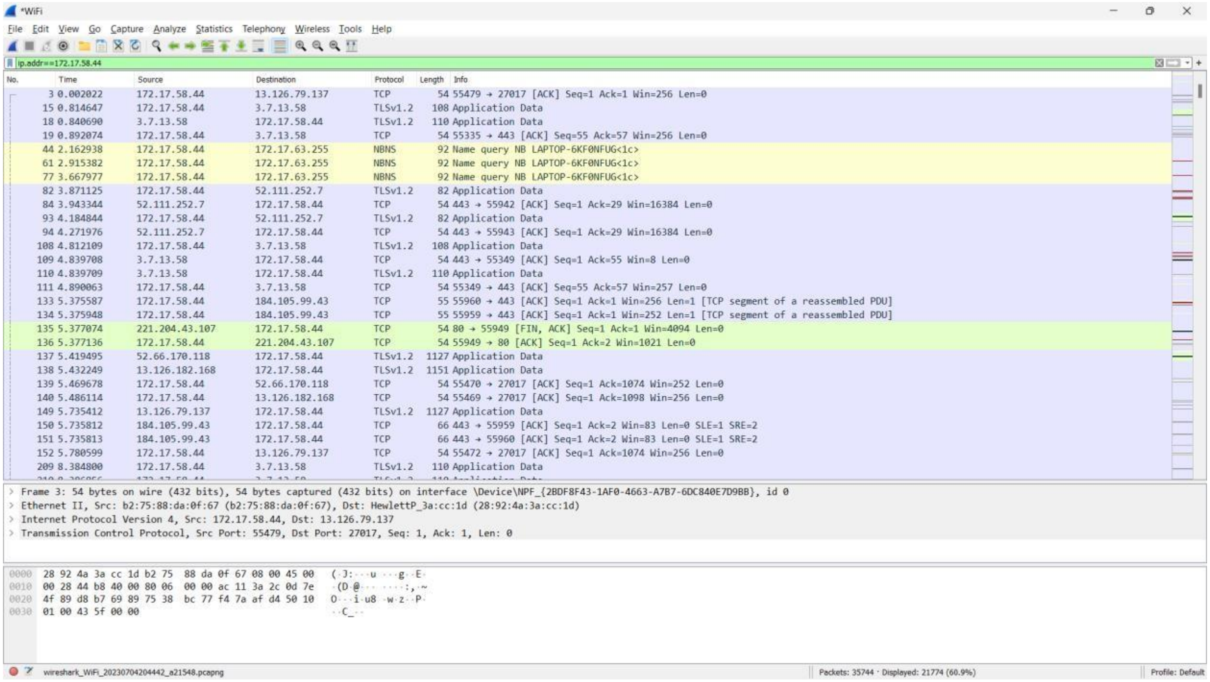
DIGITAL ASSIGNMENT 4 **21BKT0091**

GAGAN CHAUDHARY

4 July 2023

AIM:- . To filter packets based on various criteria's.

1. Filtering traffic on specific IP Address:


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

ip.addr==172.17.58.44

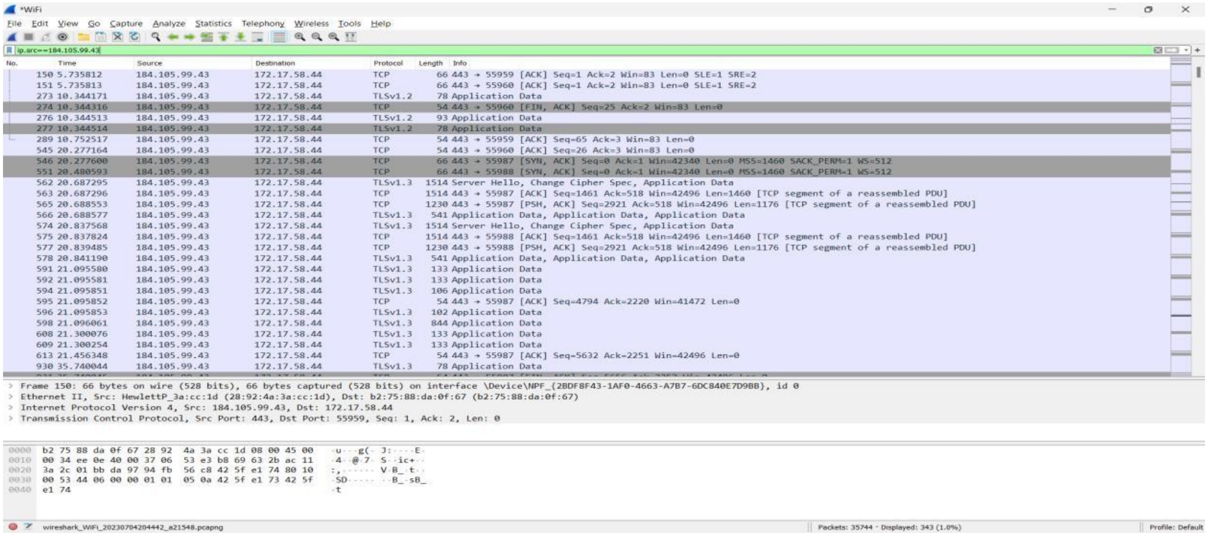
```
No.  Time      Source          Destination     Protocol Length Info
   3 0.002022  172.17.58.44    13.126.79.137   TCP        54 55479 → 27017 [ACK] Seq=1 Ack=1 Win=256 Len=0
  15 0.814647  172.17.58.44    3.7.13.58       TLSv1.2   108 Application Data
  18 0.840690  3.7.13.58       172.17.58.44    TLSv1.2   110 Application Data
  19 0.892074  172.17.58.44    3.7.13.58       TCP        54 55335 → 443 [ACK] Seq=55 Ack=57 Win=256 Len=0
  44 2.162938  172.17.58.44    172.17.63.255   NBNS       92 Name query NB LAPTOP-6KF0NFUG<1c>
  61 2.915382  172.17.58.44    172.17.63.255   NBNS       92 Name query NB LAPTOP-6KF0NFUG<1c>
  77 3.667977  172.17.58.44    172.17.63.255   NBNS       92 Name query NB LAPTOP-6KF0NFUG<1c>
  82 3.871125  172.17.58.44    52.111.252.7    TLSv1.2    82 Application Data
  84 3.943344  52.111.252.7    172.17.58.44    TCP        54 443 → 55942 [ACK] Seq=1 Ack=29 Win=16384 Len=0
  93 4.184844  172.17.58.44    52.111.252.7    TLSv1.2    82 Application Data
  94 4.271976  52.111.252.7    172.17.58.44    TCP        54 443 → 55943 [ACK] Seq=1 Ack=29 Win=16384 Len=0
 108 4.812109  172.17.58.44    3.7.13.58       TLSv1.2   108 Application Data
 109 4.839708  3.7.13.58       172.17.58.44    TCP        54 443 → 55349 [ACK] Seq=1 Ack=55 Win=8 Len=0
 110 4.839709  3.7.13.58       172.17.58.44    TLSv1.2   110 Application Data
 111 4.890063  172.17.58.44    3.7.13.58       TCP        54 55349 → 443 [ACK] Seq=55 Ack=57 Win=257 Len=0
 133 5.375587  172.17.58.44    184.105.99.43   TCP        55 55960 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
 134 5.375948  172.17.58.44    184.105.99.43   TCP        55 55959 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled PDU]
 135 5.377074  221.204.43.107  172.17.58.44    TCP        54 80 → 55949 [FIN, ACK] Seq=1 Ack=1 Win=4094 Len=0
 136 5.377136  172.17.58.44    221.204.43.107  TCP        54 55949 → 80 [ACK] Seq=1 Ack=2 Win=1021 Len=0
 137 5.419495  52.66.170.118   172.17.58.44    TLSv1.2  1127 Application Data
 138 5.432249  13.126.182.168  172.17.58.44    TLSv1.2  1151 Application Data
 139 5.469678  172.17.58.44    52.66.170.118   TCP        54 55470 → 27017 [ACK] Seq=1 Ack=1074 Win=252 Len=0
 140 5.486114  172.17.58.44    13.126.182.168  TCP        54 55469 → 27017 [ACK] Seq=1 Ack=1098 Win=256 Len=0
 149 5.735412  13.126.79.137   172.17.58.44    TLSv1.2  1127 Application Data
 150 5.735812  184.105.99.43   172.17.58.44    TCP        66 443 → 55959 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
 151 5.735813  184.105.99.43   172.17.58.44    TCP        66 443 → 55960 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
 152 5.780599  172.17.58.44    13.126.79.137   TCP        54 55472 → 27017 [ACK] Seq=1 Ack=1074 Win=256 Len=0
 209 8.384800  172.17.58.44    3.7.13.58       TLSv1.2   110 Application Data
```

```
> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 13.126.79.137
> Transmission Control Protocol, Src Port: 55479, Dst Port: 27017, Seq: 1, Ack: 1, Len: 0
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 28 44 b8 40 00 80 06  00 00 ac 11 3a 2c 0d 7e   ·(D·@··· ····:,·~
0020  4f 89 d8 b7 69 89 75 38  bc 77 f4 7a af d4 50 10   O···i·u8 ·w·z··P·
0030  01 00 43 5f 00 00                                  ··C_··
```

wireshark_WiFi_20230704204442_a21548.pcapng | Packets: 35744 · Displayed: 21774 (60.9%) | Profile: Default

2. Filter by source address:


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

ip.src==184.105.99.43

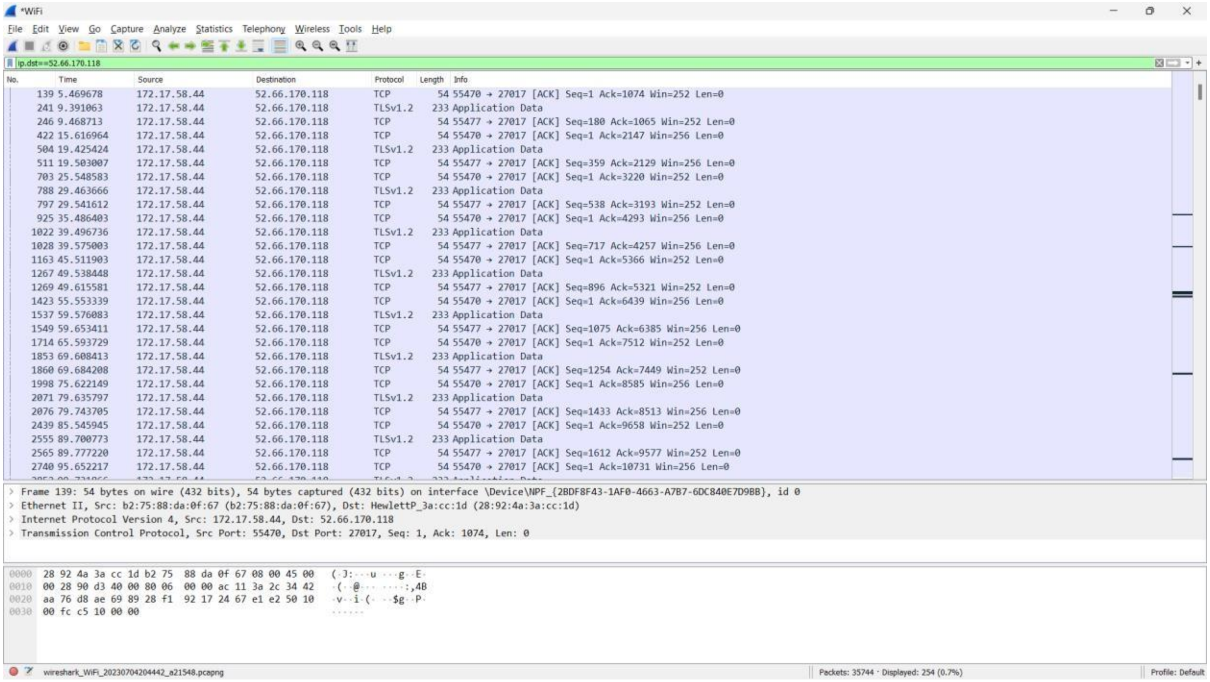
```
No.  Time       Source          Destination     Protocol Length Info
 150 5.735812   184.105.99.43   172.17.58.44    TCP        66 443 → 55959 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
 151 5.735813   184.105.99.43   172.17.58.44    TCP        66 443 → 55960 [ACK] Seq=1 Ack=2 Win=83 Len=0 SLE=1 SRE=2
 273 10.344171  184.105.99.43   172.17.58.44    TLSv1.2    78 Application Data
 274 10.344316  184.105.99.43   172.17.58.44    TCP        54 443 → 55960 [FIN, ACK] Seq=25 Ack=2 Win=83 Len=0
 276 10.344513  184.105.99.43   172.17.58.44    TLSv1.2    93 Application Data
 277 10.344514  184.105.99.43   172.17.58.44    TLSv1.2    78 Application Data
 289 10.752517  184.105.99.43   172.17.58.44    TCP        54 443 → 55959 [ACK] Seq=65 Ack=3 Win=83 Len=0
 545 20.277164  184.105.99.43   172.17.58.44    TCP        54 443 → 55960 [ACK] Seq=26 Ack=3 Win=83 Len=0
 546 20.277600  184.105.99.43   172.17.58.44    TCP        66 443 → 55987 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM=1 WS=512
 551 20.480593  184.105.99.43   172.17.58.44    TCP        66 443 → 55988 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM=1 WS=512
 562 20.687295  184.105.99.43   172.17.58.44    TLSv1.3  1514 Server Hello, Change Cipher Spec, Application Data
 563 20.687296  184.105.99.43   172.17.58.44    TCP      1514 443 → 55987 [ACK] Seq=1461 Ack=518 Win=42496 Len=1460 [TCP segment of a reassembled PDU]
 565 20.688553  184.105.99.43   172.17.58.44    TCP      1230 443 → 55987 [PSH, ACK] Seq=2921 Ack=518 Win=42496 Len=1176 [TCP segment of a reassembled PDU]
 566 20.688577  184.105.99.43   172.17.58.44    TLSv1.3   541 Application Data, Application Data, Application Data
 574 20.837568  184.105.99.43   172.17.58.44    TLSv1.3  1514 Server Hello, Change Cipher Spec, Application Data
 575 20.837824  184.105.99.43   172.17.58.44    TCP      1514 443 → 55988 [ACK] Seq=1461 Ack=518 Win=42496 Len=1460 [TCP segment of a reassembled PDU]
 577 20.839485  184.105.99.43   172.17.58.44    TCP      1230 443 → 55988 [PSH, ACK] Seq=2921 Ack=518 Win=42496 Len=1176 [TCP segment of a reassembled PDU]
 578 20.841190  184.105.99.43   172.17.58.44    TLSv1.3   541 Application Data, Application Data, Application Data
 591 21.095580  184.105.99.43   172.17.58.44    TLSv1.3   133 Application Data
 592 21.095581  184.105.99.43   172.17.58.44    TLSv1.3   133 Application Data
 594 21.095851  184.105.99.43   172.17.58.44    TLSv1.3   106 Application Data
 595 21.095852  184.105.99.43   172.17.58.44    TCP        54 443 → 55987 [ACK] Seq=4794 Ack=2220 Win=41472 Len=0
 596 21.095853  184.105.99.43   172.17.58.44    TLSv1.3   102 Application Data
 598 21.096061  184.105.99.43   172.17.58.44    TLSv1.3   844 Application Data
 608 21.300076  184.105.99.43   172.17.58.44    TLSv1.3   133 Application Data
 609 21.300254  184.105.99.43   172.17.58.44    TLSv1.3   133 Application Data
 613 21.456348  184.105.99.43   172.17.58.44    TCP        54 443 → 55987 [ACK] Seq=5632 Ack=2251 Win=42496 Len=0
 930 35.740044  184.105.99.43   172.17.58.44    TLSv1.3    78 Application Data
```

```
> Frame 150: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d), Dst: b2:75:88:da:0f:67 (b2:75:88:da:0f:67)
> Internet Protocol Version 4, Src: 184.105.99.43, Dst: 172.17.58.44
> Transmission Control Protocol, Src Port: 443, Dst Port: 55959, Seq: 1, Ack: 2, Len: 0
```

```
0000  b2 75 88 da 0f 67 28 92  4a 3a cc 1d 08 00 45 00   ·u···g(· J:····E·
0010  00 34 ee 0e 40 00 37 06  53 e3 b8 69 63 2b ac 11   ·4··@·7· S··ic+··
0020  3a 2c 01 bb da 97 94 fb  56 c8 42 5f e1 74 80 10   :,······ V·B_·t··
0030  00 53 44 06 00 00 01 01  05 0a 42 5f e1 73 42 5f   ·SD····· ··B_·sB_
0040  e1 74                                              ·t
```

