Example: `udp.port == 53`



Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port==61329
```

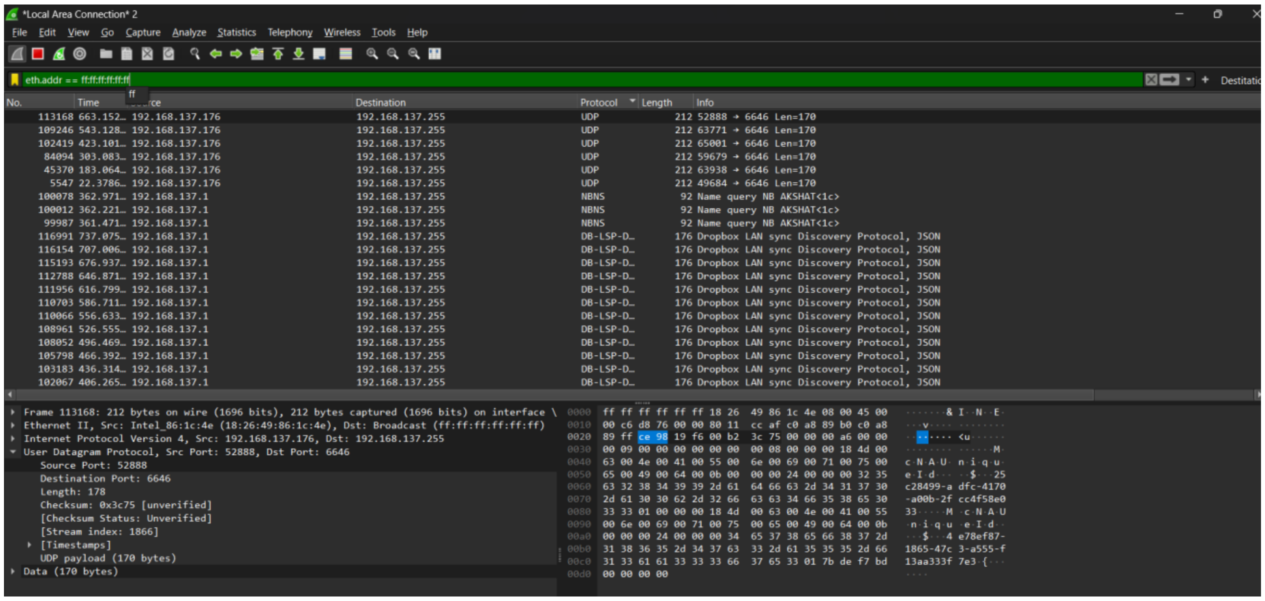
```
No.    Time       Source            Destination       Protocol  Length  Info
23429  81.8506…   142.250.199.170   192.168.137.176   UDP       63 443 → 61329 Len=21
23430  81.8536…   192.168.137.176   142.250.199.170   UDP       78 61329 → 443 Len=36
23446  81.9085…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
23465  81.9413…   142.250.199.170   192.168.137.176   UDP       68 443 → 61329 Len=26
23564  82.1449…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
23567  82.1785…   142.250.199.170   192.168.137.176   UDP       68 443 → 61329 Len=26
23587  82.3830…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
23595  82.4007…   142.250.199.170   192.168.137.176   UDP       68 443 → 61329 Len=26
23627  82.6049…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
23641  82.6486…   142.250.199.170   192.168.137.176   UDP       69 443 → 61329 Len=27
23661  82.8578…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
23672  82.9008…   142.250.199.170   192.168.137.176   UDP       69 443 → 61329 Len=27
23780  83.1093…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
23814  83.1524…   142.250.199.170   192.168.137.176   UDP       69 443 → 61329 Len=27
23917  83.5593…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
23921  83.6151…   142.250.199.170   192.168.137.176   UDP       69 443 → 61329 Len=27
24113  84.4261…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
24115  84.4935…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
24120  84.5196…   142.250.199.170   192.168.137.176   UDP       70 443 → 61329 Len=28
24538  86.1236…   192.168.137.176   142.250.199.170   UDP       71 61329 → 443 Len=29
24555  86.1434…   142.250.199.170   192.168.137.176   UDP       70 443 → 61329 Len=28
```

```
Frame 23661: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Devic
Ethernet II, Src: Intel_86:1c:4e (18:26:49:86:1c:4e), Dst: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:
Internet Protocol Version 4, Src: 192.168.137.176, Dst: 142.250.199.170
User Datagram Protocol, Src Port: 61329, Dst Port: 443
    Source Port: 61329
    Destination Port: 443
    Length: 37
    Checksum: 0x269d [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
    UDP payload (29 bytes)
Data (29 bytes)
```

```
0000  3a 7a 0e a3 97 8d 18 26  49 86 1c 4e 08 00 45 00   :z·····& I··N··E·
0010  00 39 44 b2 40 00 80 11  15 04 c0 a8 89 b0 8e fa   ·9D·@···  ········
0020  c7 aa ef 91 01 bb 00 25  26 9d 54 ed 57 5f 9e 20   ·······% &·T·W_·
0030  97 71 88 13 ab 95 00 96  9e 7a 2b 6d 5b 73 02 a0   ·q······ ·z+m[s··
0040  41 20 30 79 f7 08 a0                               A 0y···
```

4. eth.addr == xx:xx:xx:xx:xx:xx

- Application: Filters packets based on Ethernet MAC address.
- Example: `eth.addr == 00:1a:2b:3c:4d:5e`

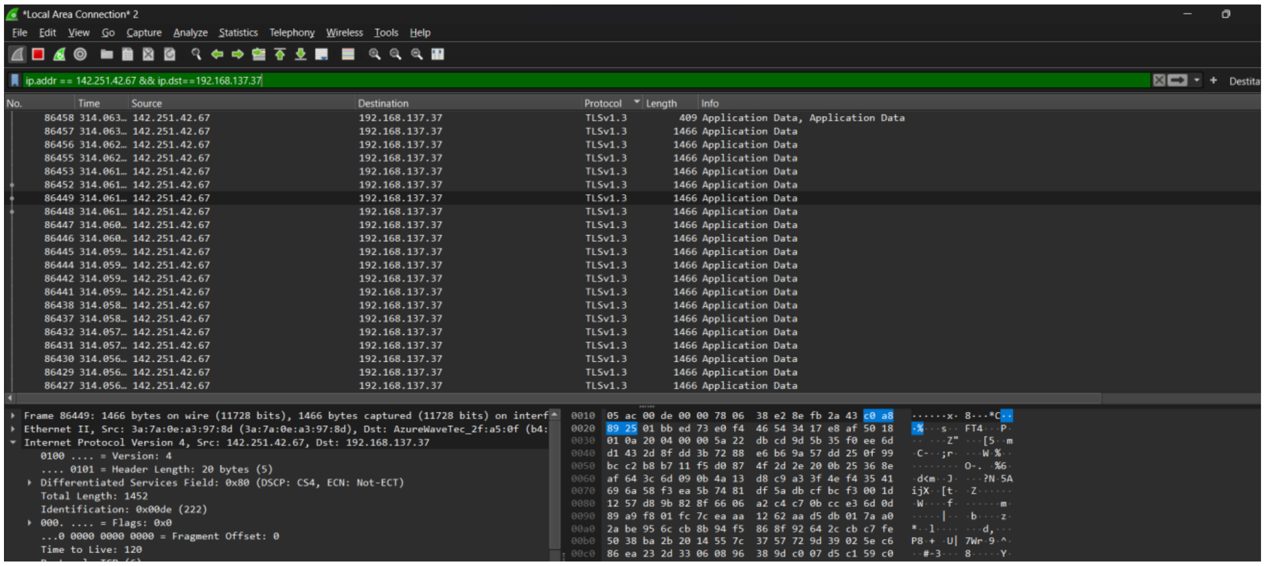

Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
eth.addr == ff:ff:ff:ff:ff:ff

No.     Time        Source            Destination       Protocol  Length Info
 113168 663.152…  192.168.137.176   192.168.137.255   UDP        212 52888 → 6646 Len=170
 109246 543.128…  192.168.137.176   192.168.137.255   UDP        212 63771 → 6646 Len=170
 102419 423.101…  192.168.137.176   192.168.137.255   UDP        212 65001 → 6646 Len=170
  84094 303.083…  192.168.137.176   192.168.137.255   UDP        212 59679 → 6646 Len=170
  45370 183.064…  192.168.137.176   192.168.137.255   UDP        212 63938 → 6646 Len=170
   5547 22.3786…  192.168.137.176   192.168.137.255   UDP        212 49684 → 6646 Len=170
 100078 362.971…  192.168.137.1     192.168.137.255   NBNS        92 Name query NB AKSHAT<1c>
 100012 362.221…  192.168.137.1     192.168.137.255   NBNS        92 Name query NB AKSHAT<1c>
  99987 361.471…  192.168.137.1     192.168.137.255   NBNS        92 Name query NB AKSHAT<1c>
 116991 737.075…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 116154 707.006…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 115193 676.937…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 112788 646.871…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 111956 616.799…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 110703 586.711…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 110066 556.633…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 108961 526.555…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 108052 496.469…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 105798 466.392…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 103183 436.314…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON
 102067 406.265…  192.168.137.1     192.168.137.255   DB-LSP-D…  176 Dropbox LAN sync Discovery Protocol, JSON

> Frame 113168: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits) on interface \
> Ethernet II, Src: Intel_86:1c:4e (18:26:49:86:1c:4e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.137.176, Dst: 192.168.137.255
v User Datagram Protocol, Src Port: 52888, Dst Port: 6646
    Source Port: 52888
    Destination Port: 6646
    Length: 178
    Checksum: 0x3c75 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1866]
  > [Timestamps]
    UDP payload (170 bytes)
> Data (170 bytes)

0000  ff ff ff ff ff ff 18 26  49 86 1c 4e 08 00 45 00   ······&I·N··E·
0010  00 c6 d8 76 00 00 80 11  cc af c0 a8 89 b0 c0 a8   ···v············
0020  89 ff ce 98 19 f6 00 b2  3c 75 00 00 00 a6 00 00   ········<u······
0030  00 09 00 00 00 00 00 00  00 08 00 00 00 18 4d 00   ··············M·
0040  63 00 4e 00 41 00 55 00  6e 00 69 00 71 00 75 00   c·N·A·U·n·i·q·u·
0050  65 00 49 00 64 00 0b 00  00 00 24 00 00 00 32 35   e·I·d·····$···25
0060  63 32 38 34 39 39 2d 61  64 66 63 2d 34 31 37 30   c28499-a dfc-4170
0070  2d 61 30 30 62 2d 32 66  63 63 34 66 35 38 65 30   -a00b-2f cc4f58e0
0080  33 33 01 00 00 00 18 4d  00 63 00 4e 00 41 00 55   33·····M ·c·N·A·U
0090  00 6e 00 69 00 71 00 75  00 65 00 49 00 64 00 0b   ·n·i·q·u ·e·I·d··
00a0  00 00 00 24 00 00 00 34  65 37 38 65 66 38 37 2d   ···$···4 e78ef87-
00b0  31 38 36 35 2d 34 37 63  33 2d 61 35 35 35 2d 66   1865-47c 3-a555-f
00c0  31 33 61 61 33 33 33 66  37 65 33 01 7b de f7 bd   13aa333f 7e3·{···
00d0  00 00 00 00                                        ····
```

