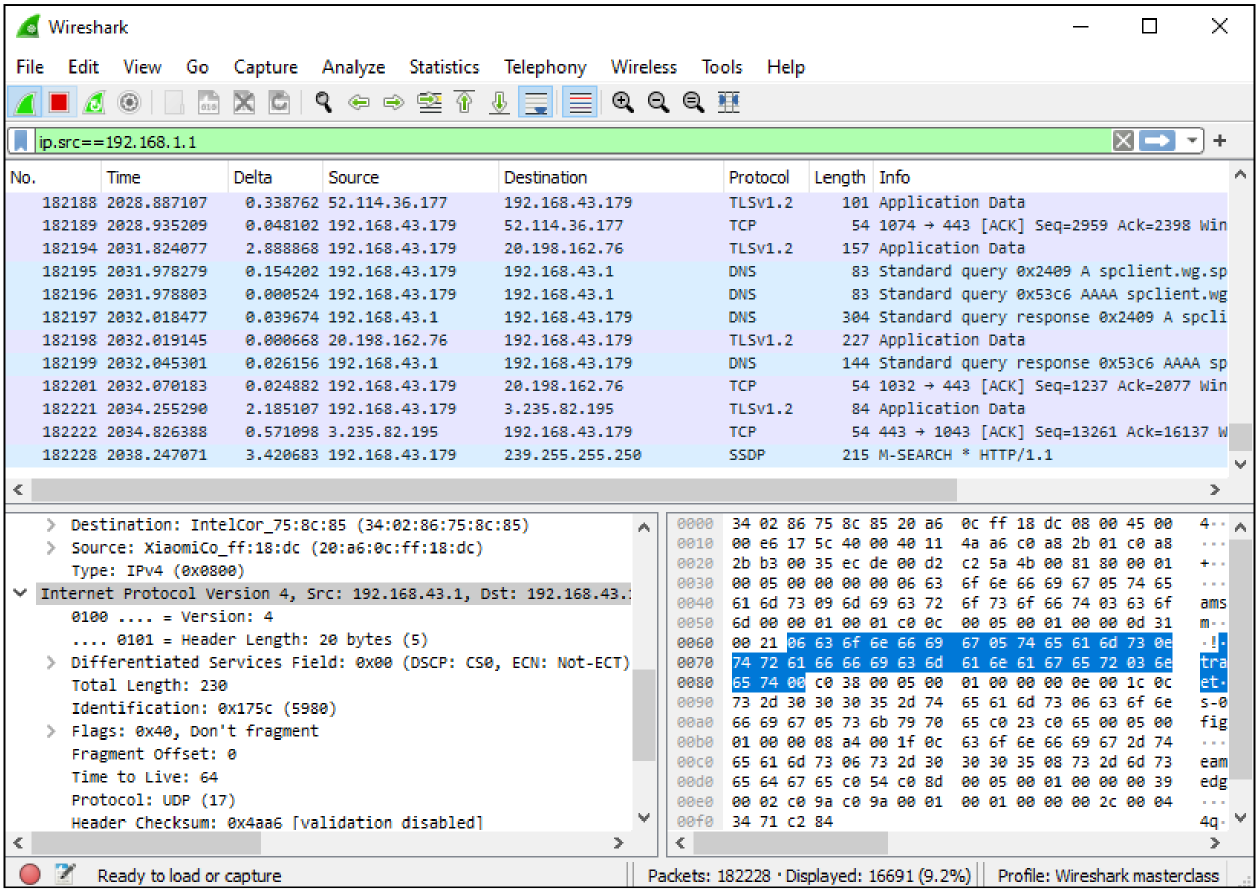
Wireshark

Wire shark is a protocol analyser. Some important filters are illustrated below:

1. Filtering packets from source Google.com (ip addr= 192.168.1.1)



Wireshark
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src==192.168.1.1

```
No.     Time        Delta    Source         Destination     Protocol Length Info
 182188 2028.887107 0.338762 52.114.36.177  192.168.43.179  TLSv1.2   101 Application Data
 182189 2028.935209 0.048102 192.168.43.179 52.114.36.177   TCP        54 1074 → 443 [ACK] Seq=2959 Ack=2398 Win
 182194 2031.824077 2.888868 192.168.43.179 20.198.162.76   TLSv1.2   157 Application Data
 182195 2031.978279 0.154202 192.168.43.179 192.168.43.1    DNS        83 Standard query 0x2409 A spclient.wg.sp
 182196 2031.978803 0.000524 192.168.43.179 192.168.43.1    DNS        83 Standard query 0x53c6 AAAA spclient.wg
 182197 2032.018477 0.039674 192.168.43.1   192.168.43.179  DNS       304 Standard query response 0x2409 A spcli
 182198 2032.019145 0.000668 20.198.162.76  192.168.43.179  TLSv1.2   227 Application Data
 182199 2032.045301 0.026156 192.168.43.1   192.168.43.179  DNS       144 Standard query response 0x53c6 AAAA sp
 182201 2032.070183 0.024882 192.168.43.179 20.198.162.76   TCP        54 1032 → 443 [ACK] Seq=1237 Ack=2077 Win
 182221 2034.255290 2.185107 192.168.43.179 3.235.82.195    TLSv1.2    84 Application Data
 182222 2034.826388 0.571098 3.235.82.195   192.168.43.179  TCP        54 443 → 1043 [ACK] Seq=13261 Ack=16137 W
 182228 2038.247071 3.420683 192.168.43.179 239.255.255.250 SSDP      215 M-SEARCH * HTTP/1.1
```

```
  > Destination: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Source: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 230
    Identification: 0x175c (5980)
  > Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x4aa6 [validation disabled]
```

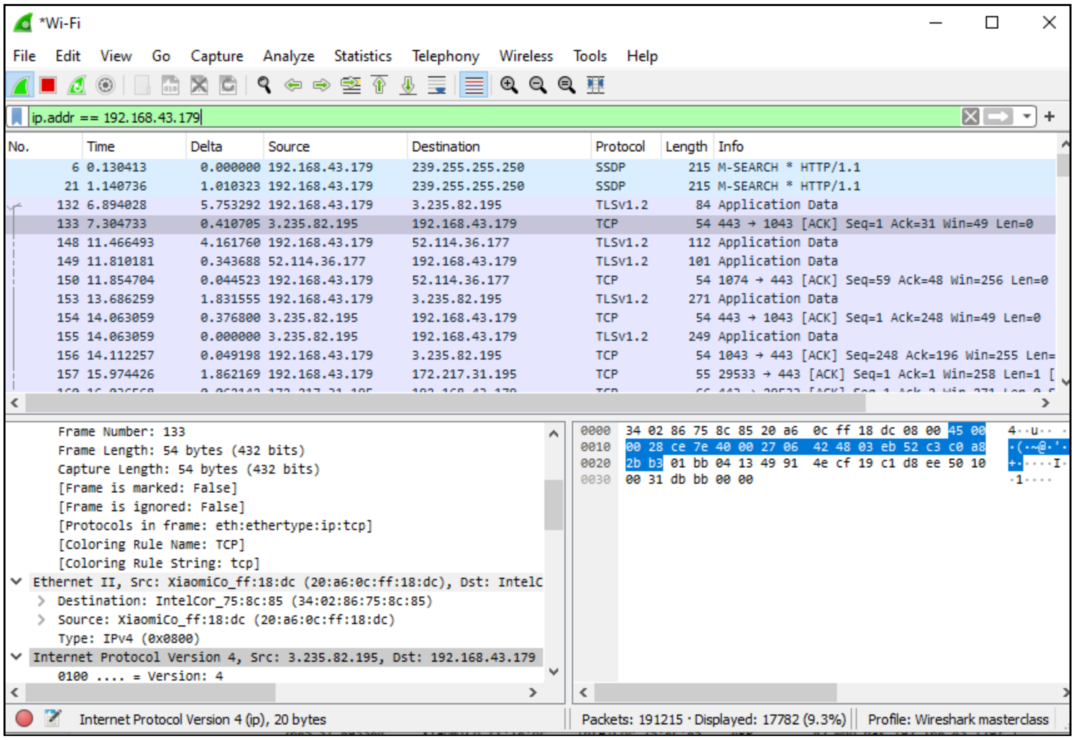
```
0000  34 02 86 75 8c 85 20 a6  0c ff 18 dc 08 00 45 00   4··
0010  00 e6 17 5c 40 00 40 11  4a a6 c0 a8 2b 01 c0 a8   ···
0020  2b b3 00 35 ec de 00 d2  c2 5a 4b 00 81 80 00 01   +··
0030  00 05 00 00 00 00 06 63  6f 6e 66 69 67 05 74 65   ···
0040  61 6d 73 09 6d 69 63 72  6f 73 6f 66 74 03 63 6f   ams
0050  6d 00 00 01 00 01 c0 0c  00 05 00 01 00 00 0d 31   m··
0060  00 21 06 63 6f 6e 66 69  67 05 74 65 61 6d 73 0e   ·!·
0070  74 72 61 66 66 69 63 6d  61 6e 61 67 65 72 03 6e   tra
0080  65 74 00 c0 38 00 05 00  01 00 00 00 0e 00 1c 0c   et·
0090  73 2d 30 30 30 35 2d 74  65 61 6d 73 06 63 6f 6e   s-0
00a0  66 69 67 05 73 6b 79 70  65 c0 23 c0 65 00 05 00   fig
00b0  01 00 00 08 a4 00 1f 0c  63 6f 6e 66 69 67 2d 74   ···
00c0  65 61 6d 73 06 73 2d 30  30 30 35 08 73 2d 6d 73   eam
00d0  65 64 67 65 c0 54 c0 8d  00 05 00 01 00 00 00 39   edg
00e0  00 02 c0 9a c0 9a 00 01  00 01 00 00 00 2c 00 04   ···
00f0  34 71 c2 84                                        4q·
```

Ready to load or capture

Packets: 182228 · Displayed: 16691 (9.2%)

Profile: Wireshark masterclass

2.Filtering a particular ip address:


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

ip.addr == 192.168.43.179

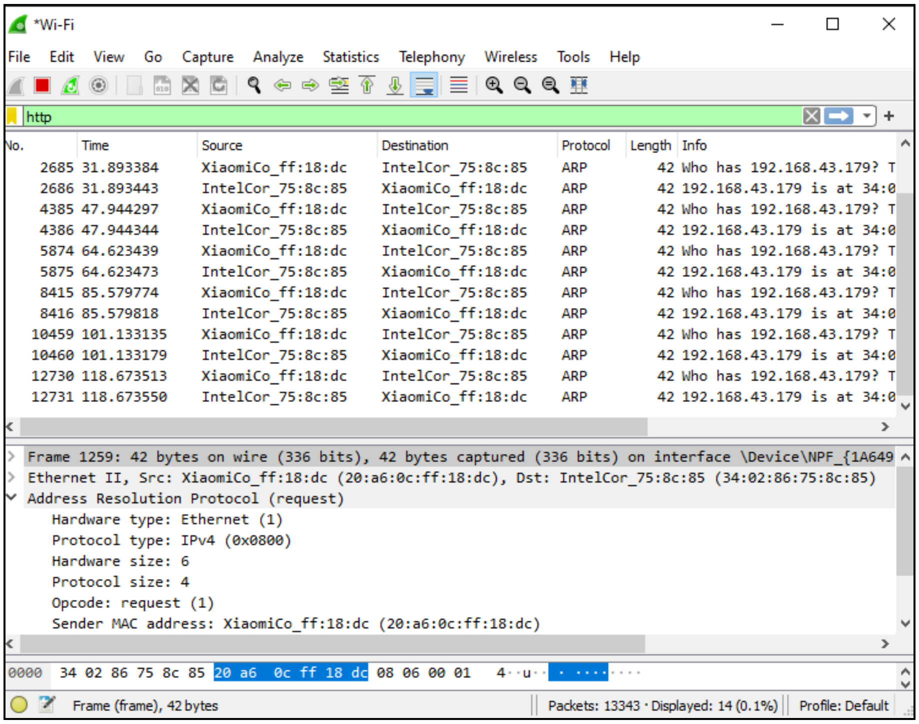
```
No.     Time        Delta    Source           Destination      Protocol Length Info
      6 0.130413    0.000000 192.168.43.179   239.255.255.250  SSDP        215 M-SEARCH * HTTP/1.1
     21 1.140736    1.010323 192.168.43.179   239.255.255.250  SSDP        215 M-SEARCH * HTTP/1.1
    132 6.894028    5.753292 192.168.43.179   3.235.82.195     TLSv1.2      84 Application Data
    133 7.304733    0.410705 3.235.82.195     192.168.43.179   TCP          54 443 → 1043 [ACK] Seq=1 Ack=31 Win=49 Len=0
    148 11.466493   4.161760 192.168.43.179   52.114.36.177    TLSv1.2     112 Application Data
    149 11.810181   0.343688 52.114.36.177    192.168.43.179   TLSv1.2     101 Application Data
    150 11.854704   0.044523 192.168.43.179   52.114.36.177    TCP          54 1074 → 443 [ACK] Seq=59 Ack=48 Win=256 Len=0
    153 13.686259   1.831555 192.168.43.179   3.235.82.195     TLSv1.2     271 Application Data
    154 14.063059   0.376800 3.235.82.195     192.168.43.179   TCP          54 443 → 1043 [ACK] Seq=1 Ack=248 Win=49 Len=0
    155 14.063059   0.000000 3.235.82.195     192.168.43.179   TLSv1.2     249 Application Data
    156 14.112257   0.049198 192.168.43.179   3.235.82.195     TCP          54 1043 → 443 [ACK] Seq=248 Ack=196 Win=255 Len=
    157 15.974426   1.862169 192.168.43.179   172.217.31.195   TCP          55 29533 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [
```

```
    Frame Number: 133
    Frame Length: 54 bytes (432 bits)
    Capture Length: 54 bytes (432 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
v Ethernet II, Src: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc), Dst: IntelC
  > Destination: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Source: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 3.235.82.195, Dst: 192.168.43.179
    0100 .... = Version: 4
```

```
0000  34 02 86 75 8c 85 20 a6  0c ff 18 dc 08 00 45 00   4··u·· ·
0010  00 28 ce 7e 40 00 27 06  42 48 03 eb 52 c3 c0 a8   ·(·~@·'·
0020  2b b3 01 bb 04 13 49 91  4e cf 19 c1 d8 ee 50 10   +·····I·
0030  00 31 db bb 00 00                                  ·1····
```

Internet Protocol Version 4 (ip), 20 bytes || Packets: 191215 · Displayed: 17782 (9.3%) || Profile: Wireshark masterclass

3. Filter HTTP addresses


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

http

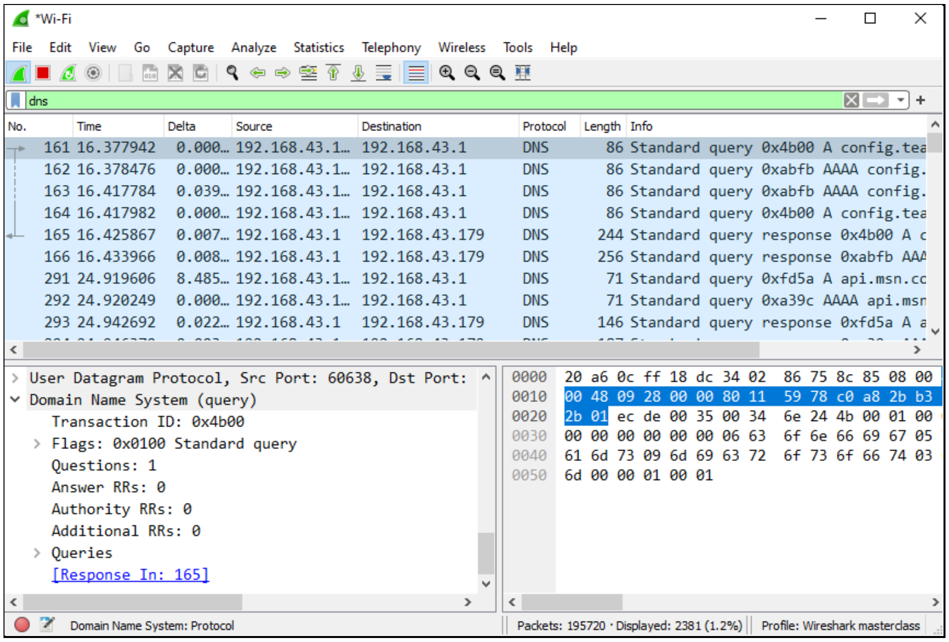
```
No.   Time        Source             Destination        Protocol  Length Info
 2685 31.893384   XiaomiCo_ff:18:dc  IntelCor_75:8c:85  ARP           42 Who has 192.168.43.179? T
 2686 31.893443   IntelCor_75:8c:85  XiaomiCo_ff:18:dc  ARP           42 192.168.43.179 is at 34:0
 4385 47.944297   XiaomiCo_ff:18:dc  IntelCor_75:8c:85  ARP           42 Who has 192.168.43.179? T
 4386 47.944344   IntelCor_75:8c:85  XiaomiCo_ff:18:dc  ARP           42 192.168.43.179 is at 34:0
 5874 64.623439   XiaomiCo_ff:18:dc  IntelCor_75:8c:85  ARP           42 Who has 192.168.43.179? T
 5875 64.623473   IntelCor_75:8c:85  XiaomiCo_ff:18:dc  ARP           42 192.168.43.179 is at 34:0
 8415 85.579774   XiaomiCo_ff:18:dc  IntelCor_75:8c:85  ARP           42 Who has 192.168.43.179? T
 8416 85.579818   IntelCor_75:8c:85  XiaomiCo_ff:18:dc  ARP           42 192.168.43.179 is at 34:0
10459 101.133135  XiaomiCo_ff:18:dc  IntelCor_75:8c:85  ARP           42 Who has 192.168.43.179? T
10460 101.133179  IntelCor_75:8c:85  XiaomiCo_ff:18:dc  ARP           42 192.168.43.179 is at 34:0
12730 118.673513  XiaomiCo_ff:18:dc  IntelCor_75:8c:85  ARP           42 Who has 192.168.43.179? T
12731 118.673550  IntelCor_75:8c:85  XiaomiCo_ff:18:dc  ARP           42 192.168.43.179 is at 34:0
```

```
> Frame 1259: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{1A649
> Ethernet II, Src: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc), Dst: IntelCor_75:8c:85 (34:02:86:75:8c:85)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc)
```

```
0000  34 02 86 75 8c 85 20 a6  0c ff 18 dc 08 06 00 01   4··u·· ·······
```

Frame (frame), 42 bytes || Packets: 13343 · Displayed: 14 (0.1%) || Profile: Default

4. Filtering traffic based on protocol:


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

```
dns
```

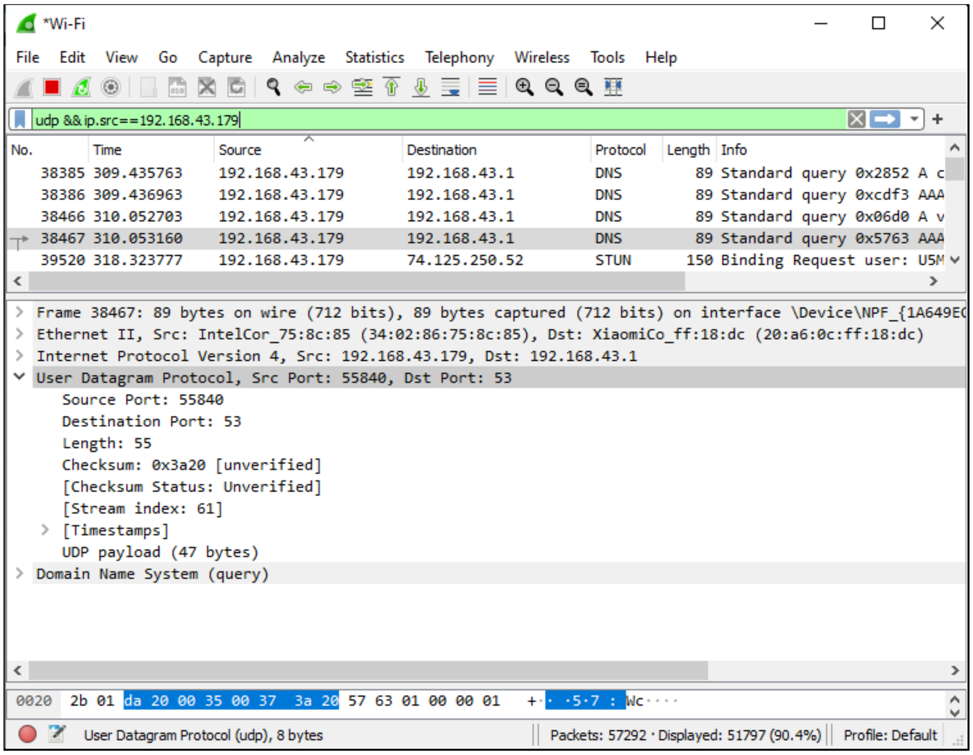
```
No.   Time       Delta   Source          Destination     Protocol Length Info
  161 16.377942  0.000…  192.168.43.1…   192.168.43.1    DNS         86 Standard query 0x4b00 A config.tea
  162 16.378476  0.000…  192.168.43.1…   192.168.43.1    DNS         86 Standard query 0xabfb AAAA config.
  163 16.417784  0.039…  192.168.43.1…   192.168.43.1    DNS         86 Standard query 0xabfb AAAA config.
  164 16.417982  0.000…  192.168.43.1…   192.168.43.1    DNS         86 Standard query 0x4b00 A config.tea
  165 16.425867  0.007…  192.168.43.1    192.168.43.179  DNS        244 Standard query response 0x4b00 A c
  166 16.433966  0.008…  192.168.43.1    192.168.43.179  DNS        256 Standard query response 0xabfb AAA
  291 24.919606  8.485…  192.168.43.1…   192.168.43.1    DNS         71 Standard query 0xfd5a A api.msn.cc
  292 24.920249  0.000…  192.168.43.1…   192.168.43.1    DNS         71 Standard query 0xa39c AAAA api.msn
  293 24.942692  0.022…  192.168.43.1    192.168.43.179  DNS        146 Standard query response 0xfd5a A a
```

```
> User Datagram Protocol, Src Port: 60638, Dst Port:
v Domain Name System (query)
    Transaction ID: 0x4b00
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  > Queries
    [Response In: 165]
```

```
0000  20 a6 0c ff 18 dc 34 02  86 75 8c 85 08 00
0010  00 48 09 28 00 00 80 11  59 78 c0 a8 2b b3
0020  2b 01 ec de 00 35 00 34  6e 24 4b 00 01 00
0030  00 00 00 00 00 00 06 63  6f 6e 66 69 67 05
0040  61 6d 73 09 6d 69 63 72  6f 73 6f 66 74 03
0050  6d 00 00 01 00 01
```