wireshark_WiFi_20230704204442_a21548.pcapng | Packets: 35744 · Displayed: 343 (1.0%) | Profile: Default

3. Filter by destination address


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

ip.dst==52.66.170.118

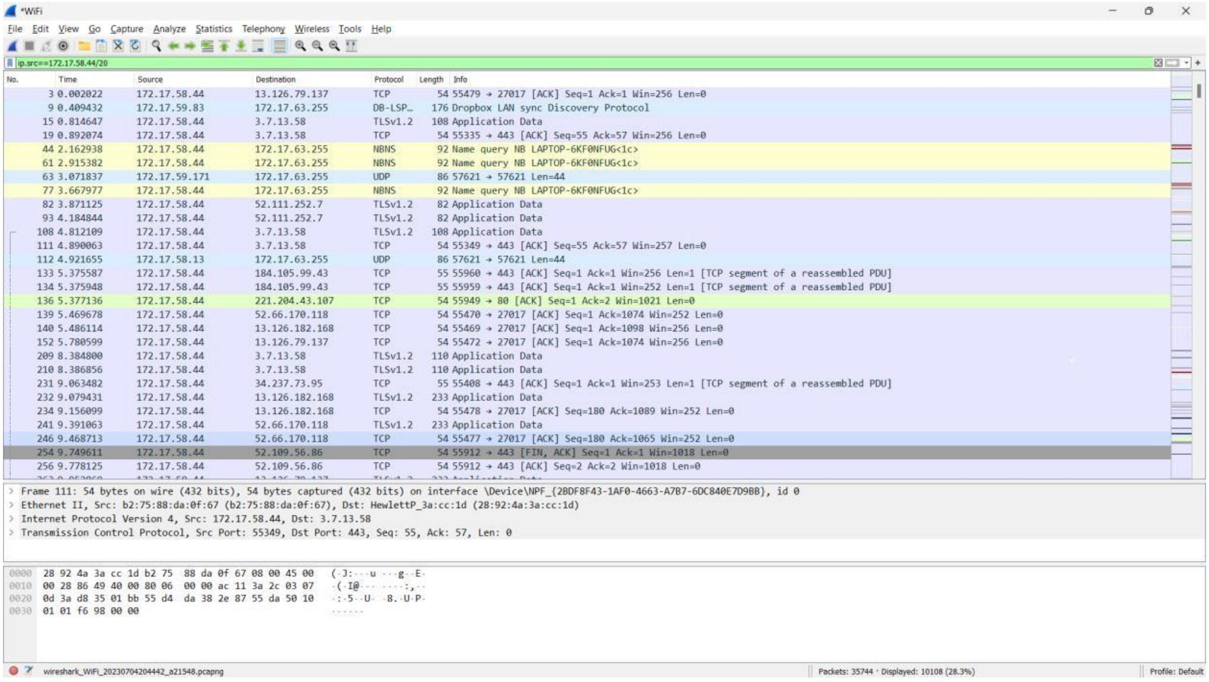
```
No.     Time        Source          Destination     Protocol  Length Info
    139 5.469678    172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=1074 Win=252 Len=0
    241 9.391063    172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
    246 9.468713    172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=180 Ack=1065 Win=252 Len=0
    422 15.616964   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=2147 Win=256 Len=0
    504 19.425424   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
    511 19.503007   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=359 Ack=2129 Win=256 Len=0
    703 25.548583   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=3220 Win=252 Len=0
    788 29.463666   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
    797 29.541612   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=538 Ack=3193 Win=252 Len=0
    925 35.486403   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=4293 Win=256 Len=0
   1022 39.496736   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
   1028 39.575003   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=717 Ack=4257 Win=256 Len=0
   1163 45.511903   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=5366 Win=252 Len=0
   1267 49.538448   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
   1269 49.615581   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=896 Ack=5321 Win=252 Len=0
   1423 55.553339   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=6439 Win=256 Len=0
   1537 59.576083   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
   1549 59.653411   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=1075 Ack=6385 Win=256 Len=0
   1714 65.593729   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=7512 Win=252 Len=0
   1853 69.608413   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
   1860 69.684208   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=1254 Ack=7449 Win=252 Len=0
   1998 75.622149   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=8585 Win=256 Len=0
   2071 79.635797   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
   2076 79.743705   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=1433 Ack=8513 Win=256 Len=0
   2439 85.545945   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=9658 Win=252 Len=0
   2555 89.700773   172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
   2565 89.777220   172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=1612 Ack=9577 Win=252 Len=0
   2740 95.652217   172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=10731 Win=256 Len=0
```

```
> Frame 139: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 52.66.170.118
> Transmission Control Protocol, Src Port: 55470, Dst Port: 27017, Seq: 1, Ack: 1074, Len: 0
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 28 90 d3 40 00 80 06  00 00 ac 11 3a 2c 34 42   ·(··@··· ····:,4B
0020  aa 76 d8 ae 69 89 28 f1  92 17 24 67 e1 e2 50 10   ·v··i·(· ··$g··P·
0030  00 fc c5 10 00 00                                  ······
```

wireshark_WiFi_20230704204442_a21548.pcapng   Packets: 35744 · Displayed: 254 (0.7%)   Profile: Default

4. Filter by IP subnet


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

ip.src==172.17.58.44/20

```
No.     Time        Source          Destination     Protocol  Length Info
      3 0.002022    172.17.58.44    13.126.79.137   TCP          54 55479 → 27017 [ACK] Seq=1 Ack=1 Win=256 Len=0
      9 0.409432    172.17.59.83    172.17.63.255   DB-LSP…     176 Dropbox LAN sync Discovery Protocol
     15 0.814647    172.17.58.44    3.7.13.58       TLSv1.2     108 Application Data
     19 0.892074    172.17.58.44    3.7.13.58       TCP          54 55335 → 443 [ACK] Seq=55 Ack=57 Win=256 Len=0
     44 2.162938    172.17.58.44    172.17.63.255   NBNS         92 Name query NB LAPTOP-6KF0NFUG<1c>
     61 2.915382    172.17.58.44    172.17.63.255   NBNS         92 Name query NB LAPTOP-6KF0NFUG<1c>
     63 3.071837    172.17.59.171   172.17.63.255   UDP          86 57621 → 57621 Len=44
     77 3.667977    172.17.58.44    172.17.63.255   NBNS         92 Name query NB LAPTOP-6KF0NFUG<1c>
     82 3.871125    172.17.58.44    52.111.252.7    TLSv1.2      82 Application Data
     93 4.184844    172.17.58.44    52.111.252.7    TLSv1.2      82 Application Data
    108 4.812109    172.17.58.44    3.7.13.58       TLSv1.2     108 Application Data
    111 4.890063    172.17.58.44    3.7.13.58       TCP          54 55349 → 443 [ACK] Seq=55 Ack=57 Win=257 Len=0
    112 4.921655    172.17.58.13    172.17.63.255   UDP          86 57621 → 57621 Len=44
    133 5.375587    172.17.58.44    184.105.99.43   TCP          55 55960 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
    134 5.375948    172.17.58.44    184.105.99.43   TCP          55 55959 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1 [TCP segment of a reassembled PDU]
    136 5.377136    172.17.58.44    221.204.43.107  TCP          54 55949 → 80 [ACK] Seq=1 Ack=2 Win=1021 Len=0
    139 5.469678    172.17.58.44    52.66.170.118   TCP          54 55470 → 27017 [ACK] Seq=1 Ack=1074 Win=252 Len=0
    140 5.486114    172.17.58.44    13.126.182.168  TCP          54 55469 → 27017 [ACK] Seq=1 Ack=1098 Win=256 Len=0
    152 5.780599    172.17.58.44    13.126.79.137   TCP          54 55472 → 27017 [ACK] Seq=1 Ack=1074 Win=256 Len=0
    209 8.384800    172.17.58.44    3.7.13.58       TLSv1.2     110 Application Data
    210 8.386856    172.17.58.44    3.7.13.58       TLSv1.2     110 Application Data
    231 9.063482    172.17.58.44    34.237.73.95    TCP          55 55408 → 443 [ACK] Seq=1 Ack=1 Win=253 Len=1 [TCP segment of a reassembled PDU]
    232 9.079431    172.17.58.44    13.126.182.168  TLSv1.2     233 Application Data
    234 9.156099    172.17.58.44    13.126.182.168  TCP          54 55478 → 27017 [ACK] Seq=180 Ack=1089 Win=252 Len=0
    241 9.391063    172.17.58.44    52.66.170.118   TLSv1.2     233 Application Data
    246 9.468713    172.17.58.44    52.66.170.118   TCP          54 55477 → 27017 [ACK] Seq=180 Ack=1065 Win=252 Len=0
    254 9.749611    172.17.58.44    52.109.56.86    TCP          54 55912 → 443 [FIN, ACK] Seq=1 Ack=1 Win=1018 Len=0
    256 9.778125    172.17.58.44    52.109.56.86    TCP          54 55912 → 443 [ACK] Seq=2 Ack=2 Win=1018 Len=0
```

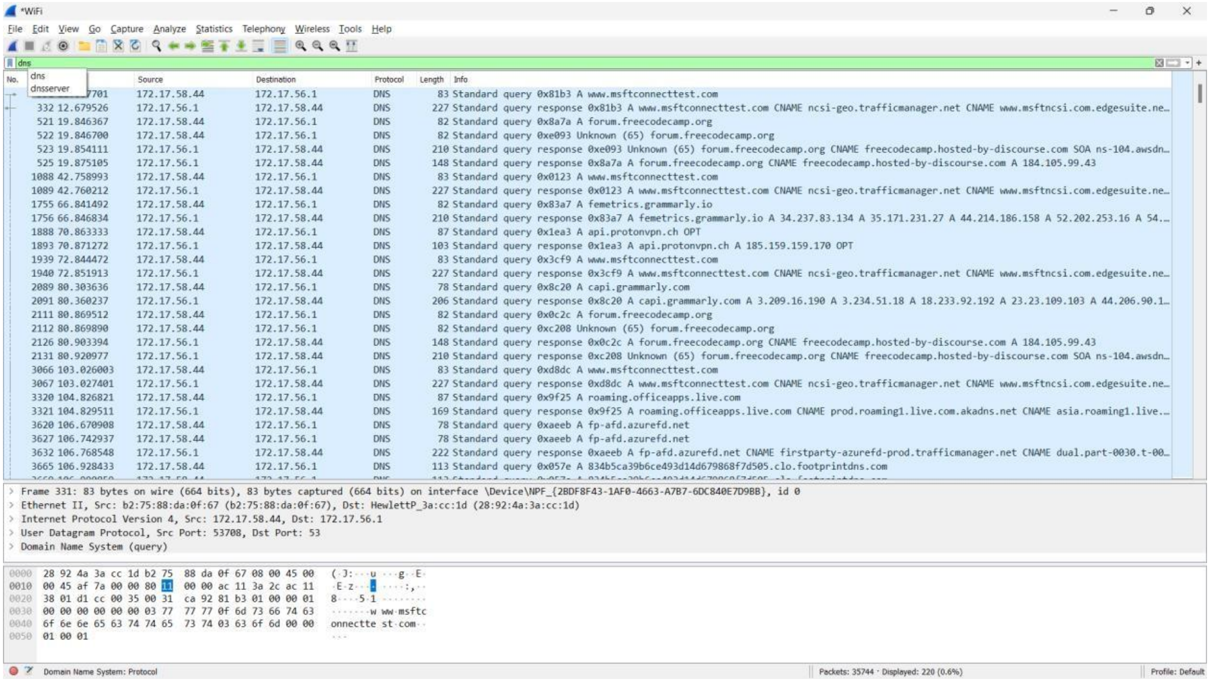
```
> Frame 111: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 3.7.13.58
> Transmission Control Protocol, Src Port: 55349, Dst Port: 443, Seq: 55, Ack: 57, Len: 0
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 28 86 49 40 00 80 06  00 00 ac 11 3a 2c 03 07   ·(·I@··· ····:,··
0020  0d 3a d8 35 01 bb 55 d4  da 38 2e 87 55 da 50 10   ·:·5··U· ·8.·U·P·
0030  01 01 f6 98 00 00                                  ······
```

wireshark_WiFi_20230704204442_a21548.pcapng   Packets: 35744 · Displayed: 10108 (28.3%)   Profile: Default