5. ip.src == x.x.x.x && ip.dst == y.y.y.y

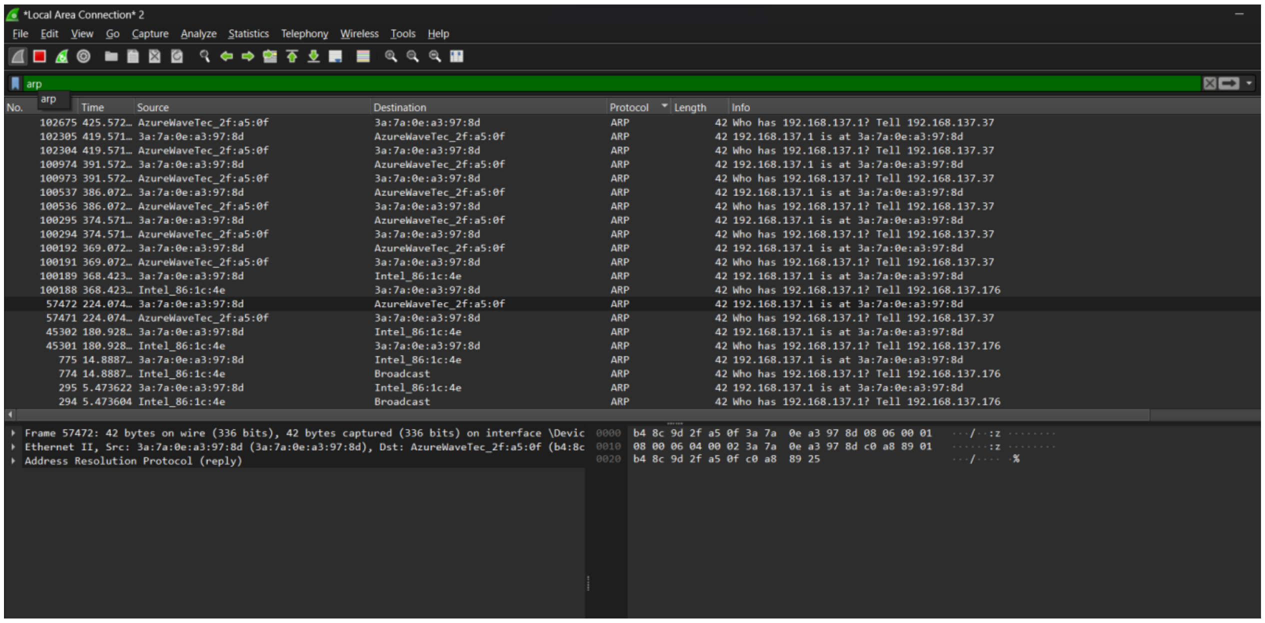
- Application: Filters packets based on both source and destination IP addresses.

- Example: `ip.src == 192.168.1.1 && ip.dst == 192.168.1.2`


Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr == 142.251.42.67 && ip.dst==192.168.137.37

No.     Time        Source            Destination       Protocol  Length Info
  86458 314.063…  142.251.42.67     192.168.137.37    TLSv1.3     409 Application Data, Application Data
  86457 314.063…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86456 314.062…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86455 314.062…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86453 314.061…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86452 314.061…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86449 314.061…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86448 314.061…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86447 314.060…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86446 314.060…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86445 314.059…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86444 314.059…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86442 314.059…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86441 314.059…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86438 314.058…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86437 314.058…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86432 314.057…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86431 314.057…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86430 314.056…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86429 314.056…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data
  86427 314.056…  142.251.42.67     192.168.137.37    TLSv1.3    1466 Application Data

> Frame 86449: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interf
> Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: AzureWaveTec_2f:a5:0f (b4:
v Internet Protocol Version 4, Src: 142.251.42.67, Dst: 192.168.137.37
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x80 (DSCP: CS4, ECN: Not-ECT)
    Total Length: 1452
    Identification: 0x00de (222)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 120

0010  05 ac 00 de 00 00 78 06  38 e2 8e fb 2a 43 c0 a8   ······x· 8···*C··
0020  89 25 01 bb ed 73 e0 f4  46 54 34 17 e8 af 50 18   ·%···s·· FT4···P·
0030  01 0a 20 04 00 00 5a 22  db cd 9d 5b 35 f0 ee 6d   ······Z" ···[5··m
0040  d1 43 2d 8f dd 3b 72 88  e6 b6 9a 57 dd 25 0f 99   ·C-··;r· ···W·%··
0050  bc c2 b8 b7 11 f5 d0 87  4f 2d 2e 20 0b 25 36 8e   ········ O-.··%6·
0060  af 64 3c 6d 09 0b 4a 13  d8 c9 a3 3f 4e f4 35 41   ·d<m··J· ···?N·5A
0070  69 6a 58 f3 ea 5b 74 81  df 5a db cf bc f3 00 1d   ijX··[t· ·Z······
0080  12 57 d8 9b 82 8f 66 06  a2 c4 c7 0b cc e3 6d 0d   ·W····f· ······m·
0090  89 a9 f8 01 fc 7c ea aa  12 62 aa d5 db 01 7a a0   ·····|·· ·b····z·
00a0  2a be 95 6c cb 8b 94 f5  86 8f 92 64 2c cb c7 fe   *··l···· ···d,···
00b0  50 38 ba 2b 20 14 55 7c  37 57 72 9d 39 02 5e c6   P8·+··U| 7Wr·9·^·
00c0  86 ea 23 2d 33 06 08 96  38 9d c0 07 d5 c1 59 c0   ··#-3··· 8·····Y·
```

6.arp

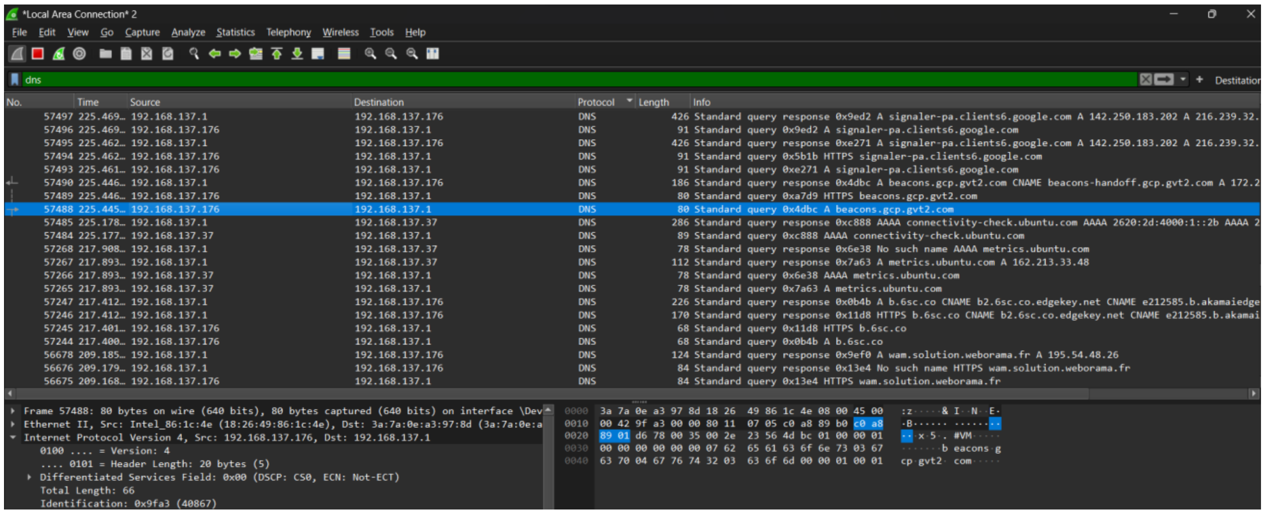

Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
arp
No.     Time        Source                     Destination                Protocol  Length  Info
102675 425.572… AzureWaveTec_2f:a5:0f  3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.37
102305 419.571… 3a:7a:0e:a3:97:8d      AzureWaveTec_2f:a5:0f  ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
102304 419.571… AzureWaveTec_2f:a5:0f  3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.37
100974 391.572… 3a:7a:0e:a3:97:8d      AzureWaveTec_2f:a5:0f  ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
100973 391.572… AzureWaveTec_2f:a5:0f  3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.37
100537 386.072… 3a:7a:0e:a3:97:8d      AzureWaveTec_2f:a5:0f  ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
100536 386.072… AzureWaveTec_2f:a5:0f  3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.37
100295 374.571… 3a:7a:0e:a3:97:8d      AzureWaveTec_2f:a5:0f  ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
100294 374.571… AzureWaveTec_2f:a5:0f  3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.37
100192 369.072… 3a:7a:0e:a3:97:8d      AzureWaveTec_2f:a5:0f  ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
100191 369.072… AzureWaveTec_2f:a5:0f  3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.37
100189 368.423… 3a:7a:0e:a3:97:8d      Intel_86:1c:4e         ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
100188 368.423… Intel_86:1c:4e         3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.176
 57472 224.074… 3a:7a:0e:a3:97:8d      AzureWaveTec_2f:a5:0f  ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
 57471 224.074… AzureWaveTec_2f:a5:0f  3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.37
 45302 180.928… 3a:7a:0e:a3:97:8d      Intel_86:1c:4e         ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
 45301 180.928… Intel_86:1c:4e         3a:7a:0e:a3:97:8d      ARP   42 Who has 192.168.137.1? Tell 192.168.137.176
   775 14.8887… 3a:7a:0e:a3:97:8d      Intel_86:1c:4e         ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
   774 14.8887… Intel_86:1c:4e         Broadcast              ARP   42 Who has 192.168.137.1? Tell 192.168.137.176
   295 5.473622 3a:7a:0e:a3:97:8d      Intel_86:1c:4e         ARP   42 192.168.137.1 is at 3a:7a:0e:a3:97:8d
   294 5.473604 Intel_86:1c:4e         Broadcast              ARP   42 Who has 192.168.137.1? Tell 192.168.137.176

> Frame 57472: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Devic
> Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: AzureWaveTec_2f:a5:0f (b4:8c
> Address Resolution Protocol (reply)

0000  b4 8c 9d 2f a5 0f 3a 7a  0e a3 97 8d 08 06 00 01   ···/··:z ········
0010  08 00 06 04 00 02 3a 7a  0e a3 97 8d c0 a8 89 01   ······:z ········
0020  b4 8c 9d 2f a5 0f c0 a8  89 25                     ···/···· ·%
```

7. dns

  - Application: Filters DNS protocol packets.