Domain Name System: Protocol | Packets: 195720 · Displayed: 2381 (1.2%) | Profile: Wireshark masterclass

5. Filtering UDP from a particular source


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

```
udp && ip.src==192.168.43.179
```

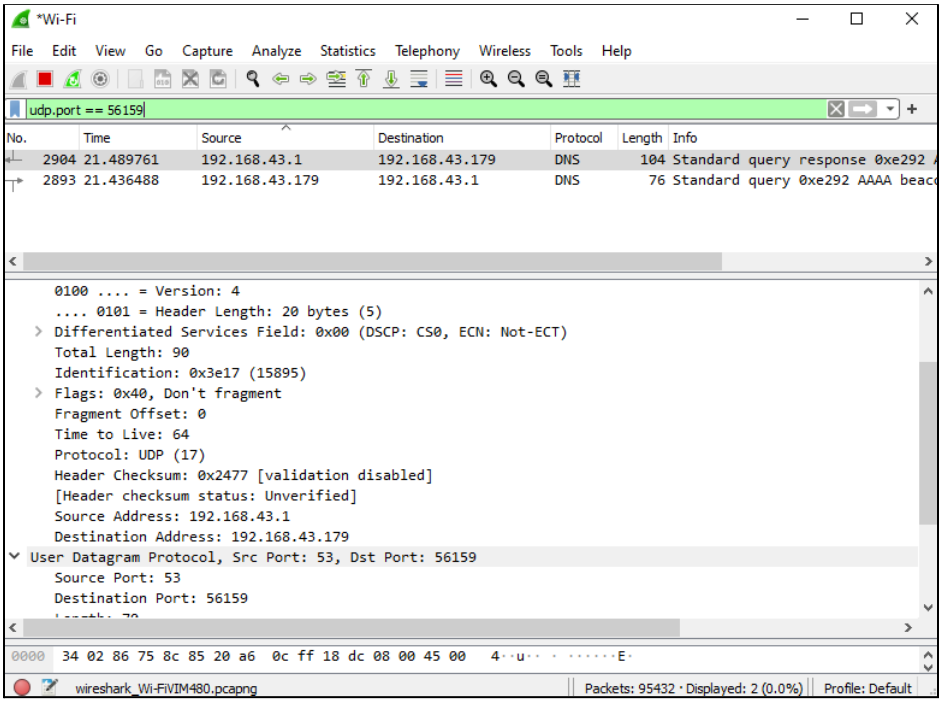
```
No.     Time        Source          Destination     Protocol Length Info
  38385 309.435763  192.168.43.179  192.168.43.1    DNS          89 Standard query 0x2852 A c
  38386 309.436963  192.168.43.179  192.168.43.1    DNS          89 Standard query 0xcdf3 AAA
  38466 310.052703  192.168.43.179  192.168.43.1    DNS          89 Standard query 0x06d0 A v
  38467 310.053160  192.168.43.179  192.168.43.1    DNS          89 Standard query 0x5763 AAA
  39520 318.323777  192.168.43.179  74.125.250.52   STUN        150 Binding Request user: U5M
```

```
> Frame 38467: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface \Device\NPF_{1A649EC
> Ethernet II, Src: IntelCor_75:8c:85 (34:02:86:75:8c:85), Dst: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc)
> Internet Protocol Version 4, Src: 192.168.43.179, Dst: 192.168.43.1
v User Datagram Protocol, Src Port: 55840, Dst Port: 53
    Source Port: 55840
    Destination Port: 53
    Length: 55
    Checksum: 0x3a20 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 61]
  > [Timestamps]
    UDP payload (47 bytes)
> Domain Name System (query)
```

```
0020  2b 01 da 20 00 35 00 37  3a 20 57 63 01 00 00 01   +· ·5·7 : Wc····
```

User Datagram Protocol (udp), 8 bytes | Packets: 57292 · Displayed: 51797 (90.4%) | Profile: Default

6. Filtering UDP port


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

udp.port == 56159

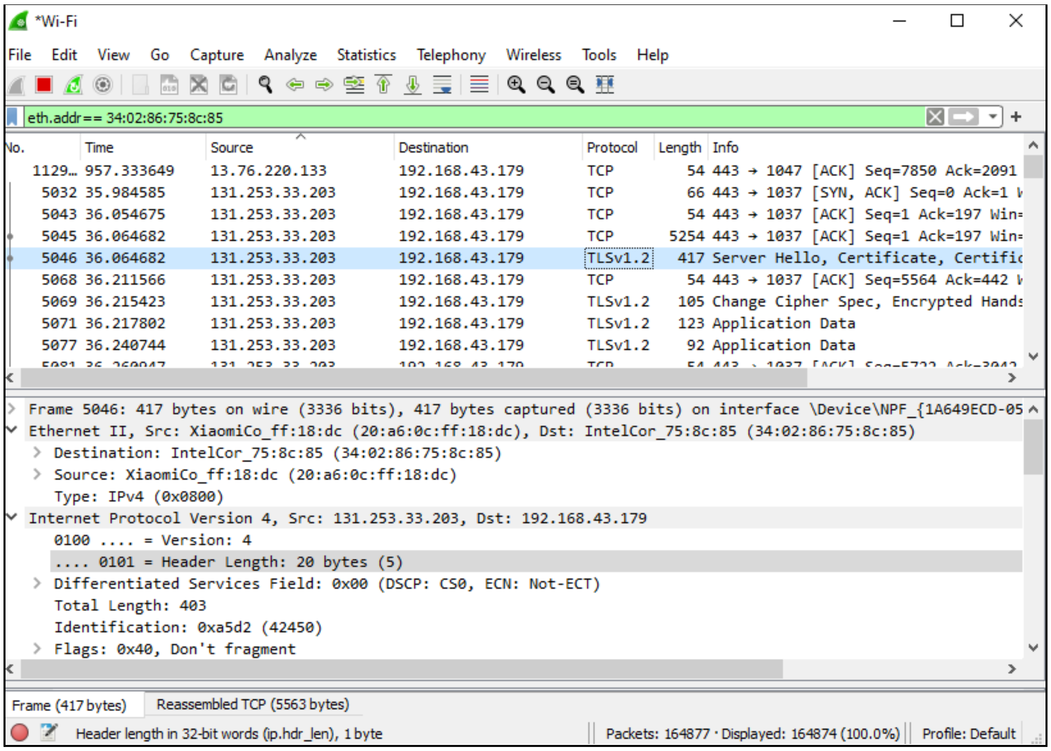
```
No.     Time        Source          Destination     Protocol  Length Info
   2904 21.489761   192.168.43.1    192.168.43.179  DNS          104 Standard query response 0xe292 A
   2893 21.436488   192.168.43.179  192.168.43.1    DNS           76 Standard query 0xe292 AAAA beac
```

```
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 90
      Identification: 0x3e17 (15895)
    > Flags: 0x40, Don't fragment
      Fragment Offset: 0
      Time to Live: 64
      Protocol: UDP (17)
      Header Checksum: 0x2477 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.43.1
      Destination Address: 192.168.43.179
  v User Datagram Protocol, Src Port: 53, Dst Port: 56159
      Source Port: 53
      Destination Port: 56159
```

```
0000  34 02 86 75 8c 85 20 a6  0c ff 18 dc 08 00 45 00   4··u·· · ······E·
```

wireshark_Wi-FiVIM480.pcapng | Packets: 95432 · Displayed: 2 (0.0%) | Profile: Default

7. Filtering by MAC address


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

eth.addr== 34:02:86:75:8c:85

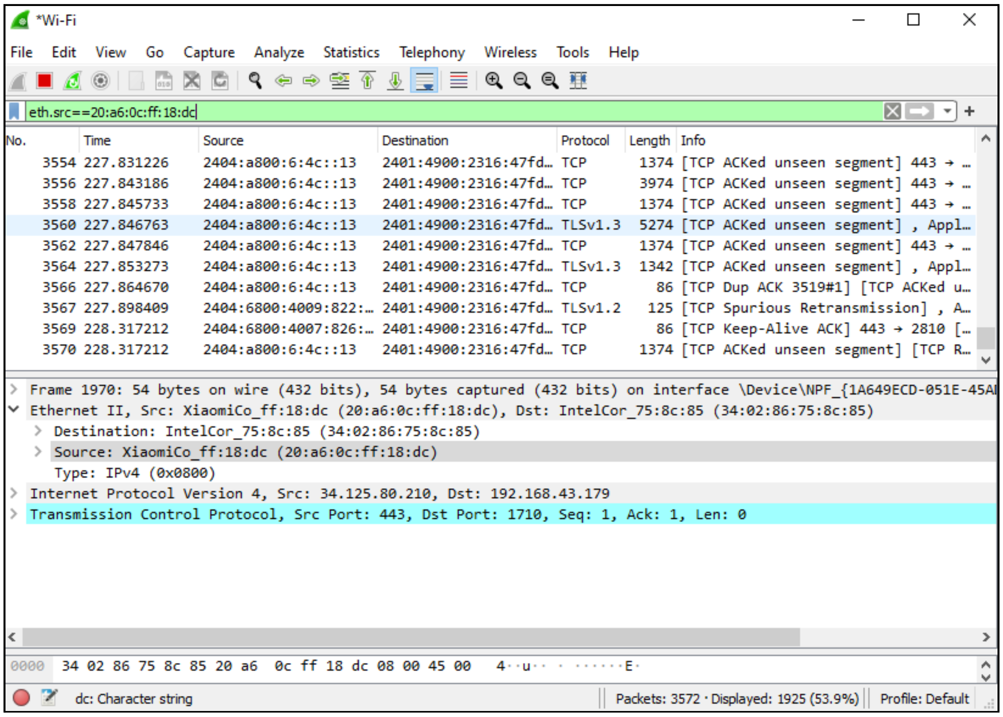
```
No.     Time        Source          Destination     Protocol  Length Info
1129…  957.333649   13.76.220.133   192.168.43.179  TCP           54 443 → 1047 [ACK] Seq=7850 Ack=2091
   5032 35.984585   131.253.33.203  192.168.43.179  TCP           66 443 → 1037 [SYN, ACK] Seq=0 Ack=1 W
   5043 36.054675   131.253.33.203  192.168.43.179  TCP           54 443 → 1037 [ACK] Seq=1 Ack=197 Win=
   5045 36.064682   131.253.33.203  192.168.43.179  TCP         5254 443 → 1037 [ACK] Seq=1 Ack=197 Win=
   5046 36.064682   131.253.33.203  192.168.43.179  TLSv1.2      417 Server Hello, Certificate, Certific
   5068 36.211566   131.253.33.203  192.168.43.179  TCP           54 443 → 1037 [ACK] Seq=5564 Ack=442 W
   5069 36.215423   131.253.33.203  192.168.43.179  TLSv1.2      105 Change Cipher Spec, Encrypted Hands
   5071 36.217802   131.253.33.203  192.168.43.179  TLSv1.2      123 Application Data
   5077 36.240744   131.253.33.203  192.168.43.179  TLSv1.2       92 Application Data
```

```
> Frame 5046: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits) on interface \Device\NPF_{1A649ECD-05
v Ethernet II, Src: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc), Dst: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Destination: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Source: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 131.253.33.203, Dst: 192.168.43.179
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 403
    Identification: 0xa5d2 (42450)
  > Flags: 0x40, Don't fragment
```