5. Filter traffic based on protocol

dns



*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver

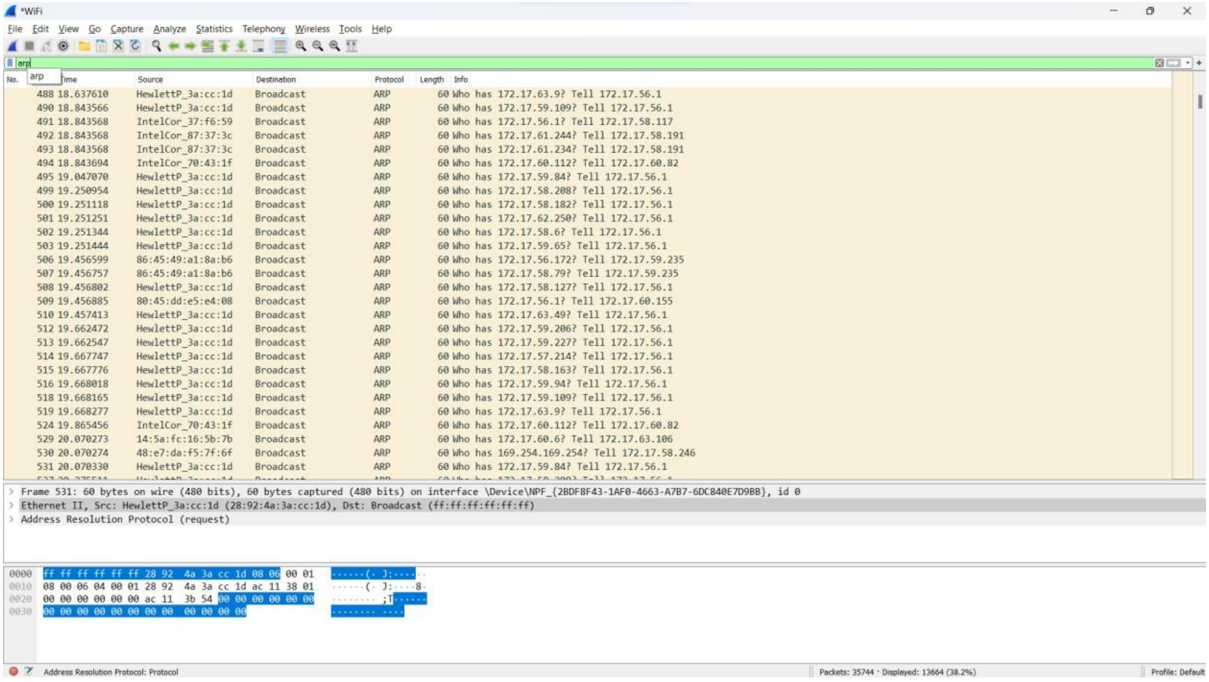
```
No.     Time          Source          Destination     Protocol  Length Info
        7701          172.17.58.44    172.17.56.1     DNS        83 Standard query 0x81b3 A www.msftconnecttest.com
  332 12.679526       172.17.56.1     172.17.58.44    DNS       227 Standard query response 0x81b3 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
  521 19.846367       172.17.58.44    172.17.56.1     DNS        82 Standard query 0x8a7a A forum.freecodecamp.org
  522 19.846700       172.17.58.44    172.17.56.1     DNS        82 Standard query 0xe093 Unknown (65) forum.freecodecamp.org
  523 19.854111       172.17.56.1     172.17.58.44    DNS       210 Standard query response 0xe093 Unknown (65) forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com SOA ns-104.awsdn…
  525 19.875105       172.17.56.1     172.17.58.44    DNS       148 Standard query response 0x8a7a A forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com A 184.105.99.43
 1088 42.758993       172.17.58.44    172.17.56.1     DNS        83 Standard query 0x0123 A www.msftconnecttest.com
 1089 42.760212       172.17.56.1     172.17.58.44    DNS       227 Standard query response 0x0123 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
 1755 66.841492       172.17.58.44    172.17.56.1     DNS        82 Standard query 0x83a7 A femetrics.grammarly.io
 1756 66.846834       172.17.56.1     172.17.58.44    DNS       210 Standard query response 0x83a7 A femetrics.grammarly.io A 34.237.83.134 A 35.171.231.27 A 44.214.186.158 A 52.202.253.16 A 54.…
 1888 70.863333       172.17.58.44    172.17.56.1     DNS        87 Standard query 0x1ea3 A api.protonvpn.ch OPT
 1893 70.871272       172.17.56.1     172.17.58.44    DNS       103 Standard query response 0x1ea3 A api.protonvpn.ch A 185.159.159.170 OPT
 1939 72.844472       172.17.58.44    172.17.56.1     DNS        83 Standard query 0x3cf9 A www.msftconnecttest.com
 1940 72.851913       172.17.56.1     172.17.58.44    DNS       227 Standard query response 0x3cf9 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
 2089 80.303636       172.17.58.44    172.17.56.1     DNS        78 Standard query 0x8c20 A capi.grammarly.com
 2091 80.360237       172.17.56.1     172.17.58.44    DNS       206 Standard query response 0x8c20 A capi.grammarly.com A 3.209.16.190 A 3.234.51.18 A 18.233.92.192 A 23.23.109.103 A 44.206.90.1…
 2111 80.869512       172.17.58.44    172.17.56.1     DNS        82 Standard query 0x0c2c A forum.freecodecamp.org
 2112 80.869890       172.17.58.44    172.17.56.1     DNS        82 Standard query 0xc208 Unknown (65) forum.freecodecamp.org
 2126 80.903394       172.17.56.1     172.17.58.44    DNS       148 Standard query response 0x0c2c A forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com A 184.105.99.43
 2131 80.920977       172.17.56.1     172.17.58.44    DNS       210 Standard query response 0xc208 Unknown (65) forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com SOA ns-104.awsdn…
 3066 103.026003      172.17.58.44    172.17.56.1     DNS        83 Standard query 0xd8dc A www.msftconnecttest.com
 3067 103.027401      172.17.56.1     172.17.58.44    DNS       227 Standard query response 0xd8dc A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
 3320 104.826821      172.17.58.44    172.17.56.1     DNS        87 Standard query 0x9f25 A roaming.officeapps.live.com
 3321 104.829511      172.17.56.1     172.17.58.44    DNS       169 Standard query response 0x9f25 A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net CNAME asia.roaming1.live.…
 3620 106.670908      172.17.58.44    172.17.56.1     DNS        78 Standard query 0xaeeb A fp-afd.azurefd.net
 3627 106.742937      172.17.58.44    172.17.56.1     DNS        78 Standard query 0xaeeb A fp-afd.azurefd.net
 3632 106.768548      172.17.56.1     172.17.58.44    DNS       222 Standard query response 0xaeeb A fp-afd.azurefd.net CNAME firstparty-azurefd-prod.trafficmanager.net CNAME dual.part-0030.t-00…
 3665 106.928433      172.17.58.44    172.17.56.1     DNS       113 Standard query 0x057e A 834b5ca39b6ce493d14d679868f7d505.clo.footprintdns.com
```

```
> Frame 331: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 172.17.56.1
> User Datagram Protocol, Src Port: 53708, Dst Port: 53
> Domain Name System (query)
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 45 af 7a 00 00 80 11  00 00 ac 11 3a 2c ac 11   ·E·z···· ····:,··
0020  38 01 d1 cc 00 35 00 31  ca 92 81 b3 01 00 00 01   8····5·1 ········
0030  00 00 00 00 00 00 03 77  77 77 0f 6d 73 66 74 63   ·······w ww·msftc
0040  6f 6e 6e 65 63 74 74 65  73 74 03 63 6f 6d 00 00   onnectte st·com··
0050  01 00 01                                           ···
```

Domain Name System: Protocol | Packets: 35744 · Displayed: 220 (0.6%) | Profile: Default

Arp



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

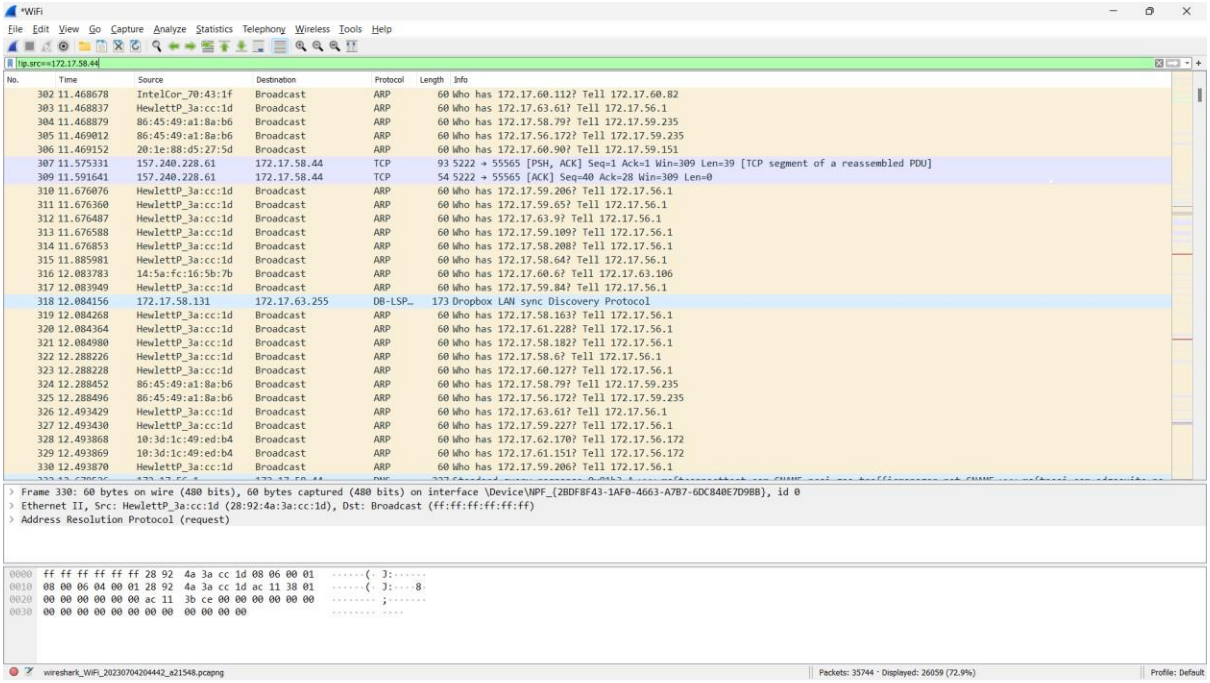
```
No.     Time          Source              Destination  Protocol  Length Info
  488 18.637610       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.63.9? Tell 172.17.56.1
  490 18.843566       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.109? Tell 172.17.56.1
  491 18.843568       IntelCor_37:f6:59   Broadcast    ARP        60 Who has 172.17.56.1? Tell 172.17.58.117
  492 18.843568       IntelCor_87:37:3c   Broadcast    ARP        60 Who has 172.17.61.244? Tell 172.17.58.191
  493 18.843568       IntelCor_87:37:3c   Broadcast    ARP        60 Who has 172.17.61.234? Tell 172.17.58.191
  494 18.843694       IntelCor_70:43:1f   Broadcast    ARP        60 Who has 172.17.60.112? Tell 172.17.60.82
  495 19.047070       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.84? Tell 172.17.56.1
  499 19.250954       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.58.208? Tell 172.17.56.1
  500 19.251118       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.58.182? Tell 172.17.56.1
  501 19.251251       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.62.250? Tell 172.17.56.1
  502 19.251344       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.58.6? Tell 172.17.56.1
  503 19.251444       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.65? Tell 172.17.56.1
  506 19.456599       86:45:49:a1:8a:b6   Broadcast    ARP        60 Who has 172.17.56.172? Tell 172.17.59.235
  507 19.456757       86:45:49:a1:8a:b6   Broadcast    ARP        60 Who has 172.17.58.79? Tell 172.17.59.235
  508 19.456802       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.58.127? Tell 172.17.56.1
  509 19.456885       80:45:dd:e5:e4:08   Broadcast    ARP        60 Who has 172.17.56.1? Tell 172.17.60.155
  510 19.457413       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.63.49? Tell 172.17.56.1
  512 19.662472       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.206? Tell 172.17.56.1
  513 19.662547       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.227? Tell 172.17.56.1
  514 19.667747       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.57.214? Tell 172.17.56.1
  515 19.667776       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.58.163? Tell 172.17.56.1
  516 19.668018       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.94? Tell 172.17.56.1
  518 19.668165       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.109? Tell 172.17.56.1
  519 19.668277       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.63.9? Tell 172.17.56.1
  524 19.865456       IntelCor_70:43:1f   Broadcast    ARP        60 Who has 172.17.60.112? Tell 172.17.60.82
  529 20.070273       14:5a:fc:16:5b:7b   Broadcast    ARP        60 Who has 172.17.60.6? Tell 172.17.63.106
  530 20.070274       48:e7:da:f5:7f:6f   Broadcast    ARP        60 Who has 169.254.169.254? Tell 172.17.58.246
  531 20.070330       HewlettP_3a:cc:1d   Broadcast    ARP        60 Who has 172.17.59.84? Tell 172.17.56.1
```

```
> Frame 531: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 28 92  4a 3a cc 1d 08 06 00 01   ······(· J:······
0010  08 00 06 04 00 01 28 92  4a 3a cc 1d ac 11 38 01   ······(· J:····8·
0020  00 00 00 00 00 00 ac 11  3b 54 00 00 00 00 00 00   ········ ;T······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Address Resolution Protocol: Protocol | Packets: 35744 · Displayed: 13664 (38.2%) | Profile: Default

6. Exclude IP address


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