  - Example: `dns`

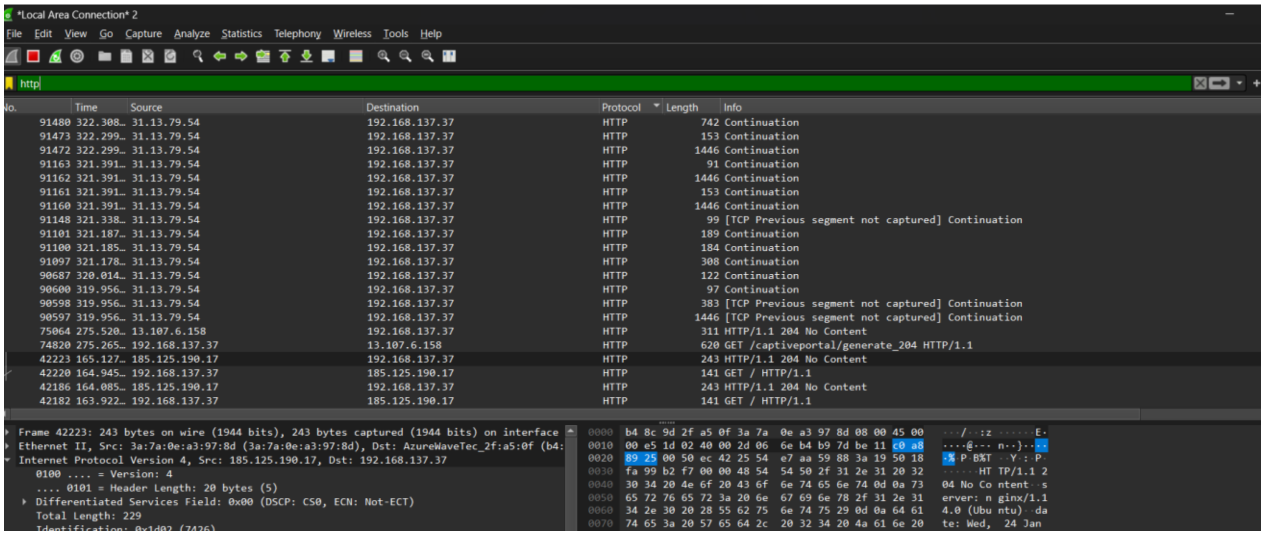

Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Destitation

```
dns
No.     Time      Source           Destination      Protocol  Length  Info
57497 225.469… 192.168.137.1    192.168.137.176  DNS  426 Standard query response 0x9ed2 A signaler-pa.clients6.google.com A 142.250.183.202 A 216.239.32.
57496 225.469… 192.168.137.176  192.168.137.1    DNS   91 Standard query 0x9ed2 A signaler-pa.clients6.google.com
57495 225.462… 192.168.137.1    192.168.137.176  DNS  426 Standard query response 0xe271 A signaler-pa.clients6.google.com A 142.250.183.202 A 216.239.32.
57494 225.462… 192.168.137.176  192.168.137.1    DNS   91 Standard query 0x5b1b HTTPS signaler-pa.clients6.google.com
57493 225.461… 192.168.137.176  192.168.137.1    DNS   91 Standard query 0xe271 A signaler-pa.clients6.google.com
57490 225.446… 192.168.137.1    192.168.137.176  DNS  186 Standard query response 0x4dbc A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 172.2
57489 225.446… 192.168.137.176  192.168.137.1    DNS   80 Standard query 0xa7d9 HTTPS beacons.gcp.gvt2.com
57488 225.445… 192.168.137.176  192.168.137.1    DNS   80 Standard query 0x4dbc A beacons.gcp.gvt2.com
57485 225.178… 192.168.137.1    192.168.137.37   DNS  286 Standard query response 0xc888 AAAA connectivity-check.ubuntu.com AAAA 2620:2d:4000:1::2b AAAA 2
57484 225.177… 192.168.137.37   192.168.137.1    DNS   89 Standard query 0xc888 AAAA connectivity-check.ubuntu.com
57268 217.908… 192.168.137.1    192.168.137.37   DNS   78 Standard query response 0x6e38 No such name AAAA metrics.ubuntu.com
57267 217.893… 192.168.137.1    192.168.137.37   DNS  112 Standard query response 0x7a63 A metrics.ubuntu.com A 162.213.33.48
57266 217.893… 192.168.137.37   192.168.137.1    DNS   78 Standard query 0x6e38 AAAA metrics.ubuntu.com
57265 217.893… 192.168.137.37   192.168.137.1    DNS   78 Standard query 0x7a63 A metrics.ubuntu.com
57247 217.412… 192.168.137.1    192.168.137.176  DNS  226 Standard query response 0x0b4b A b.6sc.co CNAME b2.6sc.co.edgekey.net CNAME e212585.b.akamaiedge
57246 217.412… 192.168.137.1    192.168.137.176  DNS  170 Standard query response 0x11d8 HTTPS b.6sc.co CNAME b2.6sc.co.edgekey.net CNAME e212585.b.akamai
57245 217.401… 192.168.137.176  192.168.137.1    DNS   68 Standard query 0x11d8 HTTPS b.6sc.co
57244 217.400… 192.168.137.176  192.168.137.1    DNS   68 Standard query 0x0b4b A b.6sc.co
56678 209.185… 192.168.137.1    192.168.137.176  DNS  124 Standard query response 0x9ef0 A wam.solution.weborama.fr A 195.54.48.26
56676 209.179… 192.168.137.1    192.168.137.176  DNS   84 Standard query response 0x13e4 No such name HTTPS wam.solution.weborama.fr
56675 209.168… 192.168.137.176  192.168.137.1    DNS   84 Standard query 0x13e4 HTTPS wam.solution.weborama.fr

> Frame 57488: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Dev
> Ethernet II, Src: Intel_86:1c:4e (18:26:49:86:1c:4e), Dst: 3a:7a:0e:a3:97:8d (3a:7a:0e:a
v Internet Protocol Version 4, Src: 192.168.137.176, Dst: 192.168.137.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 66
    Identification: 0x9fa3 (40867)

0000  3a 7a 0e a3 97 8d 18 26  49 86 1c 4e 08 00 45 00   :z·····& I··N··E·
0010  00 42 9f a3 00 00 80 11  07 05 c0 a8 89 b0 c0 a8   ·B······ ········
0020  89 01 d6 78 00 35 00 2e  23 56 4d bc 01 00 00 01   ···x·5·. #VM·····
0030  00 00 00 00 00 00 07 62  65 61 63 6f 6e 73 03 67   ·······b eacons·g
0040  63 70 04 67 76 74 32 03  63 6f 6d 00 00 01 00 01   cp·gvt2· com·····
```

8. http

  - Application: Filters HTTP protocol packets.

  - Example: `http`

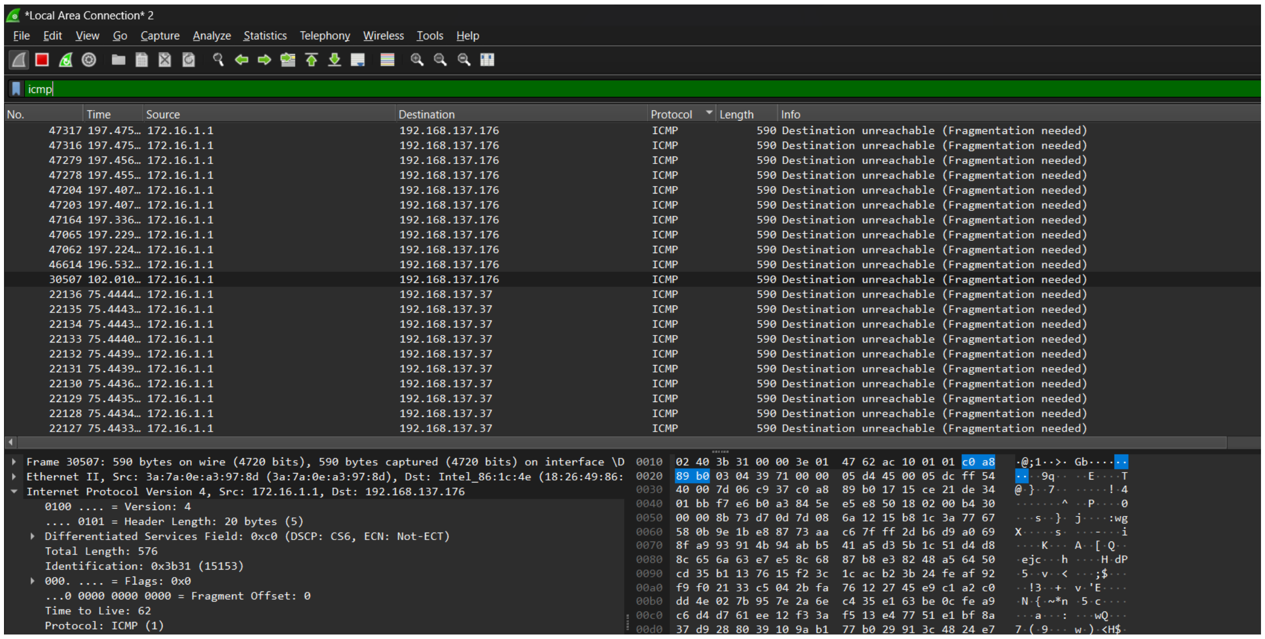


```
*Local Area Connection* 2
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help

http

No.     Time      Source            Destination       Protocol  Length  Info
  91480 322.308…  31.13.79.54       192.168.137.37    HTTP       742 Continuation
  91473 322.299…  31.13.79.54       192.168.137.37    HTTP       153 Continuation
  91472 322.299…  31.13.79.54       192.168.137.37    HTTP      1446 Continuation
  91163 321.391…  31.13.79.54       192.168.137.37    HTTP        91 Continuation
  91162 321.391…  31.13.79.54       192.168.137.37    HTTP      1446 Continuation
  91161 321.391…  31.13.79.54       192.168.137.37    HTTP       153 Continuation
  91160 321.391…  31.13.79.54       192.168.137.37    HTTP      1446 Continuation
  91148 321.338…  31.13.79.54       192.168.137.37    HTTP        99 [TCP Previous segment not captured] Continuation
  91101 321.187…  31.13.79.54       192.168.137.37    HTTP       189 Continuation
  91100 321.185…  31.13.79.54       192.168.137.37    HTTP       184 Continuation
  91097 321.178…  31.13.79.54       192.168.137.37    HTTP       308 Continuation
  90687 320.014…  31.13.79.54       192.168.137.37    HTTP       122 Continuation
  90600 319.956…  31.13.79.54       192.168.137.37    HTTP        97 Continuation
  90598 319.956…  31.13.79.54       192.168.137.37    HTTP       383 [TCP Previous segment not captured] Continuation
  90597 319.956…  31.13.79.54       192.168.137.37    HTTP      1446 [TCP Previous segment not captured] Continuation
  75064 275.520…  13.107.6.158      192.168.137.37    HTTP       311 HTTP/1.1 204 No Content
  74820 275.265…  192.168.137.37    13.107.6.158      HTTP       620 GET /captiveportal/generate_204 HTTP/1.1
  42223 165.127…  185.125.190.17    192.168.137.37    HTTP       243 HTTP/1.1 204 No Content
  42220 164.945…  192.168.137.37    185.125.190.17    HTTP       141 GET / HTTP/1.1
  42186 164.085…  185.125.190.17    192.168.137.37    HTTP       243 HTTP/1.1 204 No Content
  42182 163.922…  192.168.137.37    185.125.190.17    HTTP       141 GET / HTTP/1.1

Frame 42223: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface
Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: AzureWaveTec_2f:a5:0f (b4:
Internet Protocol Version 4, Src: 185.125.190.17, Dst: 192.168.137.37
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 229
    Identification: 0x1d02 (7426)

0000  b4 8c 9d 2f a5 0f 3a 7a  0e a3 97 8d 08 00 45 00   ···/··:z ······E·
0010  00 e5 1d 02 40 00 2d 06  6e b4 b9 7d be 11 c0 a8   ····@·-· n··}····
0020  89 25 00 50 ec 42 25 54  e7 aa 59 88 3a 19 50 18   ·%·P·B%T ··Y·:·P·
0030  fa 99 b2 f7 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT TP/1.1 2
0040  30 34 20 4e 6f 20 43 6f  6e 74 65 6e 74 0d 0a 73   04 No Co ntent··s
0050  65 72 76 65 72 3a 20 6e  67 69 6e 78 2f 31 2e 31   erver: n ginx/1.1
0060  34 2e 30 20 28 55 62 75  6e 74 75 29 0d 0a 64 61   4.0 (Ubu ntu)··da
0070  74 65 3a 20 57 65 64 2c  20 32 34 20 4a 61 6e 20   te: Wed,  24 Jan
```

9. icmp

  - Application: Filters ICMP (Internet Control Message Protocol) packets.