Frame (417 bytes) | Reassembled TCP (5563 bytes)

Header length in 32-bit words (ip.hdr_len), 1 byte | Packets: 164877 · Displayed: 164874 (100.0%) | Profile: Default

8. Filtering specific source address


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

```
eth.src==20:a6:0c:ff:18:dc
```

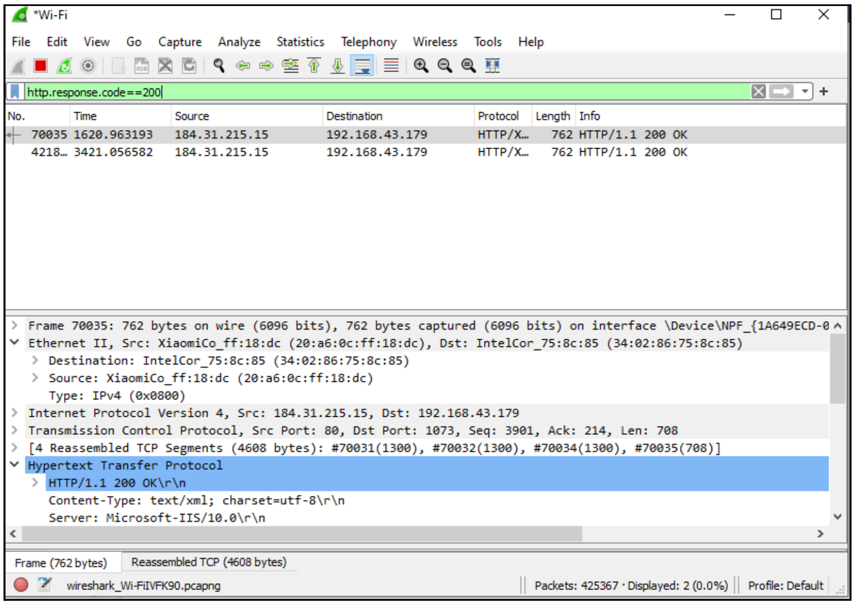
```
No.   Time        Source                Destination           Protocol Length Info
 3554 227.831226  2404:a800:6:4c::13    2401:4900:2316:47fd…  TCP      1374 [TCP ACKed unseen segment] 443 → …
 3556 227.843186  2404:a800:6:4c::13    2401:4900:2316:47fd…  TCP      3974 [TCP ACKed unseen segment] 443 → …
 3558 227.845733  2404:a800:6:4c::13    2401:4900:2316:47fd…  TCP      1374 [TCP ACKed unseen segment] 443 → …
 3560 227.846763  2404:a800:6:4c::13    2401:4900:2316:47fd…  TLSv1.3  5274 [TCP ACKed unseen segment] , Appl…
 3562 227.847846  2404:a800:6:4c::13    2401:4900:2316:47fd…  TCP      1374 [TCP ACKed unseen segment] 443 → …
 3564 227.853273  2404:a800:6:4c::13    2401:4900:2316:47fd…  TLSv1.3  1342 [TCP ACKed unseen segment] , Appl…
 3566 227.864670  2404:a800:6:4c::13    2401:4900:2316:47fd…  TCP        86 [TCP Dup ACK 3519#1] [TCP ACKed u…
 3567 227.898409  2404:6800:4009:822:…  2401:4900:2316:47fd…  TLSv1.2   125 [TCP Spurious Retransmission] , A…
 3569 228.317212  2404:6800:4007:826:…  2401:4900:2316:47fd…  TCP        86 [TCP Keep-Alive ACK] 443 → 2810 […
 3570 228.317212  2404:a800:6:4c::13    2401:4900:2316:47fd…  TCP      1374 [TCP ACKed unseen segment] [TCP R…
```

```
> Frame 1970: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{1A649ECD-051E-45A
v Ethernet II, Src: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc), Dst: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Destination: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Source: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 34.125.80.210, Dst: 192.168.43.179
> Transmission Control Protocol, Src Port: 443, Dst Port: 1710, Seq: 1, Ack: 1, Len: 0
```

```
0000  34 02 86 75 8c 85 20 a6  0c ff 18 dc 08 00 45 00   4··u·· · ······E·
```

```
dc: Character string          Packets: 3572 · Displayed: 1925 (53.9%)    Profile: Default
```

9. Filtering by response code:


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

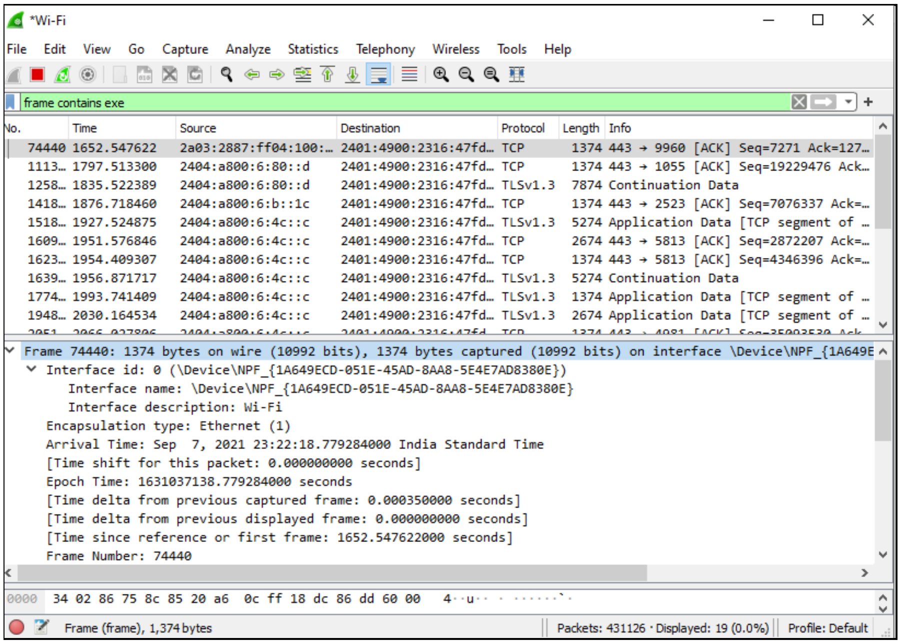
```
http.response.code==200
```

```
No.   Time         Source         Destination     Protocol Length Info
70035 1620.963193  184.31.215.15  192.168.43.179  HTTP/X…    762 HTTP/1.1 200 OK
4218… 3421.056582  184.31.215.15  192.168.43.179  HTTP/X…    762 HTTP/1.1 200 OK
```

```
> Frame 70035: 762 bytes on wire (6096 bits), 762 bytes captured (6096 bits) on interface \Device\NPF_{1A649ECD-0
v Ethernet II, Src: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc), Dst: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Destination: IntelCor_75:8c:85 (34:02:86:75:8c:85)
  > Source: XiaomiCo_ff:18:dc (20:a6:0c:ff:18:dc)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 184.31.215.15, Dst: 192.168.43.179
> Transmission Control Protocol, Src Port: 80, Dst Port: 1073, Seq: 3901, Ack: 214, Len: 708
> [4 Reassembled TCP Segments (4608 bytes): #70031(1300), #70032(1300), #70034(1300), #70035(708)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: text/xml; charset=utf-8\r\n
    Server: Microsoft-IIS/10.0\r\n
```

```
Frame (762 bytes)    Reassembled TCP (4608 bytes)
wireshark_Wi-FiIVFK90.pcapng          Packets: 425367 · Displayed: 2 (0.0%)    Profile: Default
```

10. Finding executable file types:


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

frame contains exe

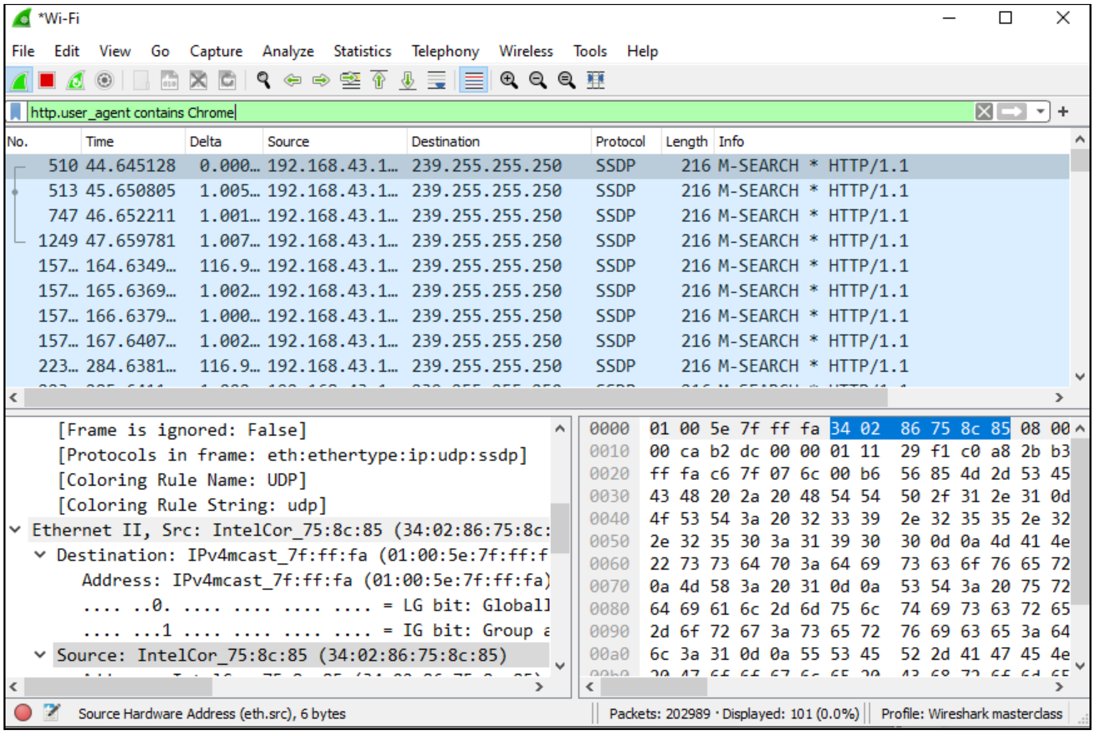
```
No.    Time         Source                  Destination           Protocol Length Info
74440 1652.547622  2a03:2887:ff04:100:…  2401:4900:2316:47fd… TCP      1374 443 → 9960 [ACK] Seq=7271 Ack=127…
1113… 1797.513300  2404:a800:6:80::d     2401:4900:2316:47fd… TCP      1374 443 → 1055 [ACK] Seq=19229476 Ack…
1258… 1835.522389  2404:a800:6:80::d     2401:4900:2316:47fd… TLSv1.3  7874 Continuation Data
1418… 1876.718460  2404:a800:6:b::1c     2401:4900:2316:47fd… TCP      1374 443 → 2523 [ACK] Seq=7076337 Ack=…
1518… 1927.524875  2404:a800:6:4c::c     2401:4900:2316:47fd… TLSv1.3  5274 Application Data [TCP segment of …
1609… 1951.576846  2404:a800:6:4c::c     2401:4900:2316:47fd… TCP      2674 443 → 5813 [ACK] Seq=2872207 Ack=…
1623… 1954.409307  2404:a800:6:4c::c     2401:4900:2316:47fd… TCP      1374 443 → 5813 [ACK] Seq=4346396 Ack=…
1639… 1956.871717  2404:a800:6:4c::c     2401:4900:2316:47fd… TLSv1.3  5274 Continuation Data
1774… 1993.741409  2404:a800:6:4c::c     2401:4900:2316:47fd… TLSv1.3  1374 Application Data [TCP segment of …
1948… 2030.164534  2404:a800:6:4c::c     2401:4900:2316:47fd… TLSv1.3  2674 Application Data [TCP segment of …
```

```
Frame 74440: 1374 bytes on wire (10992 bits), 1374 bytes captured (10992 bits) on interface \Device\NPF_{1A649E
  Interface id: 0 (\Device\NPF_{1A649ECD-051E-45AD-8AA8-5E4E7AD8380E})
      Interface name: \Device\NPF_{1A649ECD-051E-45AD-8AA8-5E4E7AD8380E}
      Interface description: Wi-Fi
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep  7, 2021 23:22:18.779284000 India Standard Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1631037138.779284000 seconds
  [Time delta from previous captured frame: 0.000350000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 1652.547622000 seconds]
  Frame Number: 74440
```

```
0000  34 02 86 75 8c 85 20 a6  0c ff 18 dc 86 dd 60 00   4··u·· · ······`·
```