```
!ip.src==172.17.58.44
```

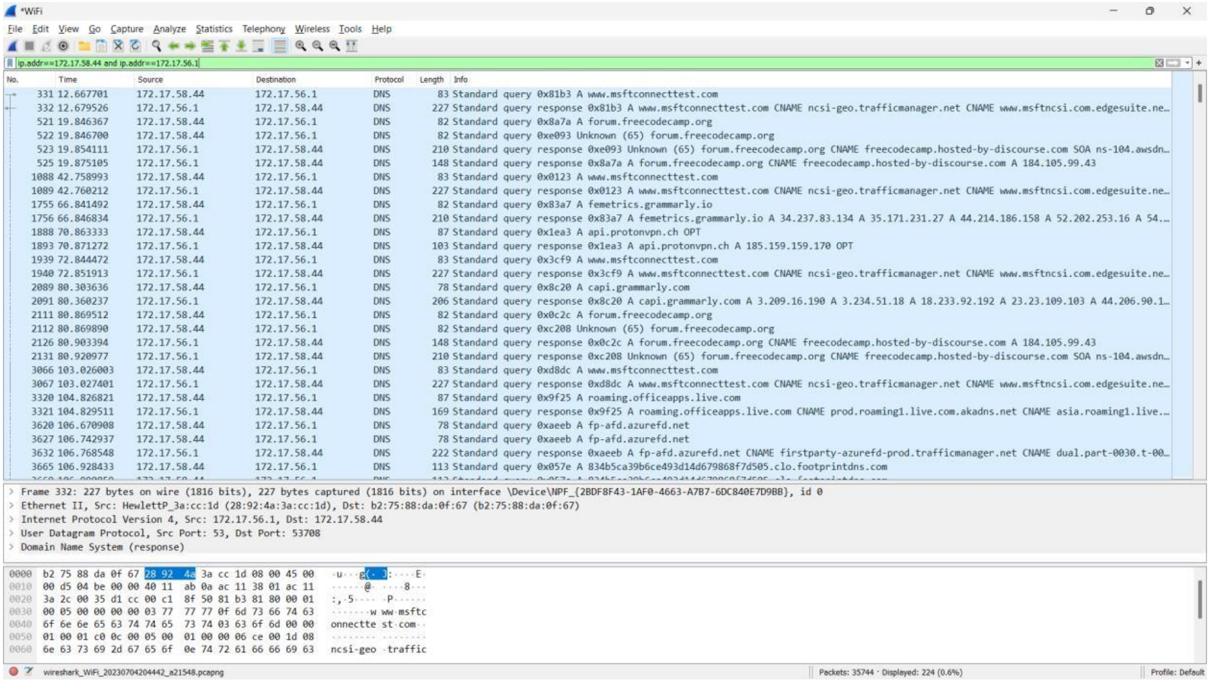
```
No.  Time        Source              Destination     Protocol Length Info
 302 11.468678   IntelCor_70:43:1f   Broadcast       ARP        60 Who has 172.17.60.112? Tell 172.17.60.82
 303 11.468837   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.63.61? Tell 172.17.56.1
 304 11.468879   86:45:49:a1:8a:b6   Broadcast       ARP        60 Who has 172.17.58.79? Tell 172.17.59.235
 305 11.469012   86:45:49:a1:8a:b6   Broadcast       ARP        60 Who has 172.17.56.172? Tell 172.17.59.235
 306 11.469152   20:1e:88:d5:27:5d   Broadcast       ARP        60 Who has 172.17.60.90? Tell 172.17.59.151
 307 11.575331   157.240.228.61      172.17.58.44    TCP        93 5222 → 55565 [PSH, ACK] Seq=1 Ack=1 Win=309 Len=39 [TCP segment of a reassembled PDU]
 309 11.591641   157.240.228.61      172.17.58.44    TCP        54 5222 → 55565 [ACK] Seq=40 Ack=28 Win=309 Len=0
 310 11.676076   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.59.206? Tell 172.17.56.1
 311 11.676360   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.59.65? Tell 172.17.56.1
 312 11.676487   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.63.9? Tell 172.17.56.1
 313 11.676588   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.59.109? Tell 172.17.56.1
 314 11.676853   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.58.208? Tell 172.17.56.1
 315 11.885981   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.58.64? Tell 172.17.56.1
 316 12.083783   14:5a:fc:16:5b:7b   Broadcast       ARP        60 Who has 172.17.60.6? Tell 172.17.63.106
 317 12.083949   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.59.84? Tell 172.17.56.1
 318 12.084156   172.17.58.131       172.17.63.255   DB-LSP…   173 Dropbox LAN sync Discovery Protocol
 319 12.084268   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.58.163? Tell 172.17.56.1
 320 12.084364   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.61.228? Tell 172.17.56.1
 321 12.084980   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.58.182? Tell 172.17.56.1
 322 12.288226   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.58.6? Tell 172.17.56.1
 323 12.288228   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.60.127? Tell 172.17.56.1
 324 12.288452   86:45:49:a1:8a:b6   Broadcast       ARP        60 Who has 172.17.58.79? Tell 172.17.59.235
 325 12.288496   86:45:49:a1:8a:b6   Broadcast       ARP        60 Who has 172.17.56.172? Tell 172.17.59.235
 326 12.493429   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.63.61? Tell 172.17.56.1
 327 12.493430   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.59.227? Tell 172.17.56.1
 328 12.493868   10:3d:1c:49:ed:b4   Broadcast       ARP        60 Who has 172.17.62.170? Tell 172.17.56.172
 329 12.493869   10:3d:1c:49:ed:b4   Broadcast       ARP        60 Who has 172.17.61.151? Tell 172.17.56.172
 330 12.493870   HewlettP_3a:cc:1d   Broadcast       ARP        60 Who has 172.17.59.206? Tell 172.17.56.1
```

```
> Frame 330: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 28 92  4a 3a cc 1d 08 06 00 01   ······(· J:······
0010  08 00 06 04 00 01 28 92  4a 3a cc 1d ac 11 38 01   ······(· J:····8·
0020  00 00 00 00 00 00 ac 11  3b ce 00 00 00 00 00 00   ········ ;·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

```
wireshark_WiFi_20230704204442_a21548.pcapng          Packets: 35744 · Displayed: 26059 (72.9%)          Profile: Default
```

7. Show traffic between two workstations or subnet


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

```
ip.addr==172.17.58.44 and ip.addr==172.17.56.1
```

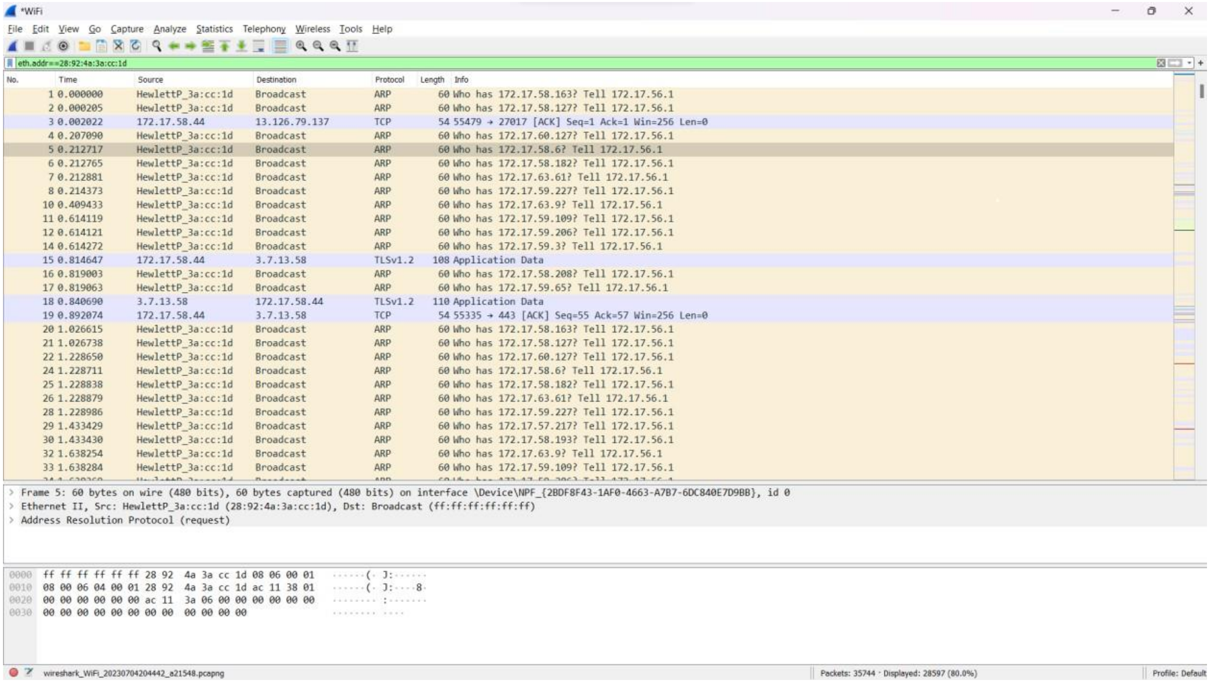
```
No.   Time         Source          Destination     Protocol Length Info
  331 12.667701    172.17.58.44    172.17.56.1     DNS        83 Standard query 0x81b3 A www.msftconnecttest.com
  332 12.679526    172.17.56.1     172.17.58.44    DNS       227 Standard query response 0x81b3 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
  521 19.846367    172.17.58.44    172.17.56.1     DNS        82 Standard query 0x8a7a A forum.freecodecamp.org
  522 19.846700    172.17.58.44    172.17.56.1     DNS        82 Standard query 0xe093 Unknown (65) forum.freecodecamp.org
  523 19.854111    172.17.56.1     172.17.58.44    DNS       210 Standard query response 0xe093 Unknown (65) forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com SOA ns-104.awsdn…
  525 19.875105    172.17.56.1     172.17.58.44    DNS       148 Standard query response 0x8a7a A forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com A 184.105.99.43
 1088 42.758993    172.17.58.44    172.17.56.1     DNS        83 Standard query 0x0123 A www.msftconnecttest.com
 1089 42.760212    172.17.56.1     172.17.58.44    DNS       227 Standard query response 0x0123 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
 1755 66.841492    172.17.58.44    172.17.56.1     DNS        82 Standard query 0x83a7 A femetrics.grammarly.io
 1756 66.846834    172.17.56.1     172.17.58.44    DNS       210 Standard query response 0x83a7 A femetrics.grammarly.io A 34.237.83.134 A 35.171.231.27 A 44.214.186.158 A 52.202.253.16 A 54.…
 1888 70.863333    172.17.58.44    172.17.56.1     DNS        87 Standard query 0x1ea3 A api.protonvpn.ch OPT
 1893 70.871272    172.17.56.1     172.17.58.44    DNS       103 Standard query response 0x1ea3 A api.protonvpn.ch A 185.159.159.170 OPT
 1939 72.844472    172.17.58.44    172.17.56.1     DNS        83 Standard query 0x3cf9 A www.msftconnecttest.com
 1940 72.851913    172.17.56.1     172.17.58.44    DNS       227 Standard query response 0x3cf9 A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
 2089 80.303636    172.17.58.44    172.17.56.1     DNS        78 Standard query 0x8c20 A capi.grammarly.com
 2091 80.360237    172.17.56.1     172.17.58.44    DNS       206 Standard query response 0x8c20 A capi.grammarly.com A 3.209.16.190 A 3.234.51.18 A 18.233.92.192 A 23.23.109.103 A 44.206.90.1…
 2111 80.869512    172.17.58.44    172.17.56.1     DNS        82 Standard query 0x0c2c A forum.freecodecamp.org
 2112 80.869890    172.17.58.44    172.17.56.1     DNS        82 Standard query 0xc208 Unknown (65) forum.freecodecamp.org
 2126 80.903394    172.17.56.1     172.17.58.44    DNS       148 Standard query response 0x0c2c A forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com A 184.105.99.43
 2131 80.920977    172.17.56.1     172.17.58.44    DNS       210 Standard query response 0xc208 Unknown (65) forum.freecodecamp.org CNAME freecodecamp.hosted-by-discourse.com SOA ns-104.awsdn…
 3066 103.026003   172.17.58.44    172.17.56.1     DNS        83 Standard query 0xd8dc A www.msftconnecttest.com
 3067 103.027401   172.17.56.1     172.17.58.44    DNS       227 Standard query response 0xd8dc A www.msftconnecttest.com CNAME ncsi-geo.trafficmanager.net CNAME www.msftncsi.com.edgesuite.ne…
 3320 104.826821   172.17.58.44    172.17.56.1     DNS        87 Standard query 0x9f25 A roaming.officeapps.live.com
 3321 104.829511   172.17.56.1     172.17.58.44    DNS       169 Standard query response 0x9f25 A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net CNAME asia.roaming1.live.…
 3620 106.670908   172.17.58.44    172.17.56.1     DNS        78 Standard query 0xaeeb A fp-afd.azurefd.net
 3627 106.742937   172.17.58.44    172.17.56.1     DNS        78 Standard query 0xaeeb A fp-afd.azurefd.net
 3632 106.768548   172.17.56.1     172.17.58.44    DNS       222 Standard query response 0xaeeb A fp-afd.azurefd.net CNAME firstparty-azurefd-prod.trafficmanager.net CNAME dual.part-0030.t-00…
 3665 106.928433   172.17.58.44    172.17.56.1     DNS       113 Standard query 0x057e A 834b5ca39b6ce493d14d679868f7d505.clo.footprintdns.com
```

```
> Frame 332: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d), Dst: b2:75:88:da:0f:67 (b2:75:88:da:0f:67)
> Internet Protocol Version 4, Src: 172.17.56.1, Dst: 172.17.58.44
> User Datagram Protocol, Src Port: 53, Dst Port: 53708
> Domain Name System (response)
```

```
0000  b2 75 88 da 0f 67 28 92  4a 3a cc 1d 08 00 45 00   ·u···g(· J:····E·
0010  00 d5 04 be 00 00 40 11  ab 0a ac 11 38 01 ac 11   ······@· ····8···
0020  3a 2c 00 35 d1 cc 00 c1  8f 50 81 b3 81 80 00 01   :,·5···· ·P······
0030  00 05 00 00 00 00 03 77  77 77 0f 6d 73 66 74 63   ·······w ww·msftc
0040  6f 6e 6e 65 63 74 74 65  73 74 03 63 6f 6d 00 00   onnectte st·com··
0050  01 00 01 c0 0c 00 05 00  01 00 00 06 ce 00 1d 08   ········ ········
0060  6e 63 73 69 2d 67 65 6f  0e 74 72 61 66 66 69 63   ncsi-geo ·traffic
```