  - Example: `icmp`

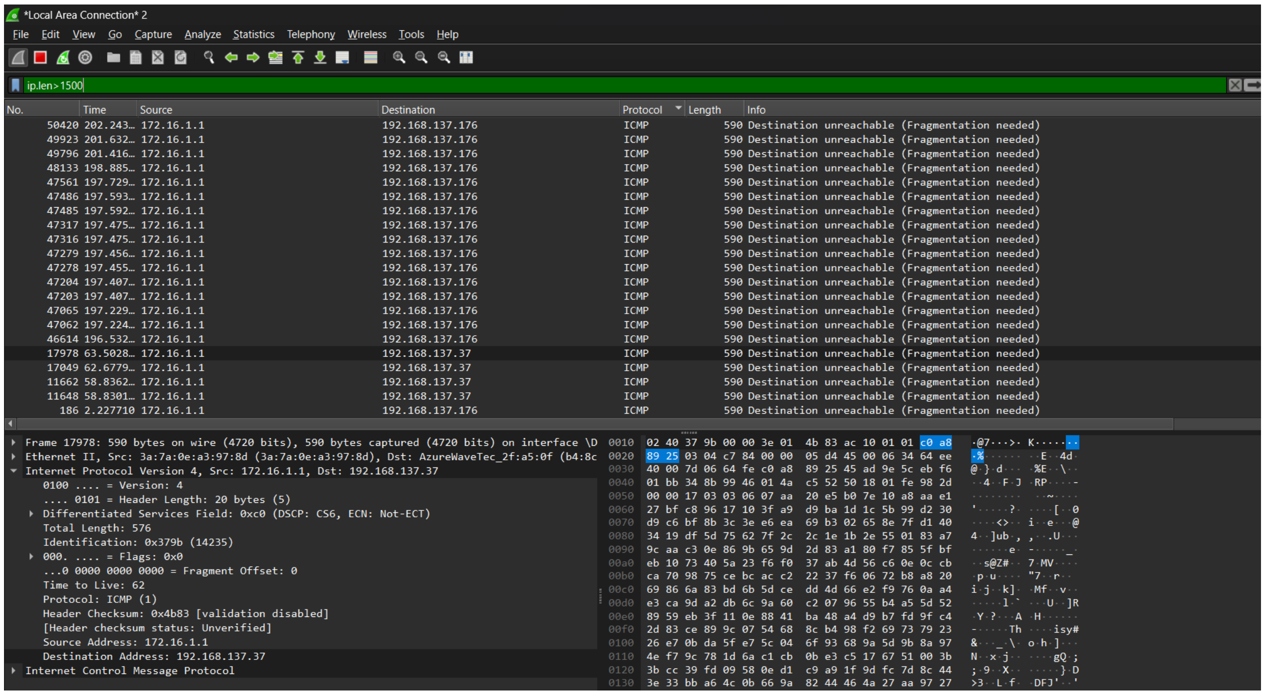


```
*Local Area Connection* 2
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help

icmp

No.     Time      Source        Destination       Protocol  Length  Info
  47317 197.475…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47316 197.475…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47279 197.456…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47278 197.455…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47204 197.407…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47203 197.407…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47164 197.336…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47065 197.229…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  47062 197.224…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  46614 196.532…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  30507 102.010…  172.16.1.1    192.168.137.176   ICMP       590 Destination unreachable (Fragmentation needed)
  22136 75.4444…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22135 75.4443…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22134 75.4443…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22133 75.4440…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22132 75.4439…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22131 75.4439…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22130 75.4436…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22129 75.4435…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22128 75.4434…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)
  22127 75.4433…  172.16.1.1    192.168.137.37    ICMP       590 Destination unreachable (Fragmentation needed)

Frame 30507: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \D
Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: Intel_86:1c:4e (18:26:49:86:
Internet Protocol Version 4, Src: 172.16.1.1, Dst: 192.168.137.176
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 576
    Identification: 0x3b31 (15153)
  000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 62
    Protocol: ICMP (1)

0010  02 40 3b 31 00 00 3e 01  47 62 ac 10 01 01 c0 a8   ·@;1··>· Gb······
0020  89 b0 03 04 39 71 00 00  05 d4 45 00 05 dc ff 54   ····9q·· ··E····T
0030  40 00 7d 06 c9 37 c0 a8  89 b0 17 15 ce 21 de 34   @·}··7·· ·····!·4
0040  01 bb f7 e6 b0 a3 84 5e  e5 e8 50 18 02 00 b4 30   ·······^ ··P····0
0050  00 00 8b 73 d7 0d 7d 08  6a 12 15 b8 1c 3a 77 67   ···s··}· j····:wg
0060  58 0b 9e 1b e8 87 73 aa  c6 7f ff 2d b6 d9 a0 69   X·····s· ···-···i
0070  8f a9 93 91 4b 94 ab b5  41 a5 d3 5b 1c 51 d4 d8   ····K··· A··[·Q··
0080  8c 65 6a 63 e7 e5 8c 68  87 b8 e3 82 48 a5 64 50   ·ejc···h ····H·dP
0090  cd 35 b1 13 76 15 f2 3c  1c ac b2 3b 24 fe af 92   ·5··v··< ···;$···
00a0  f9 f0 21 33 c5 04 2b fa  76 12 27 45 e9 c1 a2 c0   ··!3··+· v·'E····
00b0  dd 4e 02 7b 95 7e 2a 6e  c4 35 e1 63 be 0c fe a9   ·N·{·~*n ·5·c····
00c0  c6 d4 d7 61 ee 12 f3 3a  f5 13 e4 77 51 e1 bf 8a   ···a···: ···wQ···
00d0  37 d9 28 80 39 10 9a b1  77 b0 29 91 3c 48 24 e7   7·(·9··· w·)·<H$·
```

10. ip.len > 1500

  - Application: Filters packets with an IP length greater than 1500 bytes.

  - Example: `ip.len > 1500`



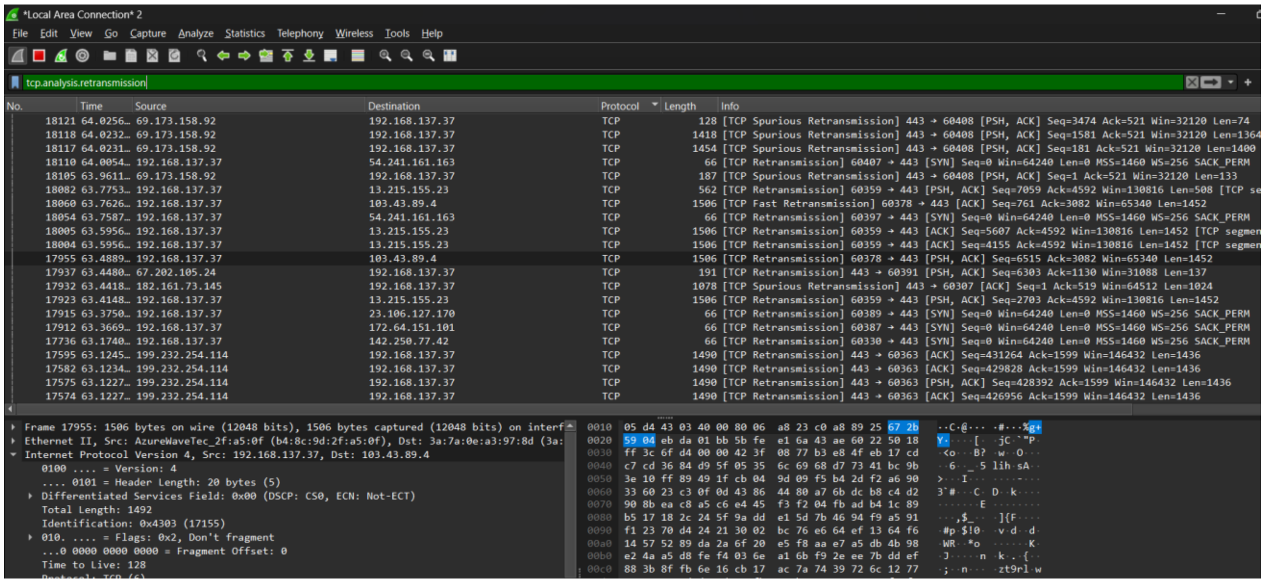
```
*Local Area Connection* 2
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
ip.len>1500

No.    Time      Source       Destination       Protocol  Length Info
 50420 202.243… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 49923 201.632… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 49796 201.416… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 48133 198.885… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47561 197.729… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47486 197.593… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47485 197.592… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47317 197.475… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47316 197.475… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47279 197.456… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47278 197.455… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47204 197.407… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47203 197.407… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47065 197.229… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 47062 197.224… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 46614 196.532… 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
 17978 63.5028… 172.16.1.1   192.168.137.37    ICMP      590 Destination unreachable (Fragmentation needed)
 17049 62.6779… 172.16.1.1   192.168.137.37    ICMP      590 Destination unreachable (Fragmentation needed)
 11662 58.8362… 172.16.1.1   192.168.137.37    ICMP      590 Destination unreachable (Fragmentation needed)
 11648 58.8301… 172.16.1.1   192.168.137.37    ICMP      590 Destination unreachable (Fragmentation needed)
   186 2.227710 172.16.1.1   192.168.137.176   ICMP      590 Destination unreachable (Fragmentation needed)
```

```
› Frame 17978: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface \D
› Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: AzureWaveTec_2f:a5:0f (b4:8c
⌄ Internet Protocol Version 4, Src: 172.16.1.1, Dst: 192.168.137.37
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
    Total Length: 576
    Identification: 0x379b (14235)
  › 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 62
    Protocol: ICMP (1)
    Header Checksum: 0x4b83 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.16.1.1
    Destination Address: 192.168.137.37
› Internet Control Message Protocol
```

```
0010  02 40 37 9b 00 00 3e 01  4b 83 ac 10 01 01 c0 a8   ·@7···>· K·······
0020  89 25 03 04 c7 84 00 00  05 d4 45 00 06 34 64 ee   ·%······ ··E··4d·
0030  40 00 7d 06 64 fe c0 a8  89 25 45 ad 9e 5c eb f6   @·}·d··· ·%E··\··
0040  01 bb 34 8b 99 46 01 4a  c5 52 50 18 01 fe 98 2d   ··4··F·J ·RP····-
0050  00 00 17 03 03 06 07 aa  20 e5 b0 7e 10 a8 aa e1   ········ ···~····
0060  27 bf c8 96 17 10 3f a9  d9 ba 1d 1c 5b 99 d2 30   '·····?· ····[··0
0070  d9 c6 bf 8b 3c 3e e6 ea  69 b3 02 65 8e 7f d1 40   ····<>·· i··e···@
0080  34 19 df 5d 75 62 7f 2c  2c 1e 1b 2e 55 01 83 a7   4··]ub·, ,···U···
0090  9c aa c3 0e 86 9b 65 9d  2d 83 a1 80 f7 85 5f bf   ······e· -·····_·
00a0  eb 10 73 40 5a 23 f6 f0  37 ab 4d 56 c6 0e 0c cb   ··s@Z#·· 7·MV····
00b0  ca 70 98 75 ce bc ac c2  22 37 f6 06 72 b8 a8 20   ·p·u···· "7··r··
00c0  69 86 6a 83 bd 6b 5d ce  dd 4d 66 e2 f9 76 0a a4   i·j··k]· ·Mf··v··
00d0  e3 ca 9d a2 db 6c 9a 60  c2 07 96 55 b4 a5 5d 52   ·····l·` ···U··]R
00e0  89 59 eb 3f 11 0e 88 41  ba 48 a4 d9 b7 fd 9f c4   ·Y·?···A ·H······
00f0  2d 83 ce 89 9c 07 54 68  8c b4 98 f2 69 73 79 23   -·····Th ····isy#
0100  26 e7 0b da 5f e7 5c 04  6f 93 68 9a 5d 9b 8a 97   &···_·\· o·h·]···
0110  4e f7 9c 78 1d 6a c1 cb  0b e3 c5 17 67 51 00 3b   N··x·j·· ····gQ·;
0120  3b cc 39 fd 09 58 0e d1  c9 a9 1f 9d fc 7d 8c 44   ;·9··X·· ·····}·D
0130  3e 33 bb a6 4c 0b 66 9a  82 44 46 4a 27 aa 97 27   >3··L·f· ·DFJ'··'
```