Frame (frame), 1,374 bytes | Packets: 431126 · Displayed: 19 (0.0%) | Profile: Default

11. Finding user agents


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

http.user_agent contains Chrome

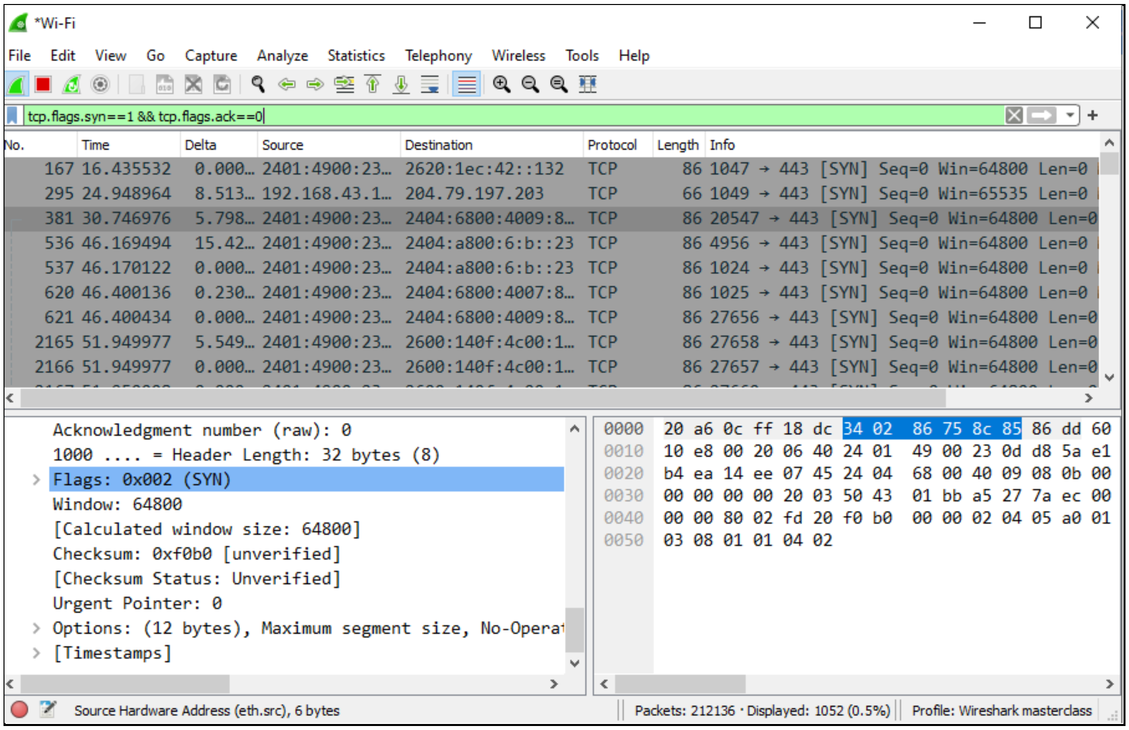
```
No.   Time        Delta    Source           Destination       Protocol Length Info
 510 44.645128    0.000…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
 513 45.650805    1.005…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
 747 46.652211    1.001…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
1249 47.659781    1.007…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
157… 164.6349…  116.9…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
157… 165.6369…    1.002…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
157… 166.6379…    1.000…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
157… 167.6407…    1.002…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
223… 284.6381…  116.9…  192.168.43.1…  239.255.255.250   SSDP      216 M-SEARCH * HTTP/1.1
```

```
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:ssdp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  Ethernet II, Src: IntelCor_75:8c:85 (34:02:86:75:8c:
    Destination: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:f
        Address: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
        .... ..0. .... .... .... .... = LG bit: Globall
        .... ...1 .... .... .... .... = IG bit: Group a
    Source: IntelCor_75:8c:85 (34:02:86:75:8c:85)
```

```
0000  01 00 5e 7f ff fa 34 02  86 75 8c 85 08 00
0010  00 ca b2 dc 00 00 01 11  29 f1 c0 a8 2b b3
0020  ff fa c6 7f 07 6c 00 b6  56 85 4d 2d 53 45
0030  43 48 20 2a 20 48 54 54  50 2f 31 2e 31 0d
0040  4f 53 54 3a 20 32 33 39  2e 32 35 35 2e 32
0050  2e 32 35 30 3a 31 39 30  30 0d 0a 4d 41 4e
0060  22 73 73 64 70 3a 64 69  73 63 6f 76 65 72
0070  0a 4d 58 3a 20 31 0d 0a  53 54 3a 20 75 72
0080  64 69 61 6c 2d 6d 75 6c  74 69 73 63 72 65
0090  2d 6f 72 67 3a 73 65 72  76 69 63 65 3a 64
00a0  6c 3a 31 0d 0a 55 53 45  52 2d 41 47 45 4e
```

Source Hardware Address (eth.src), 6 bytes | Packets: 202989 · Displayed: 101 (0.0%) | Profile: Wireshark masterclass

12. Detecting SYN floods(Possible DDoS attacks)


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

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

```
No.   Time      Delta   Source          Destination        Protocol Length Info
 167 16.435532 0.000… 2401:4900:23… 2620:1ec:42::132    TCP   86 1047 → 443 [SYN] Seq=0 Win=64800 Len=0
 295 24.948964 8.513… 192.168.43.1… 204.79.197.203      TCP   66 1049 → 443 [SYN] Seq=0 Win=65535 Len=0
 381 30.746976 5.798… 2401:4900:23… 2404:6800:4009:8…   TCP   86 20547 → 443 [SYN] Seq=0 Win=64800 Len=0
 536 46.169494 15.42… 2401:4900:23… 2404:a800:6:b::23   TCP   86 4956 → 443 [SYN] Seq=0 Win=64800 Len=0
 537 46.170122 0.000… 2401:4900:23… 2404:a800:6:b::23   TCP   86 1024 → 443 [SYN] Seq=0 Win=64800 Len=0
 620 46.400136 0.230… 2401:4900:23… 2404:6800:4007:8…   TCP   86 1025 → 443 [SYN] Seq=0 Win=64800 Len=0
 621 46.400434 0.000… 2401:4900:23… 2404:6800:4009:8…   TCP   86 27656 → 443 [SYN] Seq=0 Win=64800 Len=0
2165 51.949977 5.549… 2401:4900:23… 2600:140f:4c00:1…   TCP   86 27658 → 443 [SYN] Seq=0 Win=64800 Len=0
2166 51.949977 0.000… 2401:4900:23… 2600:140f:4c00:1…   TCP   86 27657 → 443 [SYN] Seq=0 Win=64800 Len=0
```

```
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
> Flags: 0x002 (SYN)
  Window: 64800
  [Calculated window size: 64800]
  Checksum: 0xf0b0 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
> Options: (12 bytes), Maximum segment size, No-Operat
> [Timestamps]
```

```
0000  20 a6 0c ff 18 dc 34 02  86 75 8c 85 86 dd 60
0010  10 e8 00 20 06 40 24 01  49 00 23 0d d8 5a e1
0020  b4 ea 14 ee 07 45 24 04  68 00 40 09 08 0b 00
0030  00 00 00 00 20 03 50 43  01 bb a5 27 7a ec 00
0040  00 00 80 02 fd 20 f0 b0  00 00 02 04 05 a0 01
0050  03 08 01 01 04 02
```

Source Hardware Address (eth.src), 6 bytes | Packets: 212136 · Displayed: 1052 (0.5%) | Profile: Wireshark masterclass

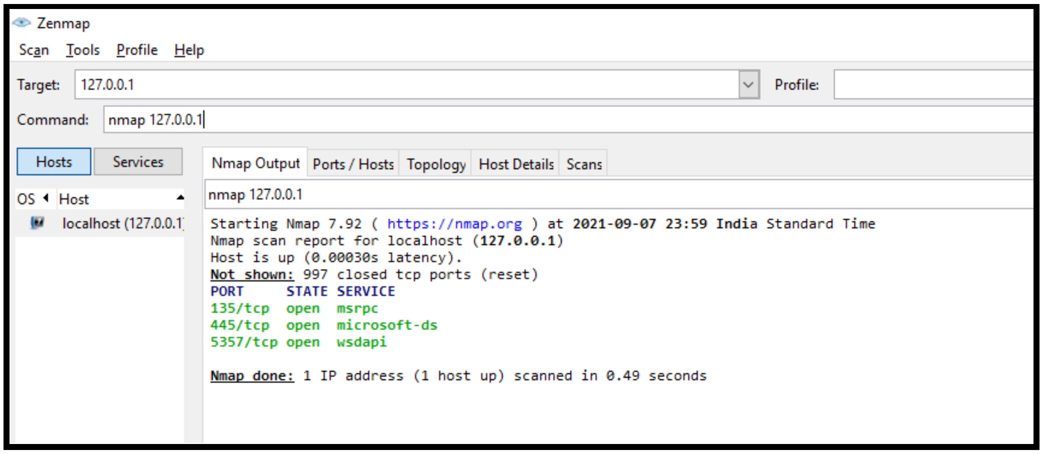
This will filter for the start of new TCP connections. If you see a constant new connections to the same destination IP, it could be a SYN or DDoS attack.