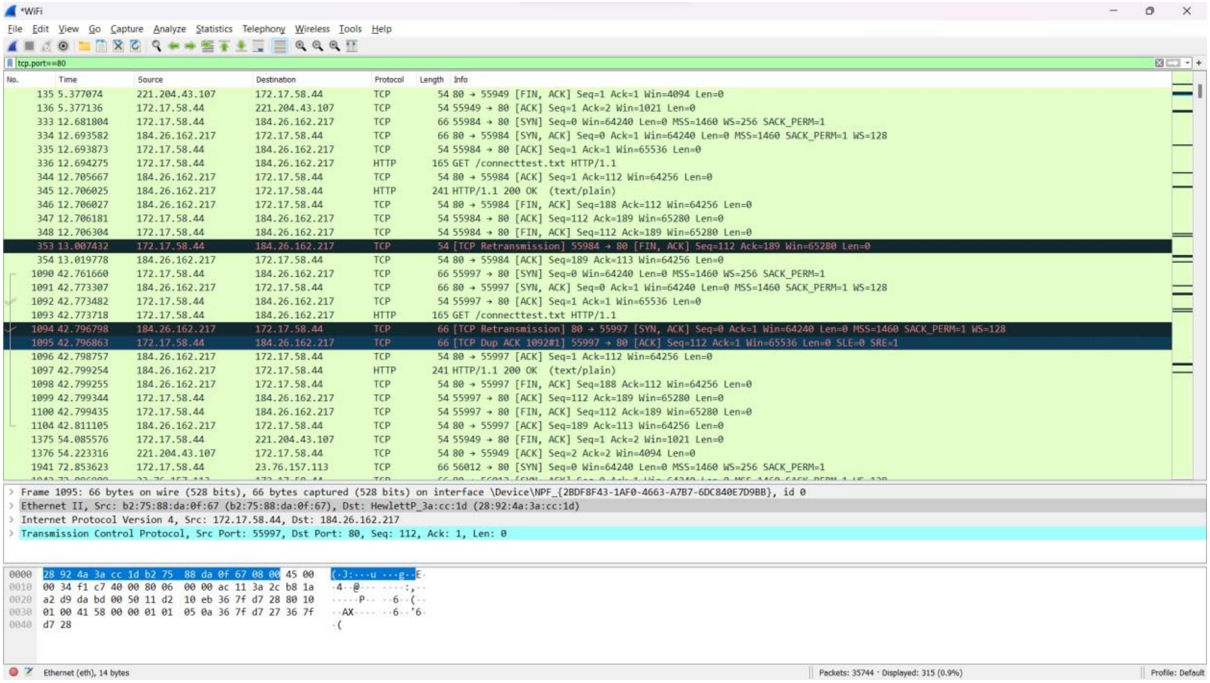
```
wireshark_WiFi_20230704204442_a21548.pcapng          Packets: 35744 · Displayed: 224 (0.6%)          Profile: Default
```

8. Filter MAC Address:


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

```
eth.addr==28:92:4a:3a:cc:1d

No.   Time      Source              Destination     Protocol  Length Info
    1 0.000000  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.163? Tell 172.17.56.1
    2 0.000205  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.127? Tell 172.17.56.1
    3 0.002022  172.17.58.44        13.126.79.137   TCP         54 55479 → 27017 [ACK] Seq=1 Ack=1 Win=256 Len=0
    4 0.207090  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.60.127? Tell 172.17.56.1
    5 0.212717  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.6? Tell 172.17.56.1
    6 0.212765  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.182? Tell 172.17.56.1
    7 0.212881  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.63.61? Tell 172.17.56.1
    8 0.214373  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.59.227? Tell 172.17.56.1
   10 0.409433  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.63.9? Tell 172.17.56.1
   11 0.614119  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.59.109? Tell 172.17.56.1
   12 0.614121  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.59.206? Tell 172.17.56.1
   14 0.614272  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.59.3? Tell 172.17.56.1
   15 0.814647  172.17.58.44        3.7.13.58       TLSv1.2    108 Application Data
   16 0.819003  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.208? Tell 172.17.56.1
   17 0.819063  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.59.65? Tell 172.17.56.1
   18 0.840690  3.7.13.58           172.17.58.44    TLSv1.2    110 Application Data
   19 0.892074  172.17.58.44        3.7.13.58       TCP         54 55335 → 443 [ACK] Seq=55 Ack=57 Win=256 Len=0
   20 1.026615  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.163? Tell 172.17.56.1
   21 1.026738  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.127? Tell 172.17.56.1
   22 1.228650  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.60.127? Tell 172.17.56.1
   24 1.228711  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.6? Tell 172.17.56.1
   25 1.228838  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.182? Tell 172.17.56.1
   26 1.228879  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.63.61? Tell 172.17.56.1
   28 1.228986  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.59.227? Tell 172.17.56.1
   29 1.433429  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.57.217? Tell 172.17.56.1
   30 1.433430  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.58.193? Tell 172.17.56.1
   32 1.638254  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.63.9? Tell 172.17.56.1
   33 1.638284  HewlettP_3a:cc:1d   Broadcast       ARP         60 Who has 172.17.59.109? Tell 172.17.56.1

> Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 28 92  4a 3a cc 1d 08 06 00 01   ······(· J:······
0010  08 00 06 04 00 01 28 92  4a 3a cc 1d ac 11 38 01   ······(· J:····8·
0020  00 00 00 00 00 00 ac 11  3a 06 00 00 00 00 00 00   ········ :·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····

wireshark_WiFi_20230704204442_a21548.pcapng    Packets: 35744 · Displayed: 28597 (80.0%)    Profile: Default
```

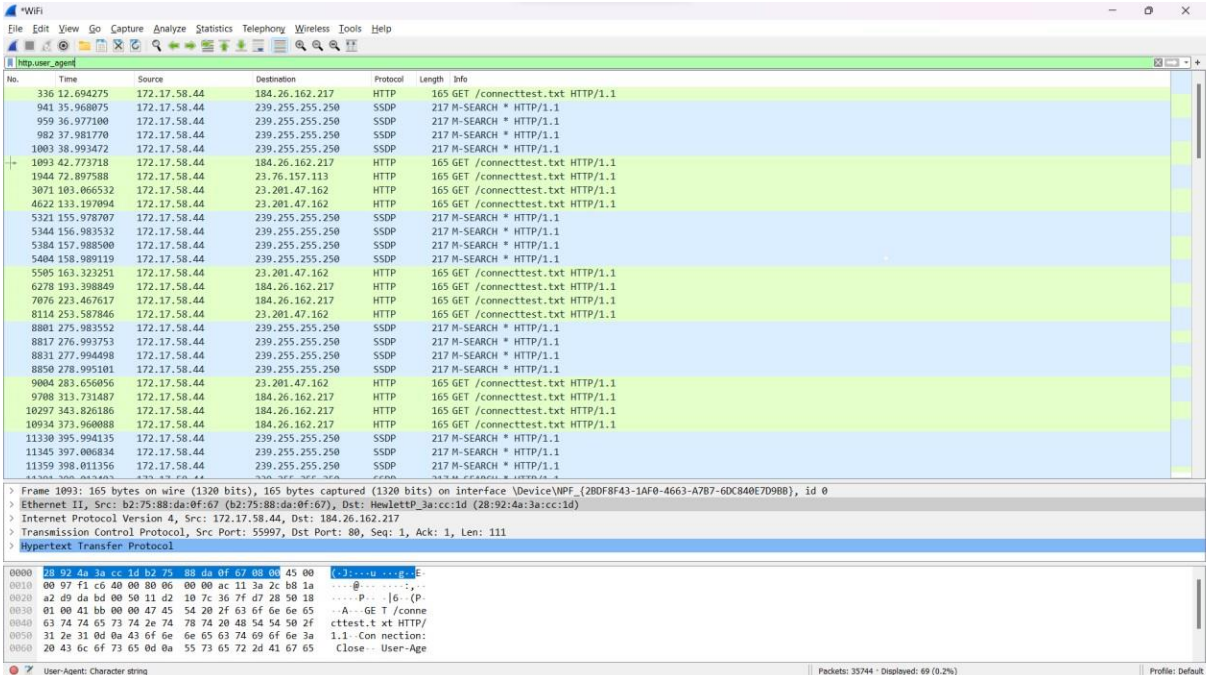
9. Filter on TCP Port:


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

```
tcp.port==80

No.   Time       Source           Destination      Protocol  Length Info
  135 5.377074   221.204.43.107   172.17.58.44     TCP         54 80 → 55949 [FIN, ACK] Seq=1 Ack=1 Win=4094 Len=0
  136 5.377136   172.17.58.44     221.204.43.107   TCP         54 55949 → 80 [ACK] Seq=1 Ack=2 Win=1021 Len=0
  333 12.681804  172.17.58.44     184.26.162.217   TCP         66 55984 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  334 12.693582  184.26.162.217   172.17.58.44     TCP         66 80 → 55984 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
  335 12.693873  172.17.58.44     184.26.162.217   TCP         54 55984 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  336 12.694275  172.17.58.44     184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
  344 12.705667  184.26.162.217   172.17.58.44     TCP         54 80 → 55984 [ACK] Seq=1 Ack=112 Win=64256 Len=0
  345 12.706025  184.26.162.217   172.17.58.44     HTTP       241 HTTP/1.1 200 OK  (text/plain)
  346 12.706027  184.26.162.217   172.17.58.44     TCP         54 80 → 55984 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
  347 12.706181  172.17.58.44     184.26.162.217   TCP         54 55984 → 80 [ACK] Seq=112 Ack=189 Win=65280 Len=0
  348 12.706304  172.17.58.44     184.26.162.217   TCP         54 55984 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
  353 13.007432  172.17.58.44     184.26.162.217   TCP         54 [TCP Retransmission] 55984 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
  354 13.019778  184.26.162.217   172.17.58.44     TCP         54 80 → 55984 [ACK] Seq=189 Ack=113 Win=64256 Len=0
 1090 42.761660  172.17.58.44     184.26.162.217   TCP         66 55997 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1091 42.773307  184.26.162.217   172.17.58.44     TCP         66 80 → 55997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1092 42.773482  172.17.58.44     184.26.162.217   TCP         54 55997 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 1093 42.773718  172.17.58.44     184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
 1094 42.796798  184.26.162.217   172.17.58.44     TCP         66 [TCP Retransmission] 80 → 55997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1095 42.796863  172.17.58.44     184.26.162.217   TCP         66 [TCP Dup ACK 1092#1] 55997 → 80 [ACK] Seq=112 Ack=1 Win=65536 Len=0 SLE=0 SRE=1
 1096 42.798757  184.26.162.217   172.17.58.44     TCP         54 80 → 55997 [ACK] Seq=1 Ack=112 Win=64256 Len=0
 1097 42.799254  184.26.162.217   172.17.58.44     HTTP       241 HTTP/1.1 200 OK  (text/plain)
 1098 42.799255  184.26.162.217   172.17.58.44     TCP         54 80 → 55997 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
 1099 42.799344  172.17.58.44     184.26.162.217   TCP         54 55997 → 80 [ACK] Seq=112 Ack=189 Win=65280 Len=0
 1100 42.799435  172.17.58.44     184.26.162.217   TCP         54 55997 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
 1104 42.811105  184.26.162.217   172.17.58.44     TCP         54 80 → 55997 [ACK] Seq=189 Ack=113 Win=64256 Len=0
 1375 54.085576  172.17.58.44     221.204.43.107   TCP         54 55949 → 80 [FIN, ACK] Seq=1 Ack=2 Win=1021 Len=0
 1376 54.223316  221.204.43.107   172.17.58.44     TCP         54 80 → 55949 [ACK] Seq=2 Ack=2 Win=4094 Len=0
 1941 72.853623  172.17.58.44     23.76.157.113    TCP         66 56012 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 1095: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 184.26.162.217
> Transmission Control Protocol, Src Port: 55997, Dst Port: 80, Seq: 112, Ack: 1, Len: 0

0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 34 f1 c7 40 00 80 06  00 00 ac 11 3a 2c b8 1a   ·4··@··· ····:,··
0020  a2 d9 da bd 00 50 11 d2  10 eb 36 7f d7 28 80 10   ·····P·· ··6··(··
0030  01 00 41 58 00 00 01 01  05 0a 36 7f d7 27 36 7f   ··AX···· ··6··'6·
0040  d7 28                                              ·(

Ethernet (eth), 14 bytes    Packets: 35744 · Displayed: 315 (0.9%)    Profile: Default
```