11. tcp.analysis.retransmission

- Application: Filters retransmitted TCP packets.
- Example: `tcp.analysis.retransmission`



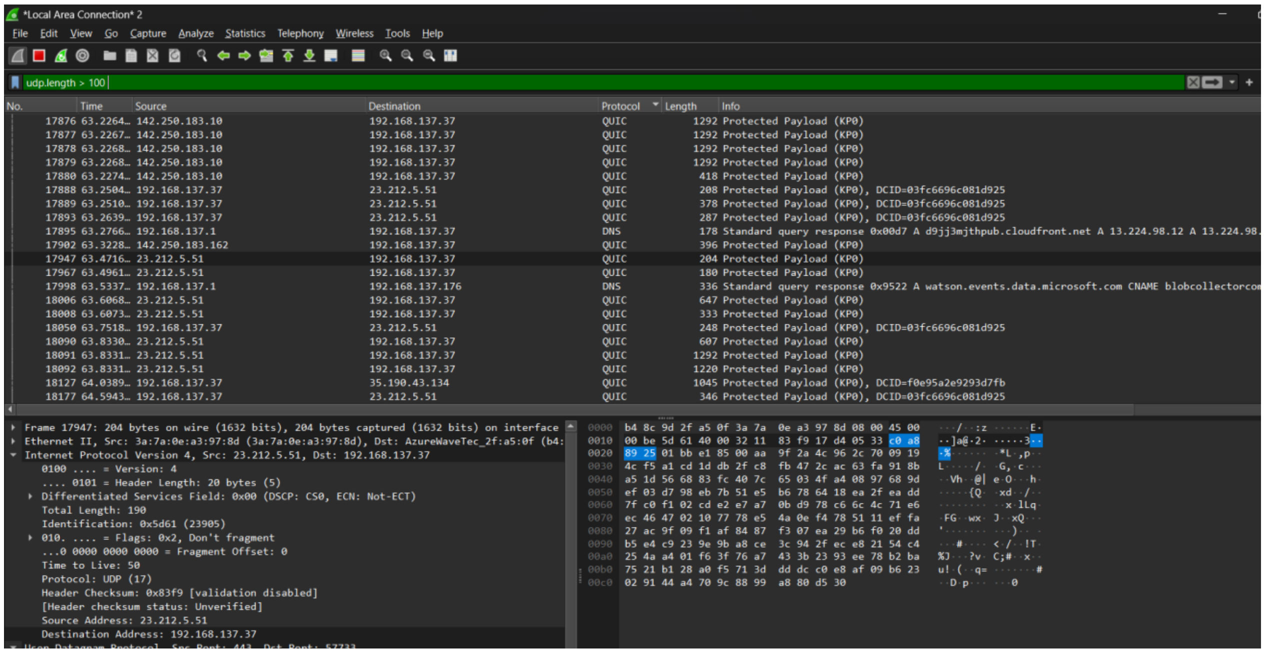
```
*Local Area Connection* 2
File  Edit  View  Go  Capture  Analyze  Statistics  Telephony  Wireless  Tools  Help
tcp.analysis.retransmission

No.    Time      Source           Destination       Protocol  Length Info
 18121 64.0256… 69.173.158.92    192.168.137.37    TCP       128 [TCP Spurious Retransmission] 443 → 60408 [PSH, ACK] Seq=3474 Ack=521 Win=32120 Len=74
 18118 64.0232… 69.173.158.92    192.168.137.37    TCP      1418 [TCP Spurious Retransmission] 443 → 60408 [PSH, ACK] Seq=1581 Ack=521 Win=32120 Len=1364
 18117 64.0231… 69.173.158.92    192.168.137.37    TCP      1454 [TCP Spurious Retransmission] 443 → 60408 [PSH, ACK] Seq=181 Ack=521 Win=32120 Len=1400
 18110 64.0054… 192.168.137.37   54.241.161.163    TCP        66 [TCP Retransmission] 60407 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 18105 63.9611… 69.173.158.92    192.168.137.37    TCP       187 [TCP Spurious Retransmission] 443 → 60408 [PSH, ACK] Seq=1 Ack=521 Win=32120 Len=133
 18082 63.7753… 192.168.137.37   13.215.155.23     TCP       562 [TCP Retransmission] 60359 → 443 [PSH, ACK] Seq=7059 Ack=4592 Win=130816 Len=508 [TCP se
 18060 63.7626… 192.168.137.37   103.43.89.4       TCP      1506 [TCP Fast Retransmission] 60378 → 443 [ACK] Seq=761 Ack=3082 Win=65340 Len=1452
 18054 63.7587… 192.168.137.37   54.241.161.163    TCP        66 [TCP Retransmission] 60397 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 18005 63.5956… 192.168.137.37   13.215.155.23     TCP      1506 [TCP Retransmission] 60359 → 443 [ACK] Seq=5607 Ack=4592 Win=130816 Len=1452 [TCP segmen
 18004 63.5956… 192.168.137.37   13.215.155.23     TCP      1506 [TCP Retransmission] 60359 → 443 [ACK] Seq=4155 Ack=4592 Win=130816 Len=1452 [TCP segmen
 17955 63.4889… 192.168.137.37   103.43.89.4       TCP      1506 [TCP Retransmission] 60378 → 443 [PSH, ACK] Seq=6515 Ack=3082 Win=65340 Len=1452
 17937 63.4480… 67.202.105.24    192.168.137.37    TCP       191 [TCP Retransmission] 443 → 60391 [PSH, ACK] Seq=6303 Ack=1130 Win=31088 Len=137
 17932 63.4418… 182.161.73.145   192.168.137.37    TCP      1078 [TCP Spurious Retransmission] 443 → 60307 [ACK] Seq=1 Ack=519 Win=64512 Len=1024
 17923 63.4148… 192.168.137.37   13.215.155.23     TCP      1506 [TCP Retransmission] 60359 → 443 [PSH, ACK] Seq=2703 Ack=4592 Win=130816 Len=1452
 17915 63.3750… 192.168.137.37   23.106.127.170    TCP        66 [TCP Retransmission] 60389 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 17912 63.3669… 192.168.137.37   172.64.151.101    TCP        66 [TCP Retransmission] 60387 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 17736 63.1740… 192.168.137.37   142.250.77.42     TCP        66 [TCP Retransmission] 60330 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 17595 63.1245… 199.232.254.114  192.168.137.37    TCP      1490 [TCP Retransmission] 443 → 60363 [ACK] Seq=431264 Ack=1599 Win=146432 Len=1436
 17582 63.1234… 199.232.254.114  192.168.137.37    TCP      1490 [TCP Retransmission] 443 → 60363 [ACK] Seq=429828 Ack=1599 Win=146432 Len=1436
 17575 63.1227… 199.232.254.114  192.168.137.37    TCP      1490 [TCP Retransmission] 443 → 60363 [PSH, ACK] Seq=428392 Ack=1599 Win=146432 Len=1436
 17574 63.1227… 199.232.254.114  192.168.137.37    TCP      1490 [TCP Retransmission] 443 → 60363 [ACK] Seq=426956 Ack=1599 Win=146432 Len=1436
```

```
› Frame 17955: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interf
› Ethernet II, Src: AzureWaveTec_2f:a5:0f (b4:8c:9d:2f:a5:0f), Dst: 3a:7a:0e:a3:97:8d (3a:
⌄ Internet Protocol Version 4, Src: 192.168.137.37, Dst: 103.43.89.4
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1492
    Identification: 0x4303 (17155)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
```

```
0010  05 d4 43 03 40 00 80 06  a8 23 c0 a8 89 25 67 2b   ··C·@··· ·#···%g+
0020  59 04 eb da 01 bb 5b fe  e1 6a 43 ae 60 22 50 18   Y·····[· ·jC·`"P·
0030  ff 3c 6f d4 00 00 42 3f  08 77 b3 e8 4f eb 17 cd   ·<o···B? ·w··O···
0040  c7 cd 36 84 d9 5f 05 35  6c 69 68 d7 73 41 bc 9b   ··6··_·5 lih·sA··
0050  3e 10 ff 89 49 1f cb 04  9d 09 f5 b4 2d f2 a6 90   >···I··· ····-···
0060  33 60 23 c3 0f 0d 43 86  44 80 a7 6b dc b8 c4 d2   3`#···C· D··k····
0070  90 8b ea c8 a5 c6 e4 45  f3 f2 04 fb ad b4 1c 89   ·······E ········
0080  b5 17 18 2c 24 5f 9a dd  e1 5d 7b 46 94 f9 a5 91   ···,$_·· ·]{F····
0090  f1 23 70 d4 24 21 30 02  bc 76 e6 64 ef 13 64 f6   ·#p·$!0· ·v·d··d·
00a0  14 57 52 89 da 2a 6f 20  e5 f8 aa e7 a5 db 4b 98   ·WR··*o  ······K·
00b0  e2 4a a5 d8 fe f4 03 6e  a1 6b f9 2e ee 7b dd ef   ·J·····n ·k·.·{··
00c0  88 3b 8f fb 6e 16 cb 17  ac 7a 74 39 72 6c 12 77   ·;··n··· ·zt9rl·w
```

12. udp.length > 100

- Application: Filters UDP packets with payload length greater than 100 bytes.
- Example: `udp.length > 100`