Nmap:

nmap — Network exploration tool and security / port scanner

Synopsis: nmap [<*Scan Type*> ...] [<*Options*>] { <*target specification*> }

1. Scanning localhost:



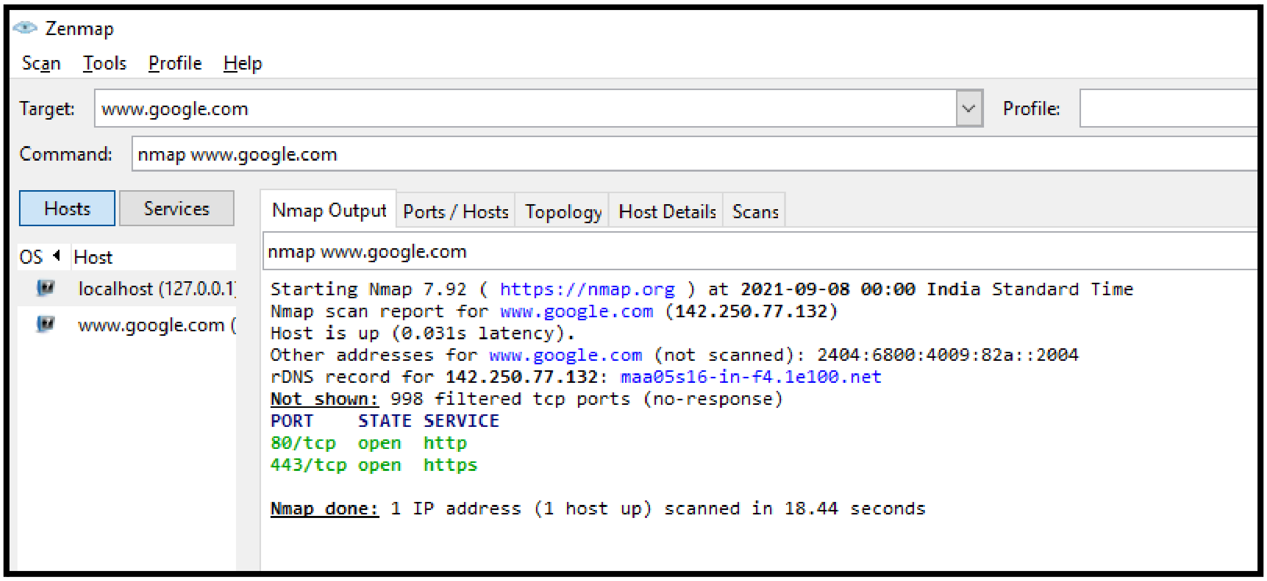
Target: 127.0.0.1

Command: nmap 127.0.0.1

```
nmap 127.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-07 23:59 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00030s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

Result:997 closed ports (ports that aren't listening)

2. Scanning target google.com

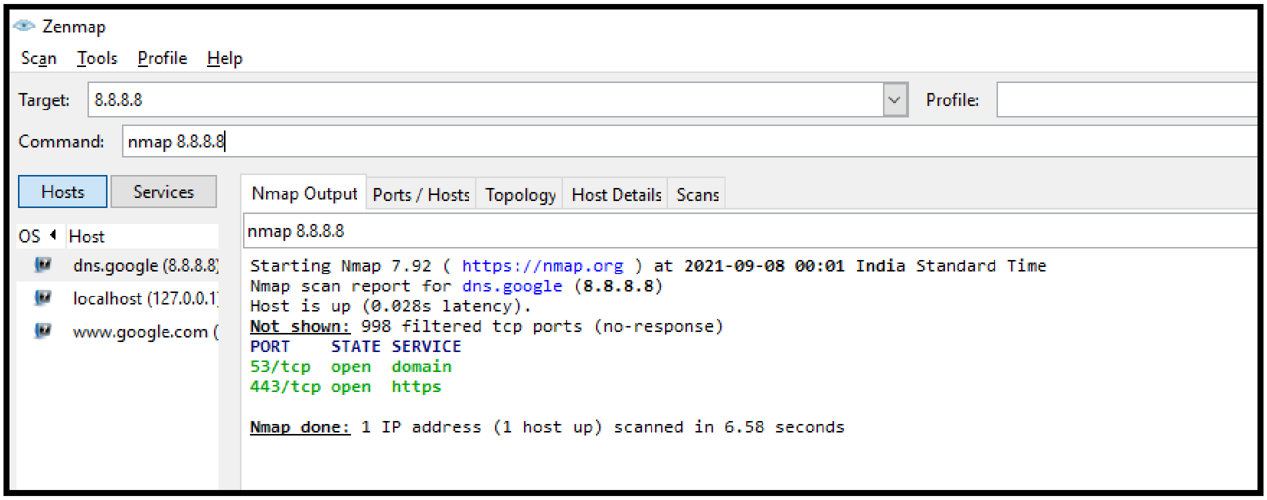


Target: www.google.com

Command: nmap www.google.com

```
nmap www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 00:00 India Standard Time
Nmap scan report for www.google.com (142.250.77.132)
Host is up (0.031s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82a::2004
rDNS record for 142.250.77.132: maa05s16-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 18.44 seconds
```

3. Scanning google DNS 8.8.8.8

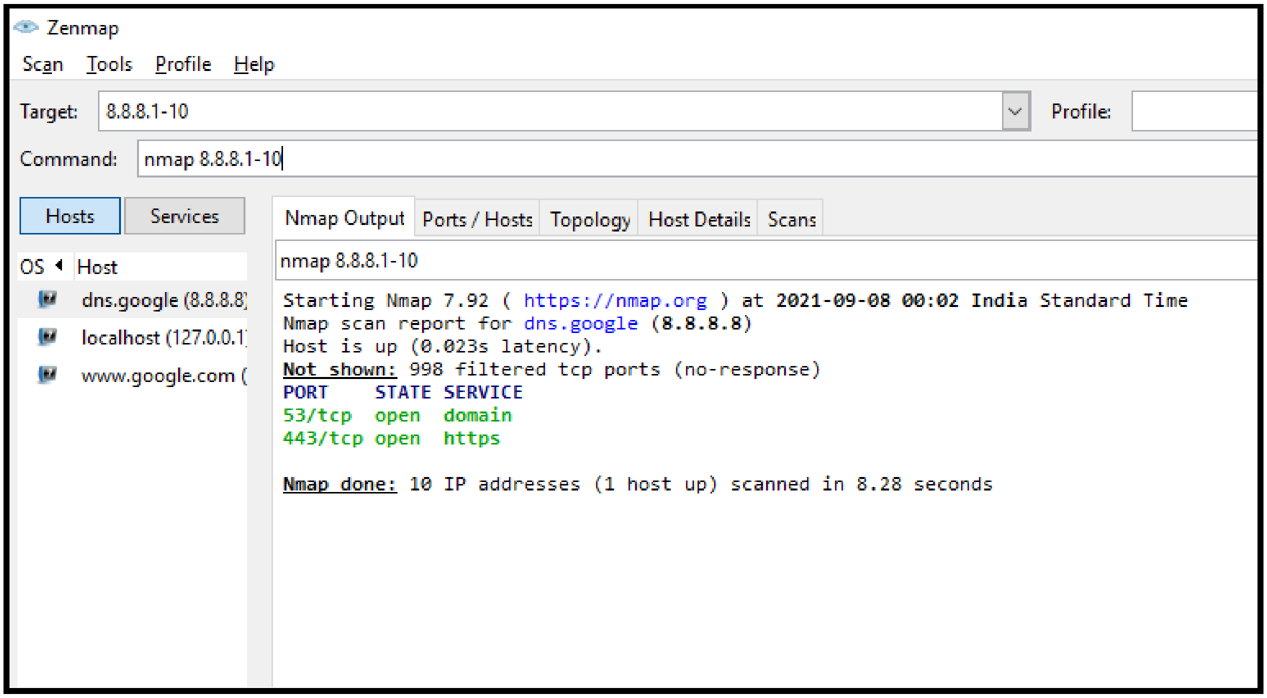


Target: 8.8.8.8

Command: nmap 8.8.8.8

```
nmap 8.8.8.8
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 00:01 India Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.028s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.58 seconds
```

4. Scanning multiple IP addresses:

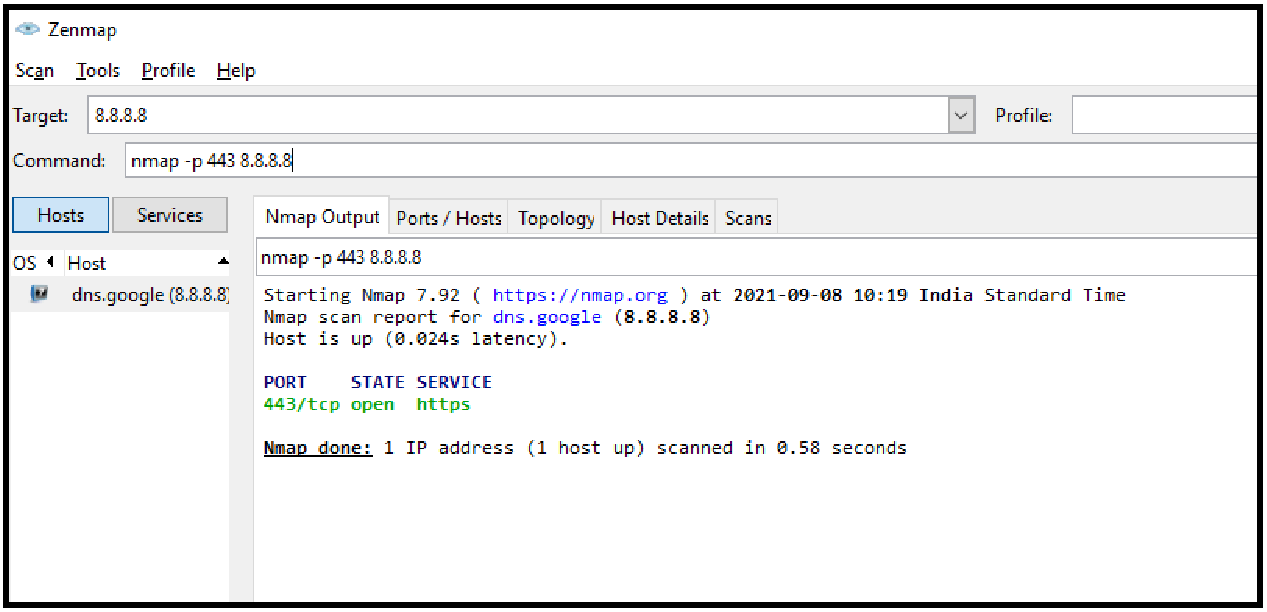


Target: 8.8.8.1-10

Command: nmap 8.8.8.1-10

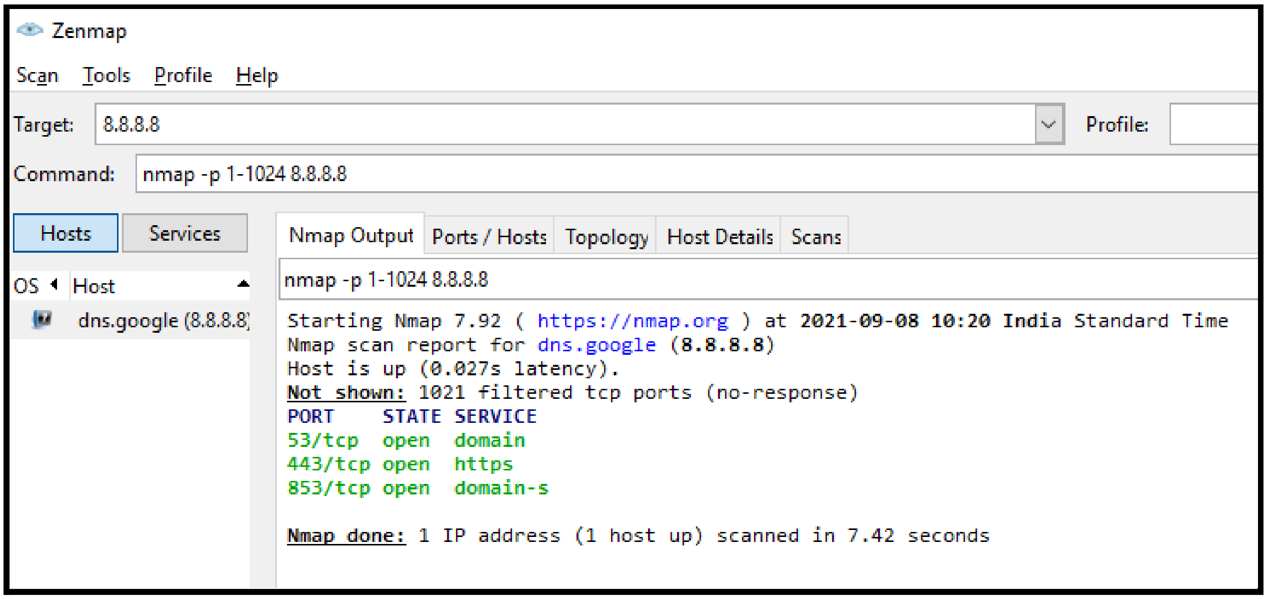
```
nmap 8.8.8.1-10
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 00:02 India Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.023s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 10 IP addresses (1 host up) scanned in 8.28 seconds
```

5. Scanning specific port 443 on a remote server