a

10. Find user name:


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

http.user_agent

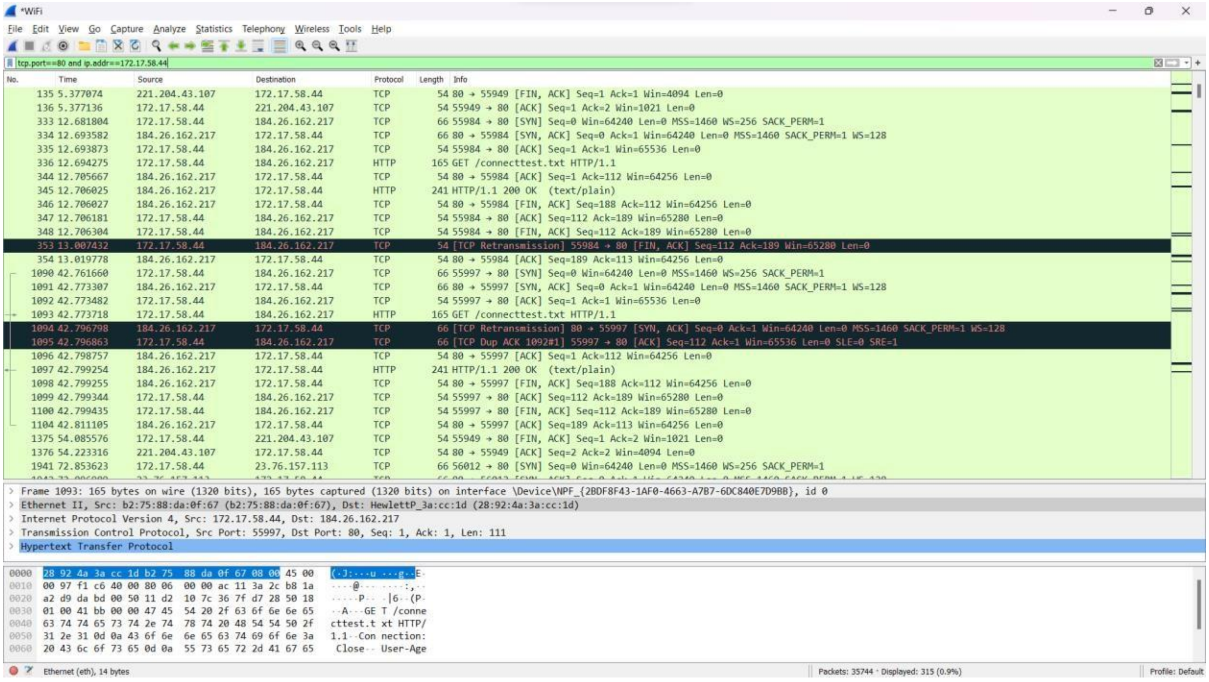
```
No.   Time          Source         Destination       Protocol  Length Info
  336 12.694275     172.17.58.44   184.26.162.217    HTTP       165 GET /connecttest.txt HTTP/1.1
  941 35.968075     172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
  959 36.977100     172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
  982 37.981770     172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 1003 38.993472     172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 1093 42.773718     172.17.58.44   184.26.162.217    HTTP       165 GET /connecttest.txt HTTP/1.1
 1944 72.897588     172.17.58.44   23.76.157.113     HTTP       165 GET /connecttest.txt HTTP/1.1
 3071 103.066532    172.17.58.44   23.201.47.162     HTTP       165 GET /connecttest.txt HTTP/1.1
 4622 133.197094    172.17.58.44   23.201.47.162     HTTP       165 GET /connecttest.txt HTTP/1.1
 5321 155.978707    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 5344 156.983532    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 5384 157.988500    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 5404 158.989119    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 5505 163.323251    172.17.58.44   23.201.47.162     HTTP       165 GET /connecttest.txt HTTP/1.1
 6278 193.398849    172.17.58.44   184.26.162.217    HTTP       165 GET /connecttest.txt HTTP/1.1
 7076 223.467617    172.17.58.44   184.26.162.217    HTTP       165 GET /connecttest.txt HTTP/1.1
 8114 253.587846    172.17.58.44   23.201.47.162     HTTP       165 GET /connecttest.txt HTTP/1.1
 8801 275.983552    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 8817 276.993753    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 8831 277.994498    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 8850 278.995101    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
 9004 283.656056    172.17.58.44   23.201.47.162     HTTP       165 GET /connecttest.txt HTTP/1.1
 9708 313.731487    172.17.58.44   184.26.162.217    HTTP       165 GET /connecttest.txt HTTP/1.1
10297 343.826186    172.17.58.44   184.26.162.217    HTTP       165 GET /connecttest.txt HTTP/1.1
10934 373.960088    172.17.58.44   184.26.162.217    HTTP       165 GET /connecttest.txt HTTP/1.1
11330 395.994135    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
11345 397.006834    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
11359 398.011356    172.17.58.44   239.255.255.250   SSDP       217 M-SEARCH * HTTP/1.1
```

```
> Frame 1093: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 184.26.162.217
> Transmission Control Protocol, Src Port: 55997, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
> Hypertext Transfer Protocol
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 97 f1 c6 40 00 80 06  00 00 ac 11 3a 2c b8 1a   ····@··· ····:,··
0020  a2 d9 da bd 00 50 11 d2  10 7c 36 7f d7 28 50 18   ·····P·· ·|6··(P·
0030  01 00 41 bb 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ··A···GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   1.1··Con nection:
0060  20 43 6c 6f 73 65 0d 0a  55 73 65 72 2d 41 67 65    Close·· User-Age
```

User-Agent: Character string | Packets: 35744 · Displayed: 69 (0.2%) | Profile: Default

11. Filter on Port and IP Address:


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

tcp.port==80 and ip.addr==172.17.58.44

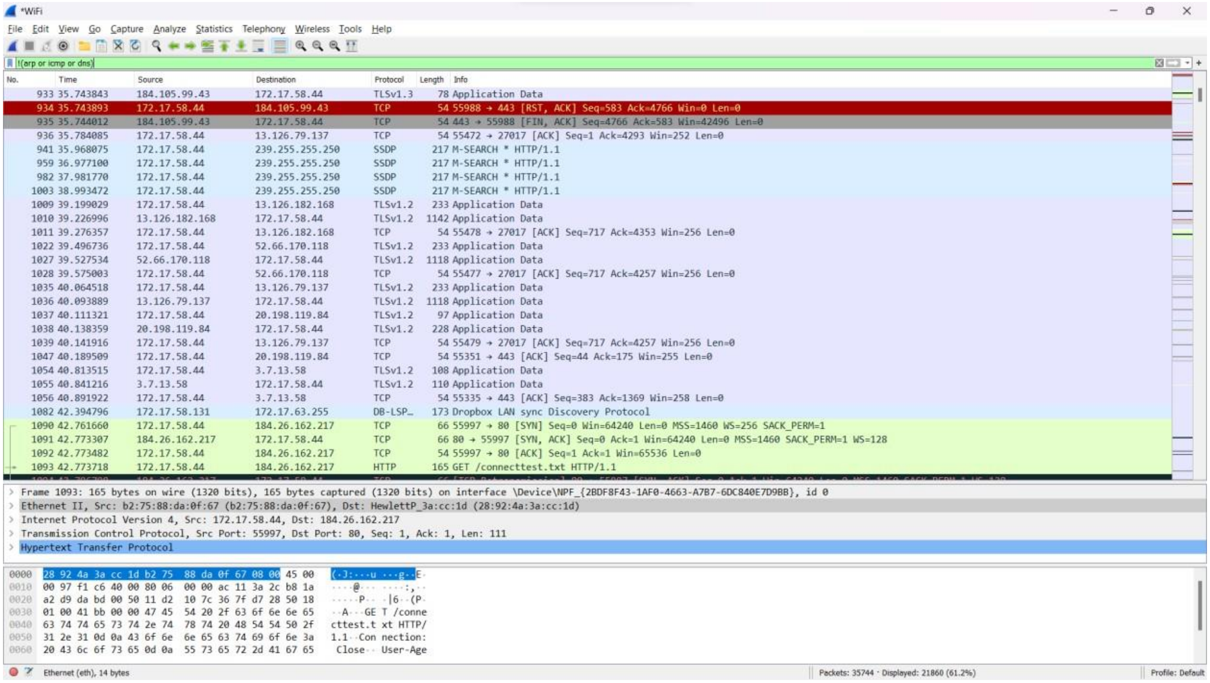
```
No.   Time          Source           Destination      Protocol  Length Info
  135 5.377074      221.204.43.107   172.17.58.44     TCP         54 80 → 55949 [FIN, ACK] Seq=1 Ack=1 Win=4094 Len=0
  136 5.377136      172.17.58.44     221.204.43.107   TCP         54 55949 → 80 [ACK] Seq=1 Ack=2 Win=1021 Len=0
  333 12.681804     172.17.58.44     184.26.162.217   TCP         66 55984 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  334 12.693582     184.26.162.217   172.17.58.44     TCP         66 80 → 55984 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
  335 12.693873     172.17.58.44     184.26.162.217   TCP         54 55984 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  336 12.694275     172.17.58.44     184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
  344 12.705667     184.26.162.217   172.17.58.44     TCP         54 80 → 55984 [ACK] Seq=1 Ack=112 Win=64256 Len=0
  345 12.706025     184.26.162.217   172.17.58.44     HTTP       241 HTTP/1.1 200 OK  (text/plain)
  346 12.706027     184.26.162.217   172.17.58.44     TCP         54 80 → 55984 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
  347 12.706181     172.17.58.44     184.26.162.217   TCP         54 55984 → 80 [ACK] Seq=112 Ack=189 Win=65280 Len=0
  348 12.706304     172.17.58.44     184.26.162.217   TCP         54 55984 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
  353 13.007432     172.17.58.44     184.26.162.217   TCP         54 [TCP Retransmission] 55984 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
  354 13.019778     184.26.162.217   172.17.58.44     TCP         54 80 → 55984 [ACK] Seq=189 Ack=113 Win=64256 Len=0
 1090 42.761660     172.17.58.44     184.26.162.217   TCP         66 55997 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1091 42.773307     184.26.162.217   172.17.58.44     TCP         66 80 → 55997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1092 42.773482     172.17.58.44     184.26.162.217   TCP         54 55997 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 1093 42.773718     172.17.58.44     184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
 1094 42.796798     184.26.162.217   172.17.58.44     TCP         66 [TCP Retransmission] 80 → 55997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1095 42.796863     172.17.58.44     184.26.162.217   TCP         66 [TCP Dup ACK 1092#1] 55997 → 80 [ACK] Seq=112 Ack=1 Win=65536 Len=0 SLE=0 SRE=1
 1096 42.798757     184.26.162.217   172.17.58.44     TCP         54 80 → 55997 [ACK] Seq=1 Ack=112 Win=64256 Len=0
 1097 42.799254     184.26.162.217   172.17.58.44     HTTP       241 HTTP/1.1 200 OK  (text/plain)
 1098 42.799255     184.26.162.217   172.17.58.44     TCP         54 80 → 55997 [FIN, ACK] Seq=188 Ack=112 Win=64256 Len=0
 1099 42.799344     172.17.58.44     184.26.162.217   TCP         54 55997 → 80 [ACK] Seq=112 Ack=189 Win=65280 Len=0
 1100 42.799435     172.17.58.44     184.26.162.217   TCP         54 55997 → 80 [FIN, ACK] Seq=112 Ack=189 Win=65280 Len=0
 1104 42.811105     184.26.162.217   172.17.58.44     TCP         54 80 → 55997 [ACK] Seq=189 Ack=113 Win=64256 Len=0
 1375 54.085576     172.17.58.44     221.204.43.107   TCP         54 55949 → 80 [FIN, ACK] Seq=1 Ack=2 Win=1021 Len=0
 1376 54.223316     221.204.43.107   172.17.58.44     TCP         54 80 → 55949 [ACK] Seq=2 Ack=2 Win=4094 Len=0
 1941 72.853623     172.17.58.44     23.76.157.113    TCP         66 56012 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
> Frame 1093: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 184.26.162.217
> Transmission Control Protocol, Src Port: 55997, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
> Hypertext Transfer Protocol
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 97 f1 c6 40 00 80 06  00 00 ac 11 3a 2c b8 1a   ····@··· ····:,··
0020  a2 d9 da bd 00 50 11 d2  10 7c 36 7f d7 28 50 18   ·····P·· ·|6··(P·
0030  01 00 41 bb 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ··A···GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   1.1··Con nection:
0060  20 43 6c 6f 73 65 0d 0a  55 73 65 72 2d 41 67 65    Close·· User-Age
```

Ethernet (eth), 14 bytes | Packets: 35744 · Displayed: 315 (0.9%) | Profile: Default

12. Filter background network noise:


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

!(arp or icmp or dns)