Local Area Connection 2

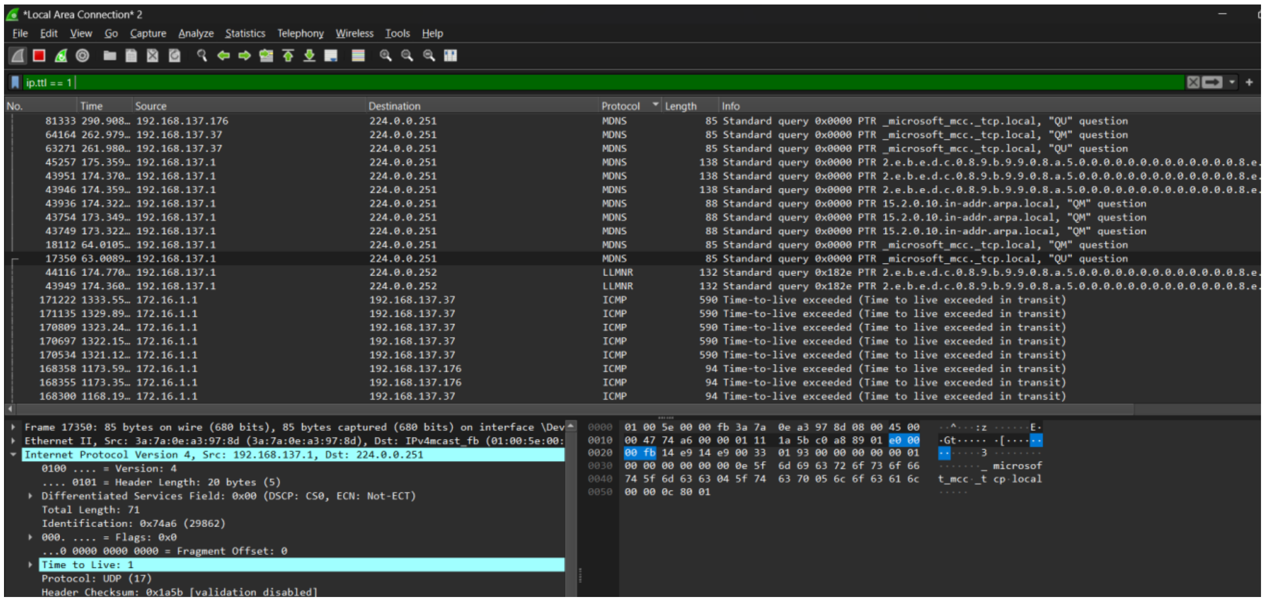
```
udp.length > 100

No.   Time       Source            Destination        Protocol  Length Info
17876 63.2264… 142.250.183.10    192.168.137.37     QUIC      1292 Protected Payload (KP0)
17877 63.2267… 142.250.183.10    192.168.137.37     QUIC      1292 Protected Payload (KP0)
17878 63.2268… 142.250.183.10    192.168.137.37     QUIC      1292 Protected Payload (KP0)
17879 63.2268… 142.250.183.10    192.168.137.37     QUIC      1292 Protected Payload (KP0)
17880 63.2274… 142.250.183.10    192.168.137.37     QUIC       418 Protected Payload (KP0)
17888 63.2504… 192.168.137.37    23.212.5.51        QUIC       208 Protected Payload (KP0), DCID=03fc6696c081d925
17889 63.2510… 192.168.137.37    23.212.5.51        QUIC       378 Protected Payload (KP0), DCID=03fc6696c081d925
17893 63.2639… 192.168.137.37    23.212.5.51        QUIC       287 Protected Payload (KP0), DCID=03fc6696c081d925
17895 63.2766… 192.168.137.1     192.168.137.37     DNS        178 Standard query response 0x00d7 A d9jj3mjthpub.cloudfront.net A 13.224.98.12 A 13.224.98.
17902 63.3228… 142.250.183.162   192.168.137.37     QUIC       396 Protected Payload (KP0)
17947 63.4716… 23.212.5.51       192.168.137.37     QUIC       204 Protected Payload (KP0)
17967 63.4961… 23.212.5.51       192.168.137.37     QUIC       180 Protected Payload (KP0)
17998 63.5337… 192.168.137.1     192.168.137.176    DNS        336 Standard query response 0x9522 A watson.events.data.microsoft.com CNAME blobcollectorcom
18006 63.6068… 23.212.5.51       192.168.137.37     QUIC       647 Protected Payload (KP0)
18008 63.6073… 23.212.5.51       192.168.137.37     QUIC       333 Protected Payload (KP0)
18050 63.7518… 192.168.137.37    23.212.5.51        QUIC       248 Protected Payload (KP0), DCID=03fc6696c081d925
18090 63.8330… 23.212.5.51       192.168.137.37     QUIC       607 Protected Payload (KP0)
18091 63.8331… 23.212.5.51       192.168.137.37     QUIC      1292 Protected Payload (KP0)
18092 63.8331… 23.212.5.51       192.168.137.37     QUIC      1220 Protected Payload (KP0)
18127 64.0389… 192.168.137.37    35.190.43.134      QUIC      1045 Protected Payload (KP0), DCID=f0e95a2e9293d7fb
18177 64.5943… 192.168.137.37    23.212.5.51        QUIC       346 Protected Payload (KP0), DCID=03fc6696c081d925
```

```
> Frame 17947: 204 bytes on wire (1632 bits), 204 bytes captured (1632 bits) on interface
> Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: AzureWaveTec_2f:a5:0f (b4:
v Internet Protocol Version 4, Src: 23.212.5.51, Dst: 192.168.137.37
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 190
    Identification: 0x5d61 (23905)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 50
    Protocol: UDP (17)
    Header Checksum: 0x83f9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 23.212.5.51
    Destination Address: 192.168.137.37
```

```
0000  b4 8c 9d 2f a5 0f 3a 7a  0e a3 97 8d 08 00 45 00   ···/··:z ······E·
0010  00 be 5d 61 40 00 32 11  83 f9 17 d4 05 33 c0 a8   ··]a@·2· ·····3··
0020  89 25 01 bb e1 85 00 aa  9f 2a 4c 96 2c 70 09 19   ·%······ ·*L·,p··
0030  4c f5 a1 cd 1d db 2f c8  fb 47 2c ac 63 fa 91 8b   L·····/· ·G,·c···
0040  a5 1d 56 68 83 fc 40 7c  65 03 4f a4 08 97 68 9d   ··Vh··@| e·O···h·
0050  ef 03 d7 98 eb 7b 51 e5  b6 78 64 18 ea 2f ea dd   ·····{Q· ·xd··/··
0060  7f c0 f1 02 cd e2 e7 a7  0b d9 78 c6 6c 4c 71 e6   ········ ··x·lLq·
0070  ec 46 47 02 10 77 78 e5  4a 0e f4 78 51 11 ef fa   ·FG··wx· J··xQ···
0080  27 ac 9f 09 f1 af 84 87  f3 07 ea 29 b6 f0 20 dd   '······· ···)·· ·
0090  b5 e4 c9 23 9e 9b a8 ce  3c 94 2f ec e8 21 54 c4   ···#···· <·/··!T·
00a0  25 4a a4 01 f6 3f 76 a7  43 3b 23 93 ee 78 b2 ba   %J···?v· C;#··x··
00b0  75 21 b1 28 a0 f5 71 3d  dd dc c0 e8 af 09 b6 23   u!·(··q= ·······#
00c0  02 91 44 a4 70 9c 88 99  a8 80 d5 30               ··D·p··· ···0
```

13. ip.ttl == 1

- Application: Filters packets with a Time-to-Live (TTL) value of 1.
- Example: `ip.ttl == 1`



Local Area Connection 2

```
ip.ttl == 1

No.    Time       Source            Destination        Protocol  Length Info
 81333 290.908… 192.168.137.176   224.0.0.251        MDNS        85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
 64164 262.979… 192.168.137.37    224.0.0.251        MDNS        85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
 63271 261.980… 192.168.137.37    224.0.0.251        MDNS        85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
 45257 175.359… 192.168.137.1     224.0.0.251        MDNS       138 Standard query 0x0000 PTR 2.e.b.e.d.c.0.8.9.b.9.9.0.8.a.5.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.
 43951 174.370… 192.168.137.1     224.0.0.251        MDNS       138 Standard query 0x0000 PTR 2.e.b.e.d.c.0.8.9.b.9.9.0.8.a.5.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.
 43946 174.359… 192.168.137.1     224.0.0.251        MDNS       138 Standard query 0x0000 PTR 2.e.b.e.d.c.0.8.9.b.9.9.0.8.a.5.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.
 43936 174.322… 192.168.137.1     224.0.0.251        MDNS        88 Standard query 0x0000 PTR 15.2.0.10.in-addr.arpa.local, "QM" question
 43754 173.349… 192.168.137.1     224.0.0.251        MDNS        88 Standard query 0x0000 PTR 15.2.0.10.in-addr.arpa.local, "QM" question
 43749 173.322… 192.168.137.1     224.0.0.251        MDNS        88 Standard query 0x0000 PTR 15.2.0.10.in-addr.arpa.local, "QM" question
 18112 64.0105… 192.168.137.1     224.0.0.251        MDNS        85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
 17350 63.0089… 192.168.137.1     224.0.0.251        MDNS        85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
 44116 174.770… 192.168.137.1     224.0.0.252        LLMNR      132 Standard query 0x182e PTR 2.e.b.e.d.c.0.8.9.b.9.9.0.8.a.5.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.
 43949 174.360… 192.168.137.1     224.0.0.252        LLMNR      132 Standard query 0x182e PTR 2.e.b.e.d.c.0.8.9.b.9.9.0.8.a.5.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.
171222 1333.55… 172.16.1.1        192.168.137.37     ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
171135 1329.89… 172.16.1.1        192.168.137.37     ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
170809 1323.24… 172.16.1.1        192.168.137.37     ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
170697 1322.15… 172.16.1.1        192.168.137.37     ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
170534 1321.12… 172.16.1.1        192.168.137.37     ICMP       590 Time-to-live exceeded (Time to live exceeded in transit)
168358 1173.59… 172.16.1.1        192.168.137.176    ICMP        94 Time-to-live exceeded (Time to live exceeded in transit)
168355 1173.35… 172.16.1.1        192.168.137.176    ICMP        94 Time-to-live exceeded (Time to live exceeded in transit)
168300 1168.19… 172.16.1.1        192.168.137.37     ICMP        94 Time-to-live exceeded (Time to live exceeded in transit)
```