```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 10:19 India Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.024s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

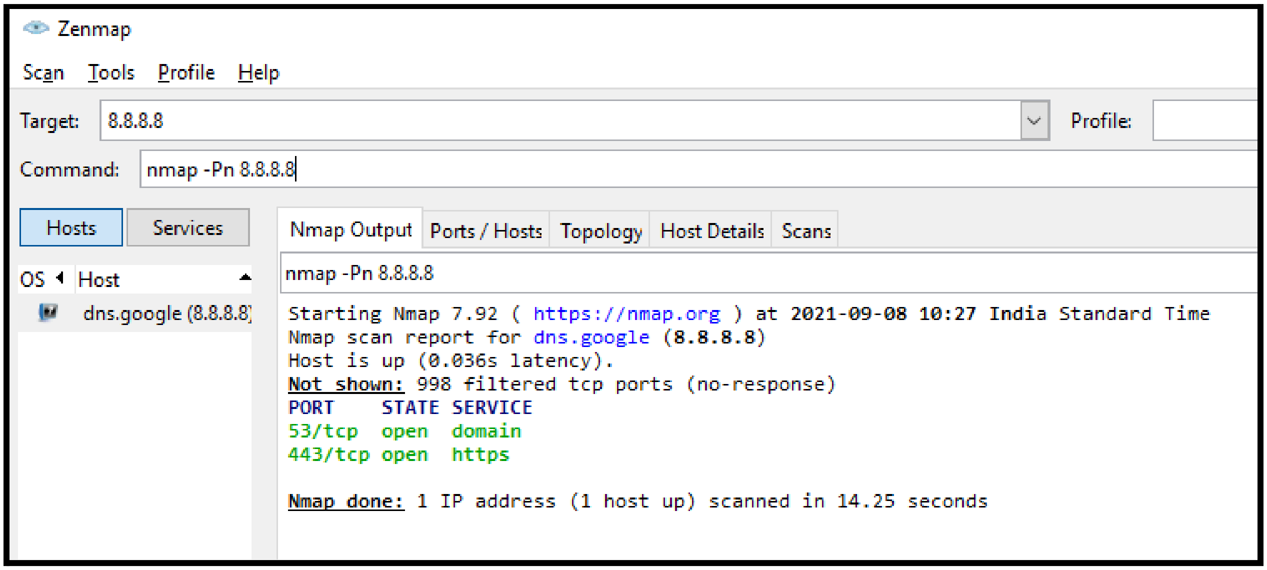
6. Scanning range of ports on a remote server (1-1024 on server 8.8.8.8)



```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 10:20 India Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.027s latency).
Not shown: 1021 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https
853/tcp open  domain-s

Nmap done: 1 IP address (1 host up) scanned in 7.42 seconds
```

Response: 1021 filtered ports (couldnt be scanned by nmap) and 3 open ports.

7. Skipping host Discovery (Scanning all hosts)

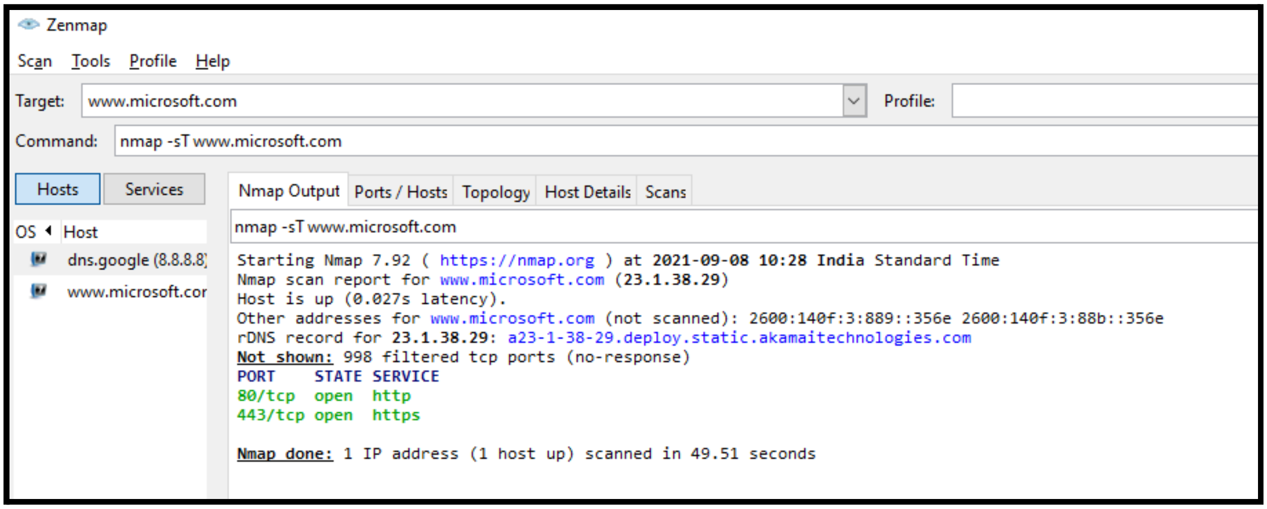


Target: 8.8.8.8

Command: nmap -Pn 8.8.8.8

```
nmap -Pn 8.8.8.8

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 10:27 India Standard Time
Nmap scan report for dns.google (8.8.8.8)
Host is up (0.036s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
53/tcp  open  domain
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 14.25 seconds
```

8. TCP connect scan on microsoft.com

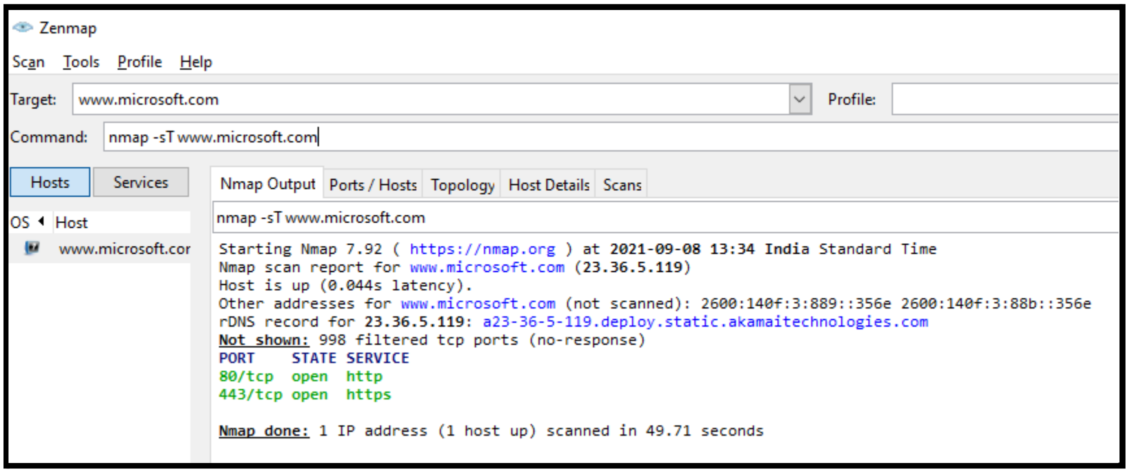


Target: www.microsoft.com

Command: nmap -sT www.microsoft.com

```
nmap -sT www.microsoft.com

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 10:28 India Standard Time
Nmap scan report for www.microsoft.com (23.1.38.29)
Host is up (0.027s latency).
Other addresses for www.microsoft.com (not scanned): 2600:140f:3:889::356e 2600:140f:3:88b::356e
rDNS record for 23.1.38.29: a23-1-38-29.deploy.static.akamaitechnologies.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 49.51 seconds
```

9. TCP SYN/Connect

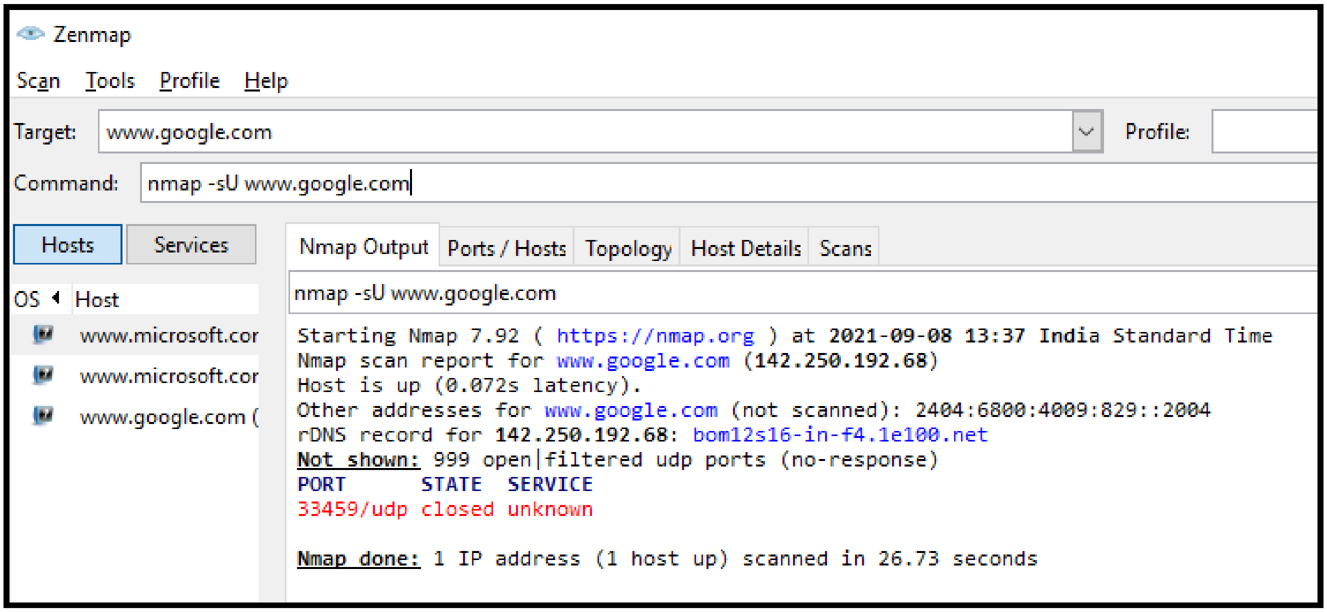


Target: www.microsoft.com

Command: nmap -sT www.microsoft.com

```
nmap -sT www.microsoft.com

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 13:34 India Standard Time
Nmap scan report for www.microsoft.com (23.36.5.119)
Host is up (0.044s latency).
Other addresses for www.microsoft.com (not scanned): 2600:140f:3:889::356e 2600:140f:3:88b::356e
rDNS record for 23.36.5.119: a23-36-5-119.deploy.static.akamaitechnologies.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 49.71 seconds
```