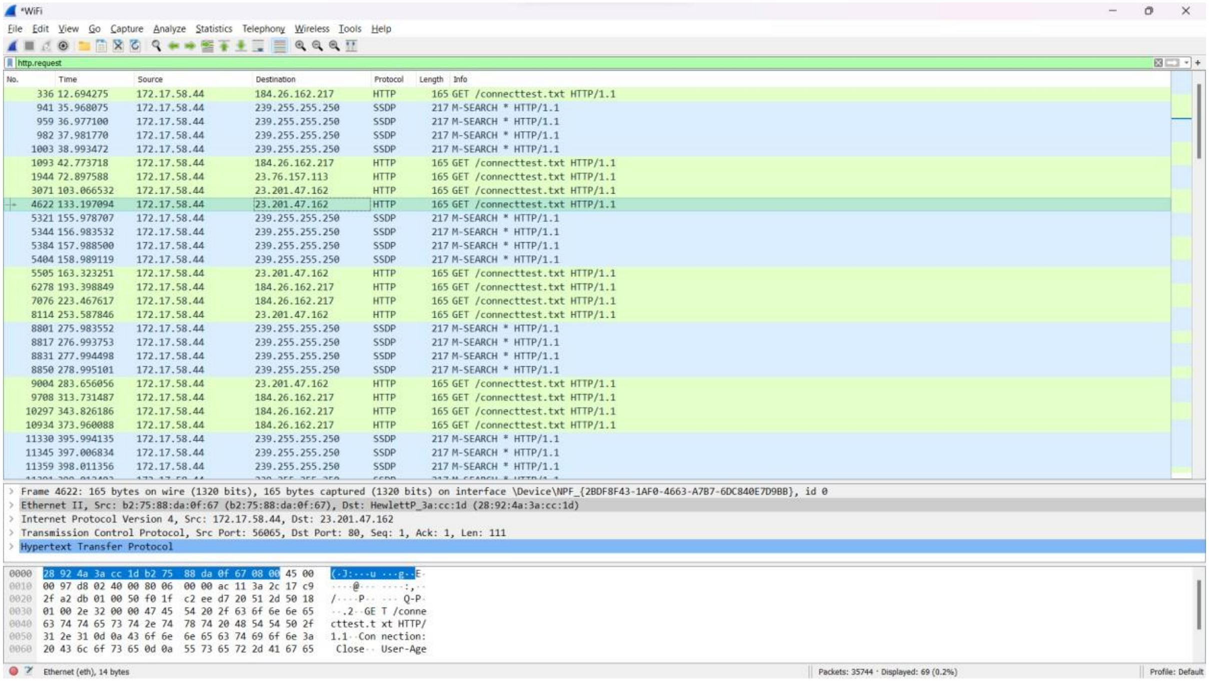
```
No.    Time       Source           Destination      Protocol  Length Info
   933 35.743843  184.105.99.43    172.17.58.44     TLSv1.3     78 Application Data
   934 35.743893  172.17.58.44     184.105.99.43    TCP         54 55988 → 443 [RST, ACK] Seq=583 Ack=4766 Win=0 Len=0
   935 35.744012  184.105.99.43    172.17.58.44     TCP         54 443 → 55988 [FIN, ACK] Seq=4766 Ack=583 Win=42496 Len=0
   936 35.784085  172.17.58.44     13.126.79.137    TCP         54 55472 → 27017 [ACK] Seq=1 Ack=4293 Win=252 Len=0
   941 35.968075  172.17.58.44     239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
   959 36.977100  172.17.58.44     239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
   982 37.981770  172.17.58.44     239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  1003 38.993472  172.17.58.44     239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  1009 39.199029  172.17.58.44     13.126.182.168   TLSv1.2    233 Application Data
  1010 39.226996  13.126.182.168   172.17.58.44     TLSv1.2   1142 Application Data
  1011 39.276357  172.17.58.44     13.126.182.168   TCP         54 55478 → 27017 [ACK] Seq=717 Ack=4353 Win=256 Len=0
  1022 39.496736  172.17.58.44     52.66.170.118    TLSv1.2    233 Application Data
  1027 39.527534  52.66.170.118    172.17.58.44     TLSv1.2   1118 Application Data
  1028 39.575003  172.17.58.44     52.66.170.118    TCP         54 55477 → 27017 [ACK] Seq=717 Ack=4257 Win=256 Len=0
  1035 40.064518  172.17.58.44     13.126.79.137    TLSv1.2    233 Application Data
  1036 40.093889  13.126.79.137    172.17.58.44     TLSv1.2   1118 Application Data
  1037 40.111321  172.17.58.44     20.198.119.84    TLSv1.2     97 Application Data
  1038 40.138359  20.198.119.84    172.17.58.44     TLSv1.2    228 Application Data
  1039 40.141916  172.17.58.44     13.126.79.137    TCP         54 55479 → 27017 [ACK] Seq=717 Ack=4257 Win=256 Len=0
  1047 40.189509  172.17.58.44     20.198.119.84    TCP         54 55351 → 443 [ACK] Seq=44 Ack=175 Win=255 Len=0
  1054 40.813515  172.17.58.44     3.7.13.58        TLSv1.2    108 Application Data
  1055 40.841216  3.7.13.58        172.17.58.44     TLSv1.2    110 Application Data
  1056 40.891922  172.17.58.44     3.7.13.58        TCP         54 55335 → 443 [ACK] Seq=383 Ack=1369 Win=258 Len=0
  1082 42.394796  172.17.58.131    172.17.63.255    DB-LSP…    173 Dropbox LAN sync Discovery Protocol
  1090 42.761660  172.17.58.44     184.26.162.217   TCP         66 55997 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  1091 42.773307  184.26.162.217   172.17.58.44     TCP         66 80 → 55997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
  1092 42.773482  172.17.58.44     184.26.162.217   TCP         54 55997 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  1093 42.773718  172.17.58.44     184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
```

```
> Frame 1093: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 184.26.162.217
> Transmission Control Protocol, Src Port: 55997, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
> Hypertext Transfer Protocol
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 97 f1 c6 40 00 80 06  00 00 ac 11 3a 2c b8 1a   ····@··· ····:,··
0020  a2 d9 da bd 00 50 11 d2  10 7c 36 7f d7 28 50 18   ·····P·· ·|6··(P·
0030  01 00 41 bb 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ··A···GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   1.1··Con nection:
0060  20 43 6c 6f 73 65 0d 0a  55 73 65 72 2d 41 67 65    Close·· User-Age
```

Ethernet (eth), 14 bytes | Packets: 35744 · Displayed: 21860 (61.2%) | Profile: Default

13. Filter for all http get requests:


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

http.request

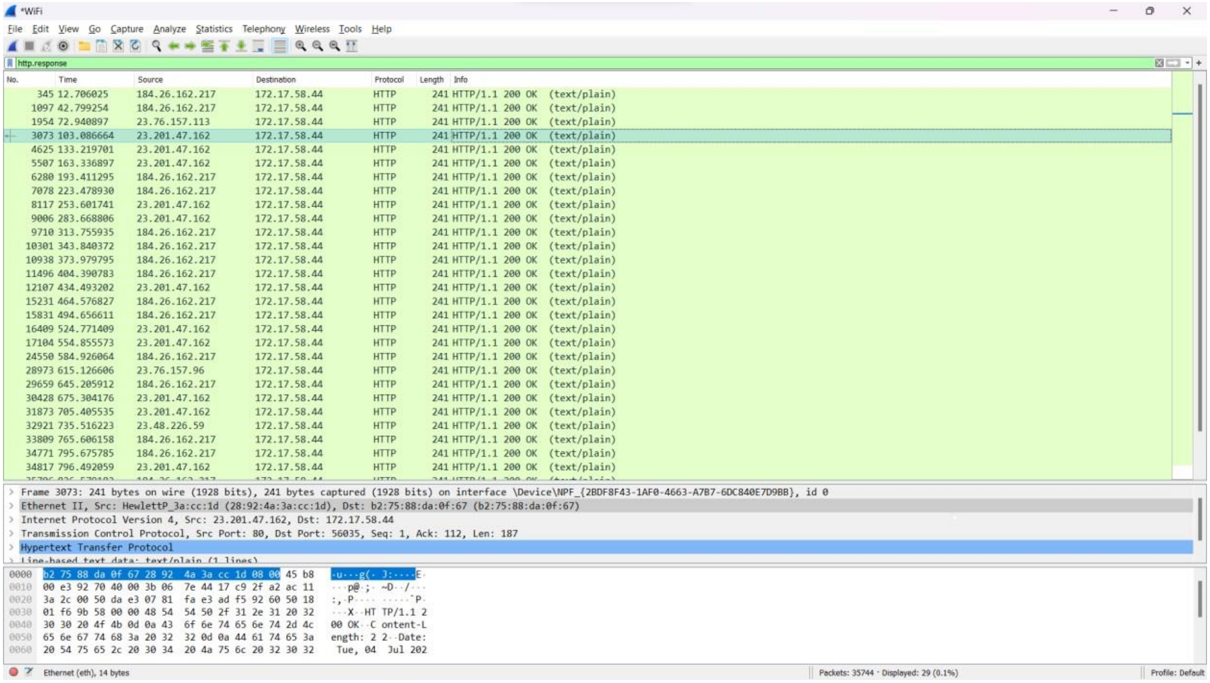
```
No.    Time        Source          Destination      Protocol  Length Info
   336 12.694275   172.17.58.44    184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
   941 35.968075   172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
   959 36.977100   172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
   982 37.981770   172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  1003 38.993472   172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  1093 42.773718   172.17.58.44    184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
  1944 72.897588   172.17.58.44    23.76.157.113    HTTP       165 GET /connecttest.txt HTTP/1.1
  3071 103.066532  172.17.58.44    23.201.47.162    HTTP       165 GET /connecttest.txt HTTP/1.1
  4622 133.197094  172.17.58.44    23.201.47.162    HTTP       165 GET /connecttest.txt HTTP/1.1
  5321 155.978707  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  5344 156.983532  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  5384 157.988500  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  5404 158.989119  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  5505 163.323251  172.17.58.44    23.201.47.162    HTTP       165 GET /connecttest.txt HTTP/1.1
  6278 193.398849  172.17.58.44    184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
  7076 223.467617  172.17.58.44    184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
  8114 253.587846  172.17.58.44    23.201.47.162    HTTP       165 GET /connecttest.txt HTTP/1.1
  8801 275.983552  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  8817 276.993753  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  8831 277.994498  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  8850 278.995101  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
  9004 283.656056  172.17.58.44    23.201.47.162    HTTP       165 GET /connecttest.txt HTTP/1.1
  9708 313.731487  172.17.58.44    184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
 10297 343.826186  172.17.58.44    184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
 10934 373.960088  172.17.58.44    184.26.162.217   HTTP       165 GET /connecttest.txt HTTP/1.1
 11330 395.994135  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
 11345 397.006834  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
 11359 398.011356  172.17.58.44    239.255.255.250  SSDP       217 M-SEARCH * HTTP/1.1
```

```
> Frame 4622: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 23.201.47.162
> Transmission Control Protocol, Src Port: 56065, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
> Hypertext Transfer Protocol
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 97 d8 02 40 00 80 06  00 00 ac 11 3a 2c 17 c9   ····@··· ····:,··
0020  2f a2 db 01 00 50 f0 1f  c2 ee d7 20 51 2d 50 18   /····P·· ··· Q-P·
0030  01 00 2e 32 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ··.2··GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   1.1··Con nection:
0060  20 43 6c 6f 73 65 0d 0a  55 73 65 72 2d 41 67 65    Close·· User-Age
```

Ethernet (eth), 14 bytes | Packets: 35744 · Displayed: 69 (0.2%) | Profile: Default

14. Filter for all HTTP Responses:


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

http.response

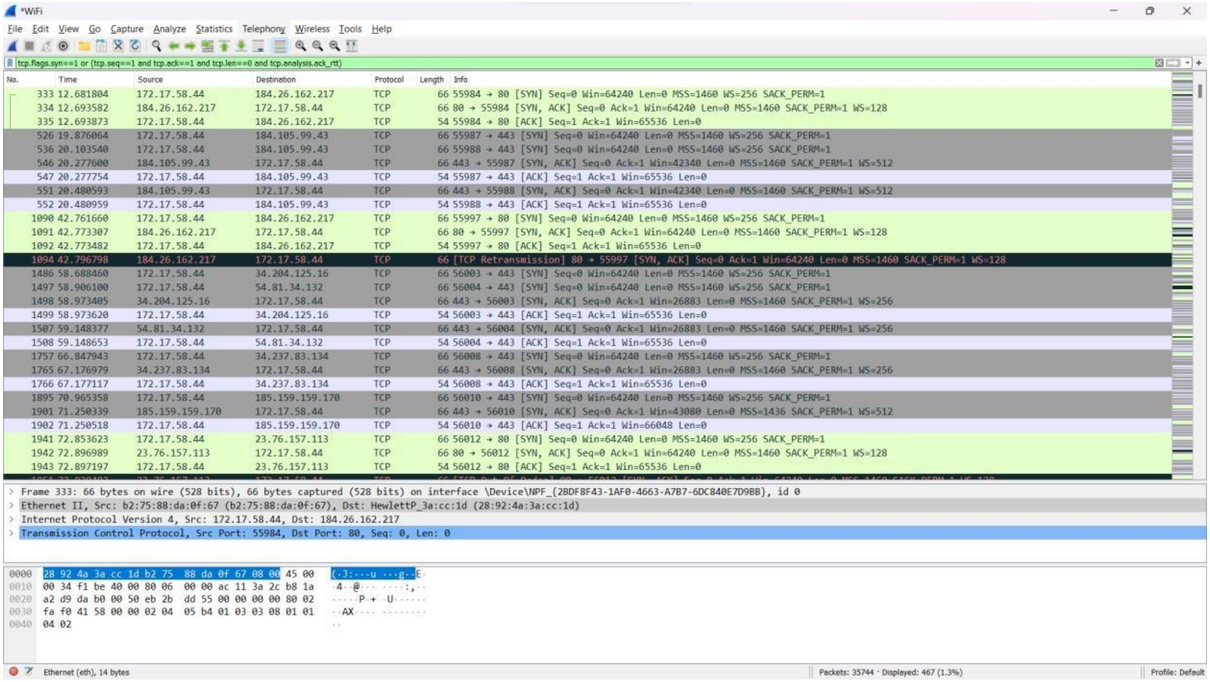
```
No.     Time        Source           Destination     Protocol  Length  Info
  345 12.706025     184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 1097 42.799254     184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 1954 72.940897     23.76.157.113    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 3073 103.086664    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 4625 133.219701    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 5507 163.336897    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 6280 193.411295    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 7078 223.478930    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 8117 253.601741    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 9006 283.668806    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
 9710 313.755935    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
10301 343.840372    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
10938 373.979795    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
11496 404.390783    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
12107 434.493202    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
15231 464.576827    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
15831 494.656611    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
16409 524.771409    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
17104 554.855573    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
24550 584.926064    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
28973 615.126606    23.76.157.96     172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
29659 645.205912    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
30428 675.304176    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
31873 705.405535    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
32921 735.516223    23.48.226.59     172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
33809 765.606158    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
34771 795.675785    184.26.162.217   172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
34817 796.492059    23.201.47.162    172.17.58.44    HTTP      241 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 3073: 241 bytes on wire (1928 bits), 241 bytes captured (1928 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d), Dst: b2:75:88:da:0f:67 (b2:75:88:da:0f:67)
> Internet Protocol Version 4, Src: 23.201.47.162, Dst: 172.17.58.44
> Transmission Control Protocol, Src Port: 80, Dst Port: 56035, Seq: 1, Ack: 112, Len: 187
> Hypertext Transfer Protocol
> Line-based text data: text/plain (1 lines)
```

```
0000  b2 75 88 da 0f 67 28 92  4a 3a cc 1d 08 00 45 b8   ·u···g(· J:····E·
0010  00 e3 92 70 40 00 3b 06  7e 44 17 c9 2f a2 ac 11   ···p@·;· ~D··/···
0020  3a 2c 00 50 da e3 07 81  fa e3 ad f5 92 60 50 18   :,·P···· ·····`P·
0030  01 f6 9b 58 00 00 48 54  54 50 2f 31 2e 31 20 32   ···X··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 4c   00 OK··C ontent-L
0050  65 6e 67 74 68 3a 20 32  32 0d 0a 44 61 74 65 3a   ength: 2 2··Date:
0060  20 54 75 65 2c 20 30 34  20 4a 75 6c 20 32 30 32    Tue, 04  Jul 202
```

Ethernet (eth), 14 bytes | Packets: 35744 · Displayed: 29 (0.1%) | Profile: Default

15. Filter on three-way handshake:


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

tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0 and tcp.analysis.ack_rtt)