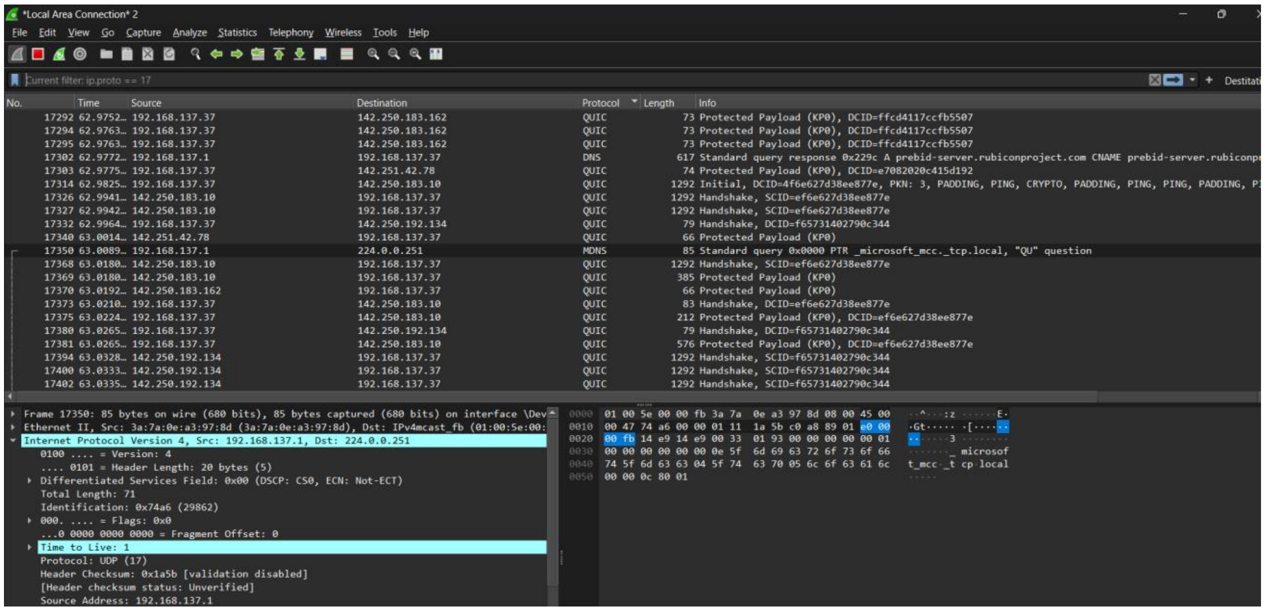
```
> Frame 17350: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Dev
> Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: IPv4mcast_fb (01:00:5e:00:
v Internet Protocol Version 4, Src: 192.168.137.1, Dst: 224.0.0.251
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 71
    Identification: 0x74a6 (29862)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  > Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x1a5b [validation disabled]
```

```
0000  01 00 5e 00 00 fb 3a 7a  0e a3 97 8d 08 00 45 00   ··^···:z ······E·
0010  00 47 74 a6 00 00 01 11  1a 5b c0 a8 89 01 e0 00   ·Gt····· ·[······
0020  00 fb 14 e9 14 e9 00 33  01 93 00 00 00 00 00 01   ·······3 ········
0030  00 00 00 00 00 00 0e 5f  6d 69 63 72 6f 73 6f 66   ·······_ microsof
0040  74 5f 6d 63 63 04 5f 74  63 70 05 6c 6f 63 61 6c   t_mcc·_t cp·local
0050  00 00 0c 80 01                                     ·····
```

14. ip.proto == 17

- Application: Filters packets with a specific IP protocol number (17 for UDP).

- Example: `ip.proto == 17`


Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: ip.proto == 17
Destitati

```
No.    Time       Source            Destination       Protocol  Length Info
 17292 62.9752… 192.168.137.37    142.250.183.162   QUIC        73 Protected Payload (KP0), DCID=ffcd4117ccfb5507
 17294 62.9763… 192.168.137.37    142.250.183.162   QUIC        73 Protected Payload (KP0), DCID=ffcd4117ccfb5507
 17295 62.9763… 192.168.137.37    142.250.183.162   QUIC        73 Protected Payload (KP0), DCID=ffcd4117ccfb5507
 17302 62.9772… 192.168.137.1     192.168.137.37    DNS        617 Standard query response 0x229c A prebid-server.rubiconproject.com CNAME prebid-server.rubiconpr
 17303 62.9775… 192.168.137.37    142.251.42.78     QUIC        74 Protected Payload (KP0), DCID=e7082020c415d192
 17314 62.9825… 192.168.137.37    142.250.183.10    QUIC      1292 Initial, DCID=4f6e627d38ee877e, PKN: 3, PADDING, PING, CRYPTO, PADDING, PING, PING, PADDING, P
 17326 62.9941… 142.250.183.10    192.168.137.37    QUIC      1292 Handshake, SCID=ef6e627d38ee877e
 17327 62.9942… 142.250.183.10    192.168.137.37    QUIC      1292 Handshake, SCID=ef6e627d38ee877e
 17332 62.9964… 192.168.137.37    142.250.192.134   QUIC        79 Handshake, DCID=f65731402790c344
 17340 63.0014… 142.251.42.78     192.168.137.37    QUIC        66 Protected Payload (KP0)
 17350 63.0089… 192.168.137.1     224.0.0.251       MDNS        85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
 17368 63.0180… 142.250.183.10    192.168.137.37    QUIC      1292 Handshake, SCID=ef6e627d38ee877e
 17369 63.0180… 142.250.183.10    192.168.137.37    QUIC       385 Protected Payload (KP0)
 17370 63.0192… 142.250.183.162   192.168.137.37    QUIC        66 Protected Payload (KP0)
 17373 63.0210… 192.168.137.37    142.250.183.10    QUIC        83 Handshake, DCID=ef6e627d38ee877e
 17375 63.0224… 192.168.137.37    142.250.183.10    QUIC       212 Protected Payload (KP0), DCID=ef6e627d38ee877e
 17380 63.0265… 192.168.137.37    142.250.192.134   QUIC        79 Handshake, DCID=f65731402790c344
 17381 63.0265… 192.168.137.37    142.250.183.10    QUIC       576 Protected Payload (KP0), DCID=ef6e627d38ee877e
 17394 63.0328… 142.250.192.134   192.168.137.37    QUIC      1292 Handshake, SCID=f65731402790c344
 17400 63.0333… 142.250.192.134   192.168.137.37    QUIC      1292 Handshake, SCID=f65731402790c344
 17402 63.0335… 142.250.192.134   192.168.137.37    QUIC      1292 Handshake, SCID=f65731402790c344
```

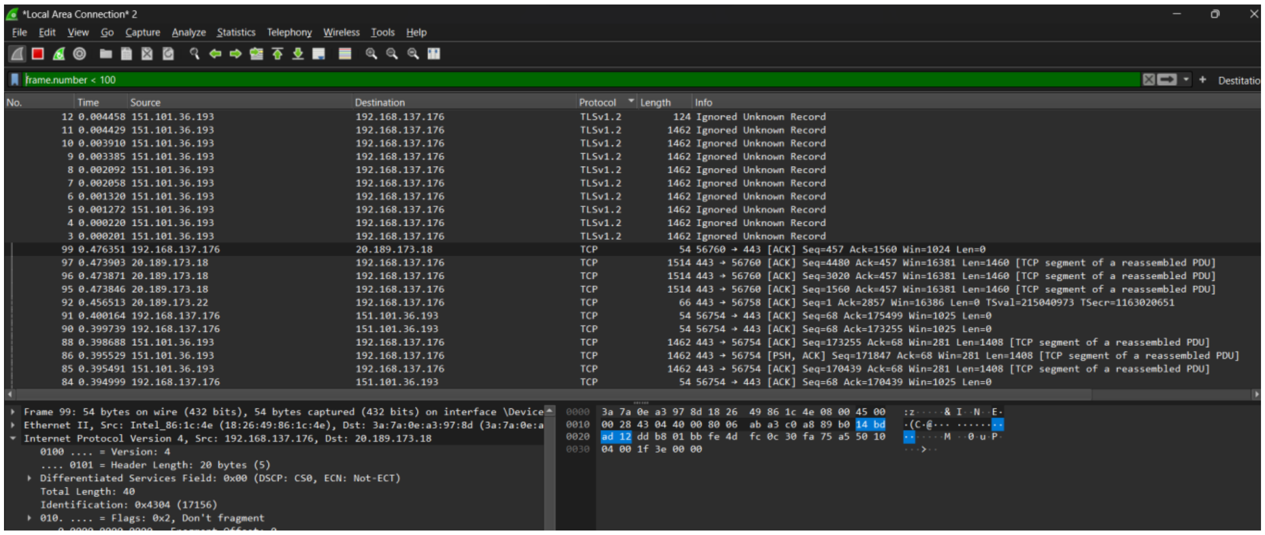
```
Frame 17350: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Dev
Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: IPv4mcast_fb (01:00:5e:00:
Internet Protocol Version 4, Src: 192.168.137.1, Dst: 224.0.0.251
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 71
    Identification: 0x74a6 (29862)
  000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 1
    Protocol: UDP (17)
    Header Checksum: 0x1a5b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.137.1
```

```
0000  01 00 5e 00 00 fb 3a 7a  0e a3 97 8d 08 00 45 00   ··^···:z ······E·
0010  00 47 74 a6 00 00 01 11  1a 5b c0 a8 89 01 e0 00   ·Gt····· ·[······
0020  00 fb 14 e9 14 e9 00 33  01 93 00 00 00 00 00 01   ·······3 ········
0030  00 00 00 00 00 00 0e 5f  6d 69 63 72 6f 73 6f 66   ·······_ microsof
0040  74 5f 6d 63 63 04 5f 74  63 70 05 6c 6f 63 61 6c   t_mcc·_t cp·local
0050  00 00 0c 80 01                                      ·····
```

15. frame.number < 100

- Application: Filters the first 100 frames in the capture.

- Example: `frame.number < 100`


Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
frame.number < 100
Destitatio

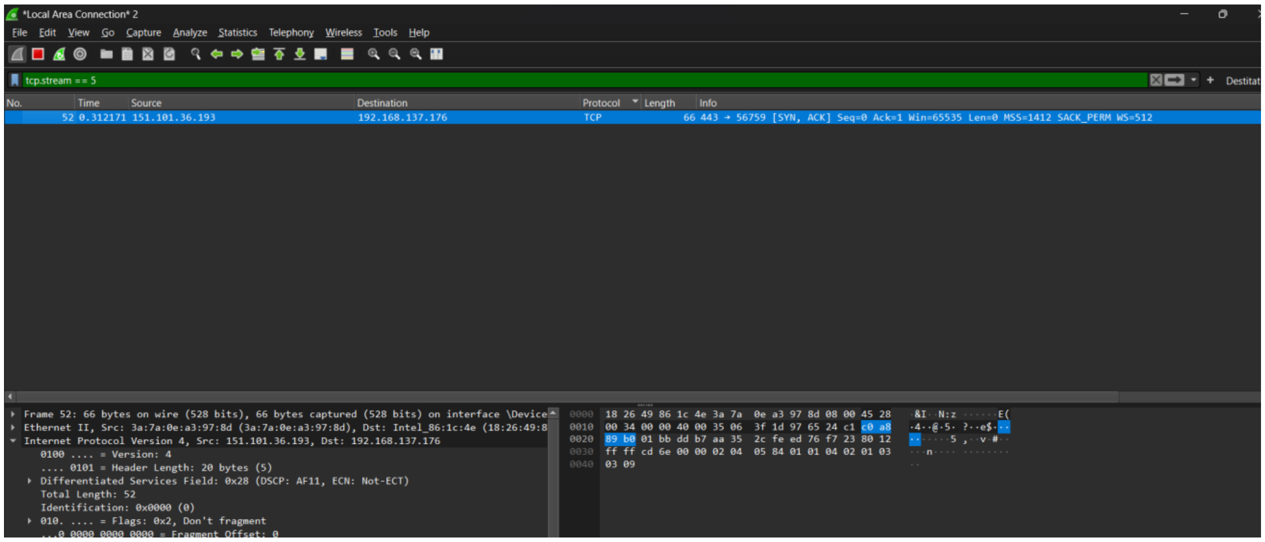
```
No.  Time     Source            Destination       Protocol  Length Info
  12 0.004458 151.101.36.193    192.168.137.176   TLSv1.2    124 Ignored Unknown Record
  11 0.004429 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
  10 0.003910 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
   9 0.003385 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
   8 0.002092 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
   7 0.002058 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
   6 0.001320 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
   5 0.001272 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
   4 0.000220 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
   3 0.000201 151.101.36.193    192.168.137.176   TLSv1.2   1462 Ignored Unknown Record
  99 0.476351 192.168.137.176   20.189.173.18     TCP         54 56760 → 443 [ACK] Seq=457 Ack=1560 Win=1024 Len=0
  97 0.473903 20.189.173.18     192.168.137.176   TCP       1514 443 → 56760 [ACK] Seq=4480 Ack=457 Win=16381 Len=1460 [TCP segment of a reassembled PDU]
  96 0.473871 20.189.173.18     192.168.137.176   TCP       1514 443 → 56760 [ACK] Seq=3020 Ack=457 Win=16381 Len=1460 [TCP segment of a reassembled PDU]
  95 0.473846 20.189.173.18     192.168.137.176   TCP       1514 443 → 56760 [ACK] Seq=1560 Ack=457 Win=16381 Len=1460 [TCP segment of a reassembled PDU]
  92 0.456513 20.189.173.22     192.168.137.176   TCP         66 443 → 56758 [ACK] Seq=1 Ack=2857 Win=16386 Len=0 TSval=215040973 TSecr=1163020651
  91 0.400164 192.168.137.176   151.101.36.193    TCP         54 56754 → 443 [ACK] Seq=68 Ack=175499 Win=1025 Len=0
  90 0.399739 192.168.137.176   151.101.36.193    TCP         54 56754 → 443 [ACK] Seq=68 Ack=173255 Win=1025 Len=0
  88 0.398688 151.101.36.193    192.168.137.176   TCP       1462 443 → 56754 [ACK] Seq=173255 Ack=68 Win=281 Len=1408 [TCP segment of a reassembled PDU]
  86 0.395529 151.101.36.193    192.168.137.176   TCP       1462 443 → 56754 [PSH, ACK] Seq=171847 Ack=68 Win=281 Len=1408 [TCP segment of a reassembled PDU]
  85 0.395491 151.101.36.193    192.168.137.176   TCP       1462 443 → 56754 [ACK] Seq=170439 Ack=68 Win=281 Len=1408 [TCP segment of a reassembled PDU]
  84 0.394999 192.168.137.176   151.101.36.193    TCP         54 56754 → 443 [ACK] Seq=68 Ack=170439 Win=1025 Len=0
```

```
Frame 99: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device
Ethernet II, Src: Intel_86:1c:4e (18:26:49:86:1c:4e), Dst: 3a:7a:0e:a3:97:8d (3a:7a:0e:a
Internet Protocol Version 4, Src: 192.168.137.176, Dst: 20.189.173.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x4304 (17156)
  010. .... = Flags: 0x2, Don't fragment
```

```
0000  3a 7a 0e a3 97 8d 18 26  49 86 1c 4e 08 00 45 00   :z·····& I··N··E·
0010  00 28 43 04 40 00 80 06  ab a3 c0 a8 89 b0 14 bd   ·(C·@··· ········
0020  ad 12 dd b8 01 bb fe 4d  fc 0c 30 fa 75 a5 50 10   ·······M ··0·u·P·
0030  04 00 1f 3e 00 00                                   ···>··
```

17. tcp.stream == x

- Application: Filters packets belonging to a specific TCP stream.
- Example: `tcp.stream == 5`


Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Destitat

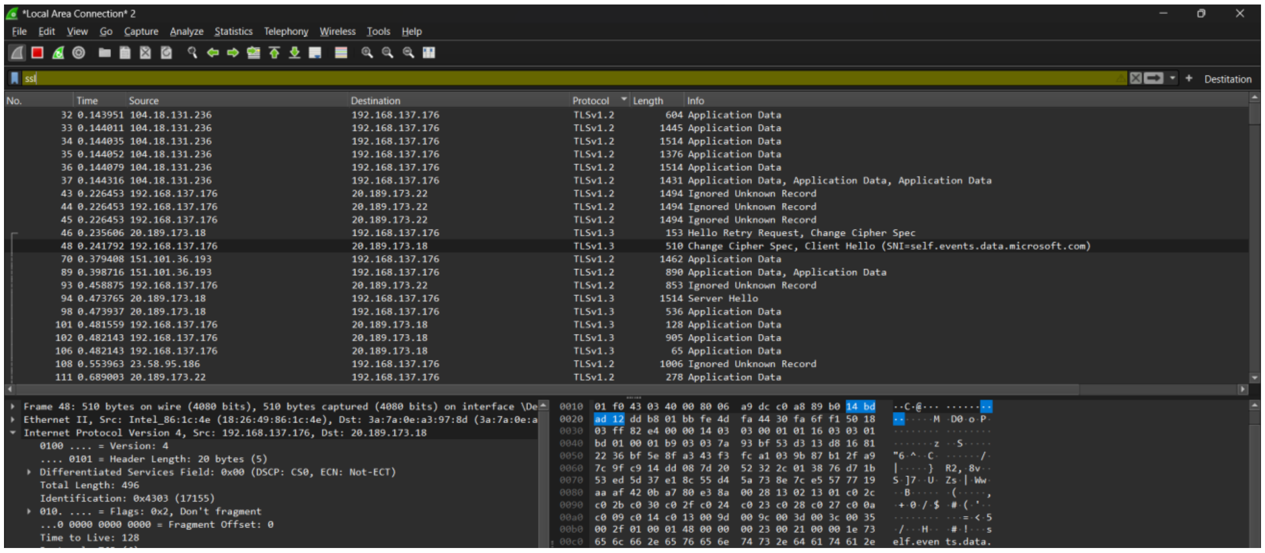
```
tcp.stream == 5

No.   Time     Source            Destination        Protocol  Length  Info
   52 0.312171 151.101.36.193    192.168.137.176    TCP           66  443 → 56759 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 SACK_PERM WS=512
```

```
› Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device
› Ethernet II, Src: 3a:7a:0e:a3:97:8d (3a:7a:0e:a3:97:8d), Dst: Intel_86:1c:4e (18:26:49:8
⌄ Internet Protocol Version 4, Src: 151.101.36.193, Dst: 192.168.137.176
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x0000 (0)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
```

```
0000  18 26 49 86 1c 4e 3a 7a  0e a3 97 8d 08 00 45 28   ·&I··N:z ······E(
0010  00 34 00 00 40 00 35 06  3f 1d 97 65 24 c1 c0 a8   ·4··@·5· ?··e$···
0020  89 b0 01 bb dd b7 aa 35  2c fe ed 76 f7 23 80 12   ·······5 ,··v·#··
0030  ff ff cd 6e 00 00 02 04  05 84 01 01 04 02 01 03   ···n···· ········
0040  03 09                                              ··
```

18. ssl

- Application: Filters SSL/TLS encrypted packets.
- Example: `ssl`


Local Area Connection 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Destitation

```
ssl

No.   Time     Source            Destination        Protocol  Length  Info
   32 0.143951 104.18.131.236    192.168.137.176    TLSv1.2      604  Application Data
   33 0.144011 104.18.131.236    192.168.137.176    TLSv1.2     1445  Application Data
   34 0.144035 104.18.131.236    192.168.137.176    TLSv1.2     1514  Application Data
   35 0.144052 104.18.131.236    192.168.137.176    TLSv1.2     1376  Application Data
   36 0.144079 104.18.131.236    192.168.137.176    TLSv1.2     1514  Application Data
   37 0.144316 104.18.131.236    192.168.137.176    TLSv1.2     1431  Application Data, Application Data, Application Data
   43 0.226453 192.168.137.176   20.189.173.22      TLSv1.2     1494  Ignored Unknown Record
   44 0.226453 192.168.137.176   20.189.173.22      TLSv1.2     1494  Ignored Unknown Record
   45 0.226453 192.168.137.176   20.189.173.22      TLSv1.2     1494  Ignored Unknown Record
   46 0.235606 20.189.173.18     192.168.137.176    TLSv1.3      153  Hello Retry Request, Change Cipher Spec
   48 0.241792 192.168.137.176   20.189.173.18      TLSv1.3      510  Change Cipher Spec, Client Hello (SNI=self.events.data.microsoft.com)
   70 0.379408 151.101.36.193    192.168.137.176    TLSv1.2     1462  Application Data
   89 0.398716 151.101.36.193    192.168.137.176    TLSv1.2      890  Application Data, Application Data
   93 0.458875 192.168.137.176   20.189.173.22      TLSv1.2      853  Ignored Unknown Record
   94 0.473765 20.189.173.18     192.168.137.176    TLSv1.3     1514  Server Hello
   98 0.473937 20.189.173.18     192.168.137.176    TLSv1.3      536  Application Data
  101 0.481559 192.168.137.176   20.189.173.18      TLSv1.3      128  Application Data
  102 0.482143 192.168.137.176   20.189.173.18      TLSv1.3      905  Application Data
  106 0.482143 192.168.137.176   20.189.173.18      TLSv1.3       65  Application Data
  108 0.553963 23.58.95.186      192.168.137.176    TLSv1.2     1006  Ignored Unknown Record
  111 0.689003 20.189.173.22     192.168.137.176    TLSv1.2      278  Application Data
```

```
› Frame 48: 510 bytes on wire (4080 bits), 510 bytes captured (4080 bits) on interface \De
› Ethernet II, Src: Intel_86:1c:4e (18:26:49:86:1c:4e), Dst: 3a:7a:0e:a3:97:8d (3a:7a:0e:a
⌄ Internet Protocol Version 4, Src: 192.168.137.176, Dst: 20.189.173.18
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 496
    Identification: 0x4303 (17155)
  › 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
```

```
0010  01 f0 43 03 40 00 80 06  a9 dc c0 a8 89 b0 14 bd   ··C·@··· ········
0020  ad 12 dd b8 01 bb fe 4d  fa 44 30 fa 6f f1 50 18   ·······M ·D0·o·P·
0030  03 ff 82 e4 00 00 14 03  03 00 01 01 16 03 03 01   ········ ········
0040  bd 01 00 01 b9 03 03 7a  93 bf 53 d3 13 d8 16 81   ·······z ··S·····
0050  22 36 bf 5e 8f a3 43 f3  fc a1 03 9b 87 b1 2f a9   "6·^··C· ······/·
0060  7c 9f c9 14 dd 08 7d 20  52 32 2c 01 38 76 d7 1b   |·····}  R2,·8v··
0070  53 ed 5d 37 e1 8c 55 d4  5a 73 8e 7c e5 57 77 19   S·]7··U· Zs·|·Ww·
0080  aa af 42 0b a7 80 e3 8a  00 28 13 02 13 01 c0 2c   ··B····· ·(·····,
0090  c0 2b c0 30 c0 2f c0 24  c0 23 c0 28 c0 27 c0 0a   ·+·0·/·$ ·#·(·'··
00a0  c0 09 c0 14 c0 13 00 9d  00 9c 00 3d 00 3c 00 35   ········ ···=·<·5
00b0  00 2f 01 00 01 48 00 00  00 23 00 21 00 00 1e 73   ·/···H·· ·#·!···s
00c0  65 6c 66 2e 65 76 65 6e  74 73 2e 64 61 74 61 2e   elf.even ts.data.
```

19. ip.addr == x.x.x.x && http.request.method == "POST"

- Application: Filters HTTP POST requests from a specific IP address.
- Example: `ip.addr == 192.168.1.1 && http.request.method == "POST"`

20. frame.time_delta > 0.1

- Application: Filters packets with a time difference between frames greater than 0.1 seconds.
- Example: `frame.time_delta > 0.1`