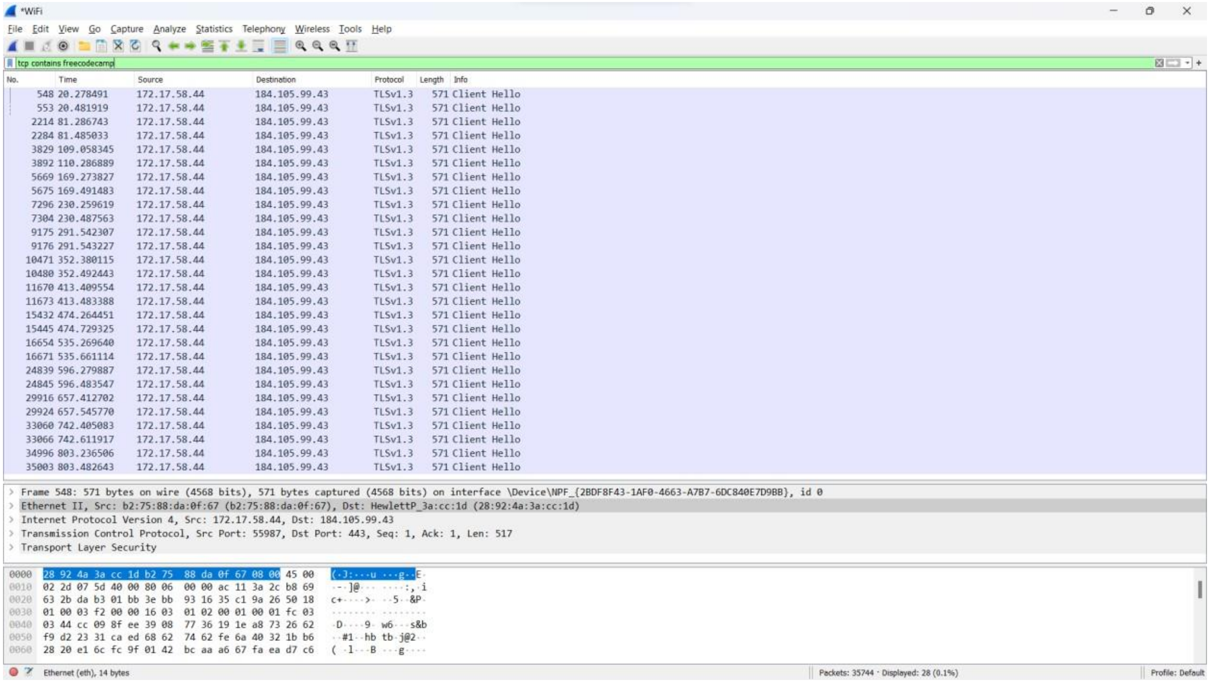
```
No.     Time        Source           Destination      Protocol  Length  Info
  333 12.681804     172.17.58.44     184.26.162.217   TCP       66 55984 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  334 12.693582     184.26.162.217   172.17.58.44     TCP       66 80 → 55984 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
  335 12.693873     172.17.58.44     184.26.162.217   TCP       54 55984 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  526 19.876064     172.17.58.44     184.105.99.43    TCP       66 55987 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  536 20.103540     172.17.58.44     184.105.99.43    TCP       66 55988 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  546 20.277600     184.105.99.43    172.17.58.44     TCP       66 443 → 55987 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM=1 WS=512
  547 20.277754     172.17.58.44     184.105.99.43    TCP       54 55987 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  551 20.480593     184.105.99.43    172.17.58.44     TCP       66 443 → 55988 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1460 SACK_PERM=1 WS=512
  552 20.480959     172.17.58.44     184.105.99.43    TCP       54 55988 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 1090 42.761660     172.17.58.44     184.26.162.217   TCP       66 55997 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1091 42.773307     184.26.162.217   172.17.58.44     TCP       66 80 → 55997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1092 42.773482     172.17.58.44     184.26.162.217   TCP       54 55997 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 1094 42.796798     184.26.162.217   172.17.58.44     TCP       66 [TCP Retransmission] 80 → 55997 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1486 58.688460     172.17.58.44     34.204.125.16    TCP       66 56003 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1497 58.906100     172.17.58.44     54.81.34.132     TCP       66 56004 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1498 58.973405     34.204.125.16    172.17.58.44     TCP       66 443 → 56003 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=256
 1499 58.973620     172.17.58.44     34.204.125.16    TCP       54 56003 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 1507 59.148377     54.81.34.132     172.17.58.44     TCP       66 443 → 56004 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=256
 1508 59.148653     172.17.58.44     54.81.34.132     TCP       54 56004 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 1757 66.847943     172.17.58.44     34.237.83.134    TCP       66 56008 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1765 67.176979     34.237.83.134    172.17.58.44     TCP       66 443 → 56008 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=1 WS=256
 1766 67.177117     172.17.58.44     34.237.83.134    TCP       54 56008 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
 1895 70.965358     172.17.58.44     185.159.159.170  TCP       66 56010 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1901 71.250339     185.159.159.170  172.17.58.44     TCP       66 443 → 56010 [SYN, ACK] Seq=0 Ack=1 Win=43080 Len=0 MSS=1436 SACK_PERM=1 WS=512
 1902 71.250518     172.17.58.44     185.159.159.170  TCP       54 56010 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
 1941 72.853623     172.17.58.44     23.76.157.113    TCP       66 56012 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1942 72.896989     23.76.157.113    172.17.58.44     TCP       66 80 → 56012 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 WS=128
 1943 72.897197     172.17.58.44     23.76.157.113    TCP       54 56012 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
```

```
> Frame 333: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 184.26.162.217
> Transmission Control Protocol, Src Port: 55984, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 34 f1 be 40 00 80 06  00 00 ac 11 3a 2c b8 1a   ·4··@··· ····:,··
0020  a2 d9 da b0 00 50 eb 2b  dd 55 00 00 00 00 80 02   ·····P·+ ·U······
0030  fa f0 41 58 00 00 02 04  05 b4 01 03 03 08 01 01   ··AX···· ········
0040  04 02                                              ··
```

Ethernet (eth), 14 bytes | Packets: 35744 · Displayed: 467 (1.3%) | Profile: Default

16. Search traffic based on a keyword


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

```
tcp contains freecodecamp
```

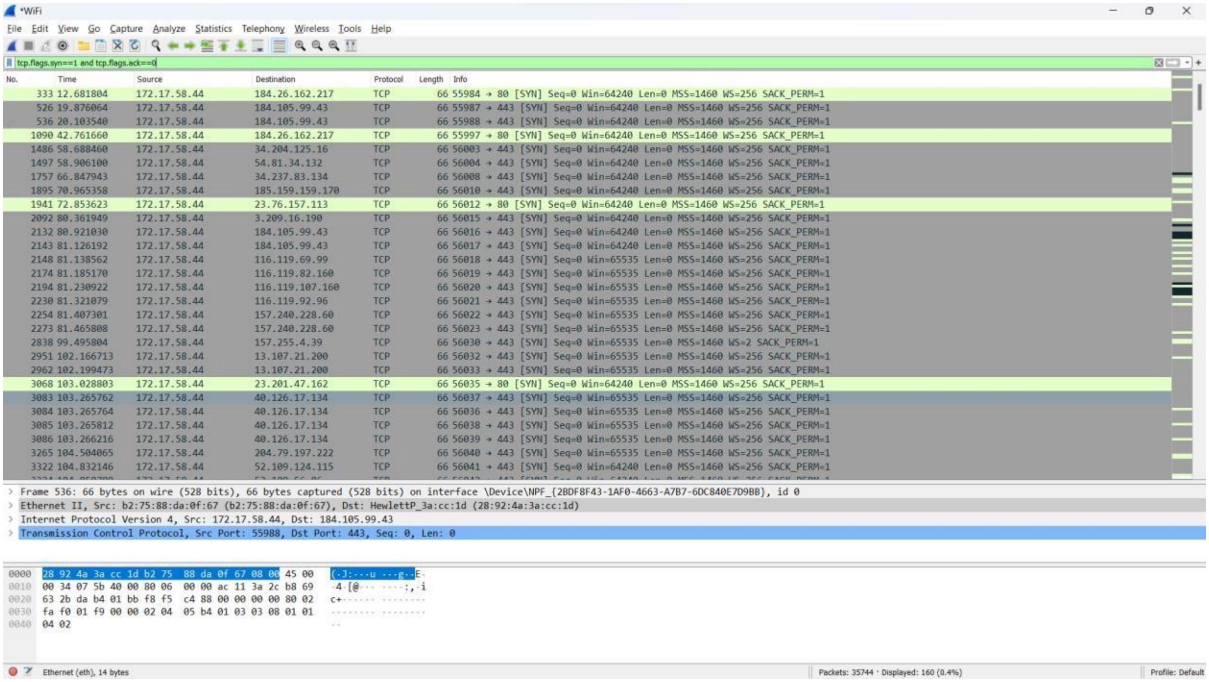
```
No.    Time        Source          Destination     Protocol  Length Info
  548 20.278491    172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
  553 20.481919    172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 2214 81.286743    172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 2284 81.485033    172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 3829 109.058345   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 3892 110.286889   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 5669 169.273827   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 5675 169.491483   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 7296 230.259619   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 7304 230.487563   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 9175 291.542307   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
 9176 291.543227   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
10471 352.380115   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
10480 352.492443   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
11670 413.409554   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
11673 413.483388   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
15432 474.264451   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
15445 474.729325   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
16654 535.269640   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
16671 535.661114   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
24839 596.279887   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
24845 596.483547   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
29916 657.412702   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
29924 657.545770   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
33060 742.405083   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
33066 742.611917   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
34996 803.236506   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
35003 803.482643   172.17.58.44    184.105.99.43   TLSv1.3   571 Client Hello
```

```
> Frame 548: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 184.105.99.43
> Transmission Control Protocol, Src Port: 55987, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  02 2d 07 5d 40 00 80 06  00 00 ac 11 3a 2c b8 69   ·-·]@··· ····:,·i
0020  63 2b da b3 01 bb 3e bb  93 16 35 c1 9a 26 50 18   c+····>· ··5··&P·
0030  01 00 03 f2 00 00 16 03  01 02 00 01 00 01 fc 03   ········ ········
0040  03 44 cc 09 8f ee 39 08  77 36 19 1e a8 73 26 62   ·D····9· w6···s&b
0050  f9 d2 23 31 ca ed 68 62  74 62 fe 6a 40 32 1b b6   ··#1··hb tb·j@2··
0060  28 20 e1 6c fc 9f 01 42  bc aa a6 67 fa ea d7 c6   ( ·l···B ···g····
```

Ethernet (eth), 14 bytes | Packets: 35744 · Displayed: 28 (0.1%) | Profile: Default

17. Detecting SYN Floods (Possible DDoS attacks)


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

```
tcp.flags.syn==1 and tcp.flags.ack==0
```

```
No.    Time        Source          Destination       Protocol  Length Info
  333 12.681804    172.17.58.44    184.26.162.217    TCP       66 55984 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  526 19.876064    172.17.58.44    184.105.99.43     TCP       66 55987 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  536 20.103540    172.17.58.44    184.105.99.43     TCP       66 55988 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1090 42.761660    172.17.58.44    184.26.162.217    TCP       66 55997 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1486 58.688460    172.17.58.44    34.204.125.16     TCP       66 56003 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1497 58.906100    172.17.58.44    54.81.34.132      TCP       66 56004 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1757 66.847943    172.17.58.44    34.237.83.134     TCP       66 56008 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1895 70.965358    172.17.58.44    185.159.159.170   TCP       66 56010 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1941 72.853623    172.17.58.44    23.76.157.113     TCP       66 56012 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2092 80.361949    172.17.58.44    3.209.16.190      TCP       66 56015 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2132 80.921030    172.17.58.44    184.105.99.43     TCP       66 56016 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2143 81.126192    172.17.58.44    184.105.99.43     TCP       66 56017 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2148 81.138562    172.17.58.44    116.119.69.99     TCP       66 56018 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2174 81.185170    172.17.58.44    116.119.82.160    TCP       66 56019 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2194 81.230922    172.17.58.44    116.119.107.160   TCP       66 56020 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2230 81.321079    172.17.58.44    116.119.92.96     TCP       66 56021 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2254 81.407301    172.17.58.44    157.240.228.60    TCP       66 56022 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2273 81.465808    172.17.58.44    157.240.228.60    TCP       66 56023 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2838 99.495804    172.17.58.44    157.255.4.39      TCP       66 56030 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2 SACK_PERM=1
 2951 102.166713   172.17.58.44    13.107.21.200     TCP       66 56032 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 2962 102.199473   172.17.58.44    13.107.21.200     TCP       66 56033 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3068 103.028803   172.17.58.44    23.201.47.162     TCP       66 56035 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3083 103.265762   172.17.58.44    40.126.17.134     TCP       66 56037 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3084 103.265764   172.17.58.44    40.126.17.134     TCP       66 56036 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3085 103.265812   172.17.58.44    40.126.17.134     TCP       66 56038 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3086 103.266216   172.17.58.44    40.126.17.134     TCP       66 56039 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3265 104.504065   172.17.58.44    204.79.197.222    TCP       66 56040 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
 3322 104.832146   172.17.58.44    52.109.124.115    TCP       66 56041 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
> Frame 536: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{2BDF8F43-1AF0-4663-A7B7-6DC840E7D9BB}, id 0
> Ethernet II, Src: b2:75:88:da:0f:67 (b2:75:88:da:0f:67), Dst: HewlettP_3a:cc:1d (28:92:4a:3a:cc:1d)
> Internet Protocol Version 4, Src: 172.17.58.44, Dst: 184.105.99.43
> Transmission Control Protocol, Src Port: 55988, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  28 92 4a 3a cc 1d b2 75  88 da 0f 67 08 00 45 00   (·J:···u ···g··E·
0010  00 34 07 5b 40 00 80 06  00 00 ac 11 3a 2c b8 69   ·4·[@··· ····:,·i
0020  63 2b da b4 01 bb f8 f5  c4 88 00 00 00 00 80 02   c+······ ········
0030  fa f0 01 f9 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

Ethernet (eth), 14 bytes | Packets: 35744 · Displayed: 160 (0.4%) | Profile: Default