10. UDP Scan



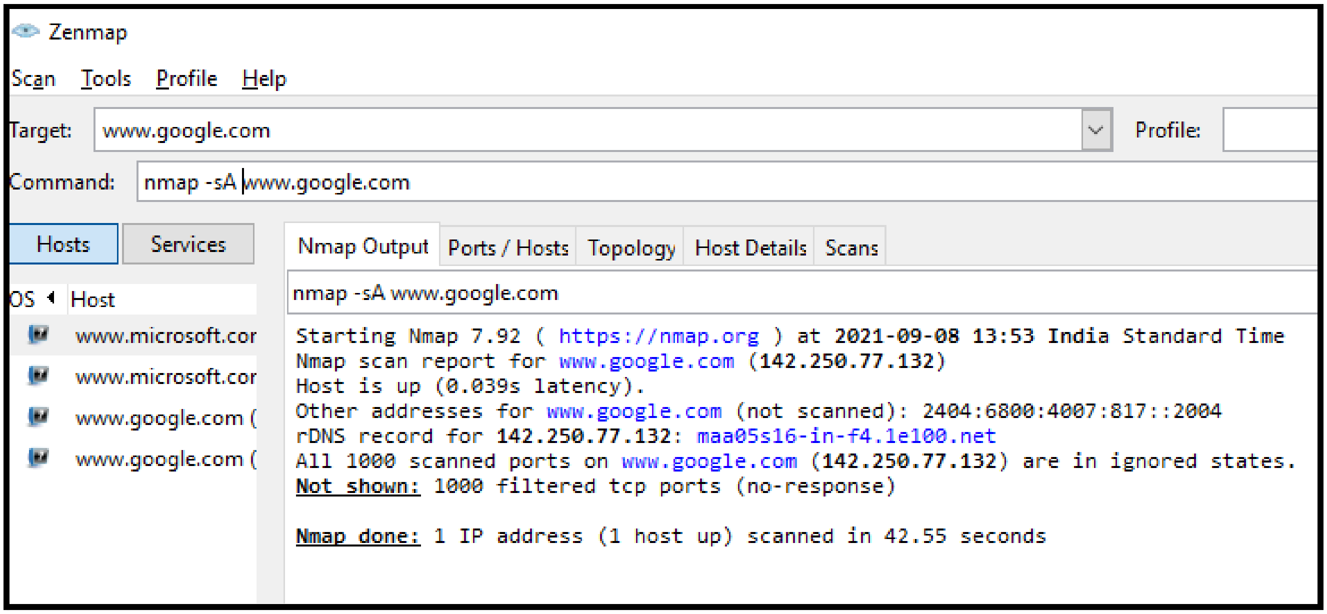
Target: www.google.com

Command: nmap -sU www.google.com

```
nmap -sU www.google.com

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 13:37 India Standard Time
Nmap scan report for www.google.com (142.250.192.68)
Host is up (0.072s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:829::2004
rDNS record for 142.250.192.68: bom12s16-in-f4.1e100.net
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
33459/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 26.73 seconds
```

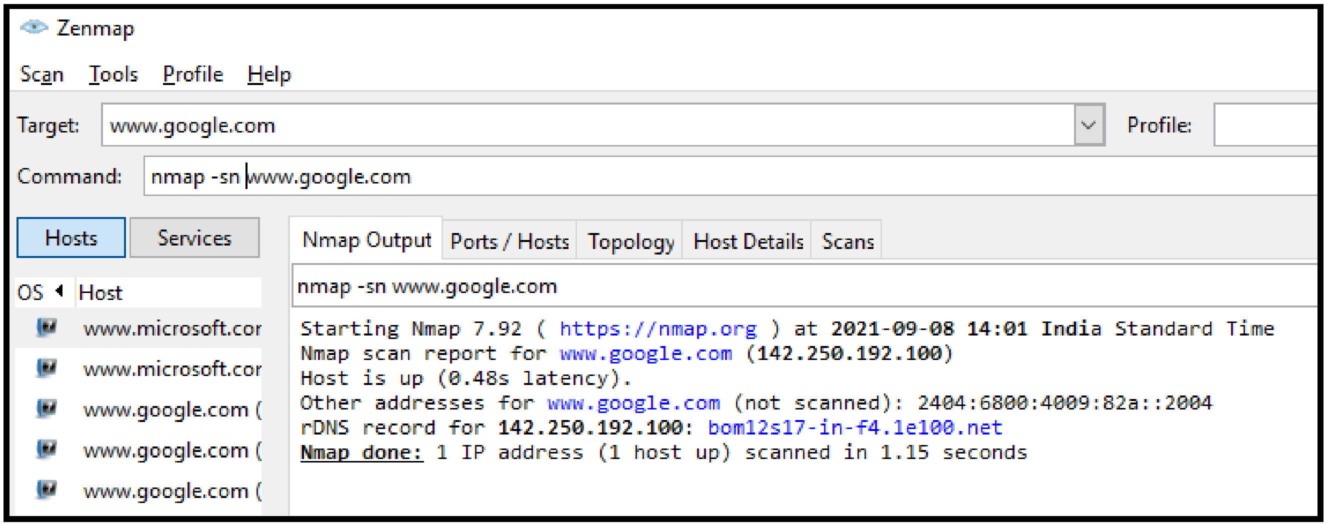
Open| filtered shows nmap is not able to decide which of the stwo states describe the ports.

11. TCP ACK port scan



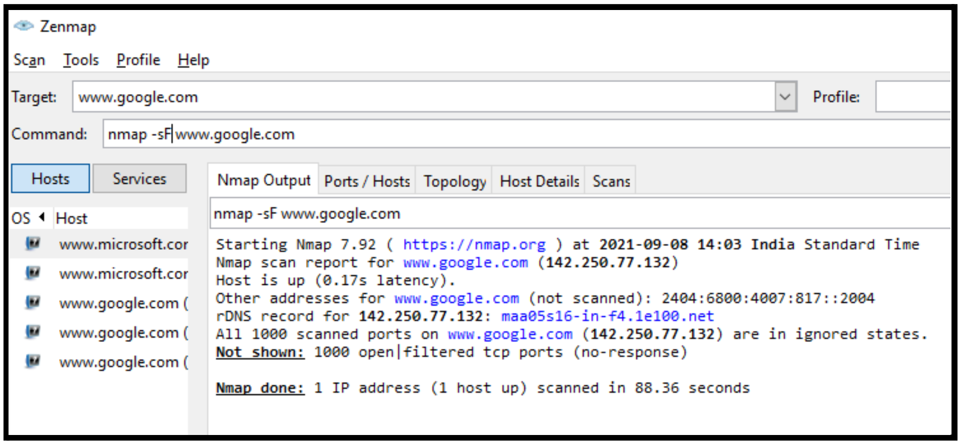
```
nmap -sA www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 13:53 India Standard Time
Nmap scan report for www.google.com (142.250.77.132)
Host is up (0.039s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4007:817::2004
rDNS record for 142.250.77.132: maa05s16-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.77.132) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 42.55 seconds
```

12. Disable port scanning, host discovery only



```
nmap -sn www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 14:01 India Standard Time
Nmap scan report for www.google.com (142.250.192.100)
Host is up (0.48s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:82a::2004
rDNS record for 142.250.192.100: bom12s17-in-f4.1e100.net
Nmap done: 1 IP address (1 host up) scanned in 1.15 seconds
```

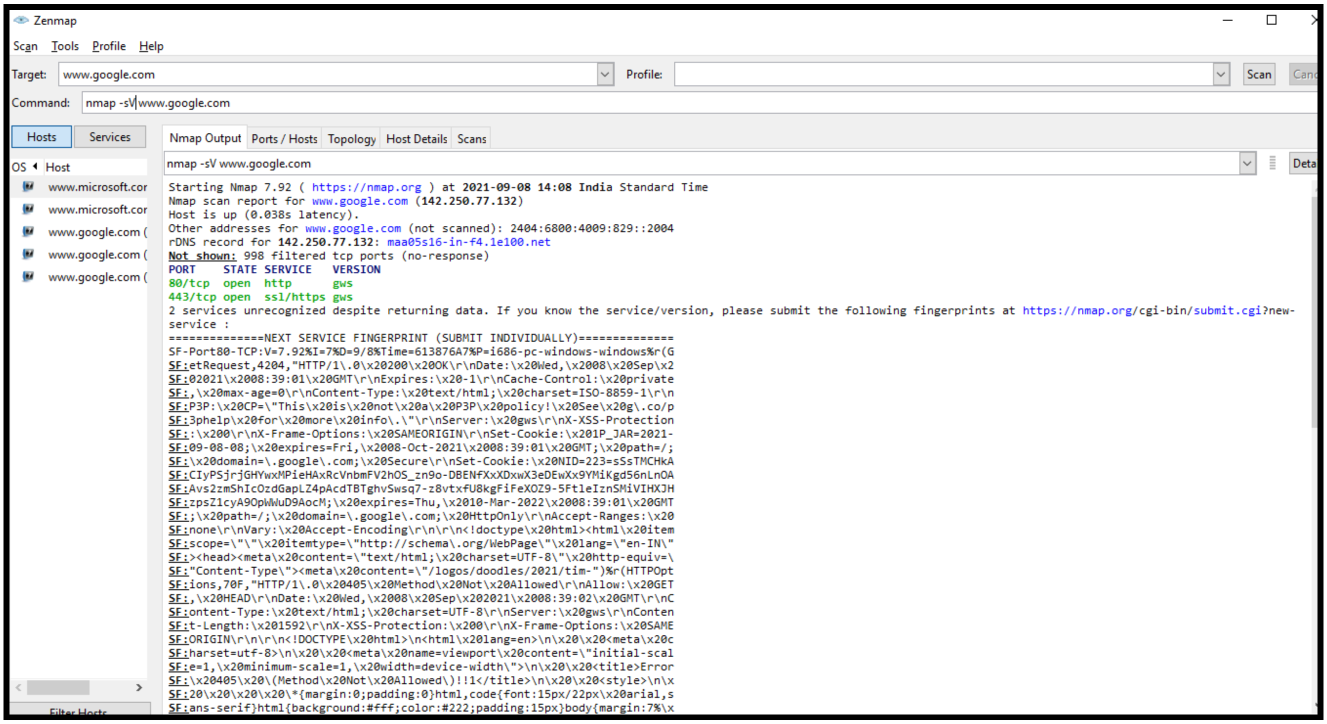
13. TCP FIN scan



Command: nmap -sF www.google.com

```
nmap -sF www.google.com

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 14:03 India Standard Time
Nmap scan report for www.google.com (142.250.77.132)
Host is up (0.17s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4007:817::2004
rDNS record for 142.250.77.132: maa05s16-in-f4.1e100.net
All 1000 scanned ports on www.google.com (142.250.77.132) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 88.36 seconds
```

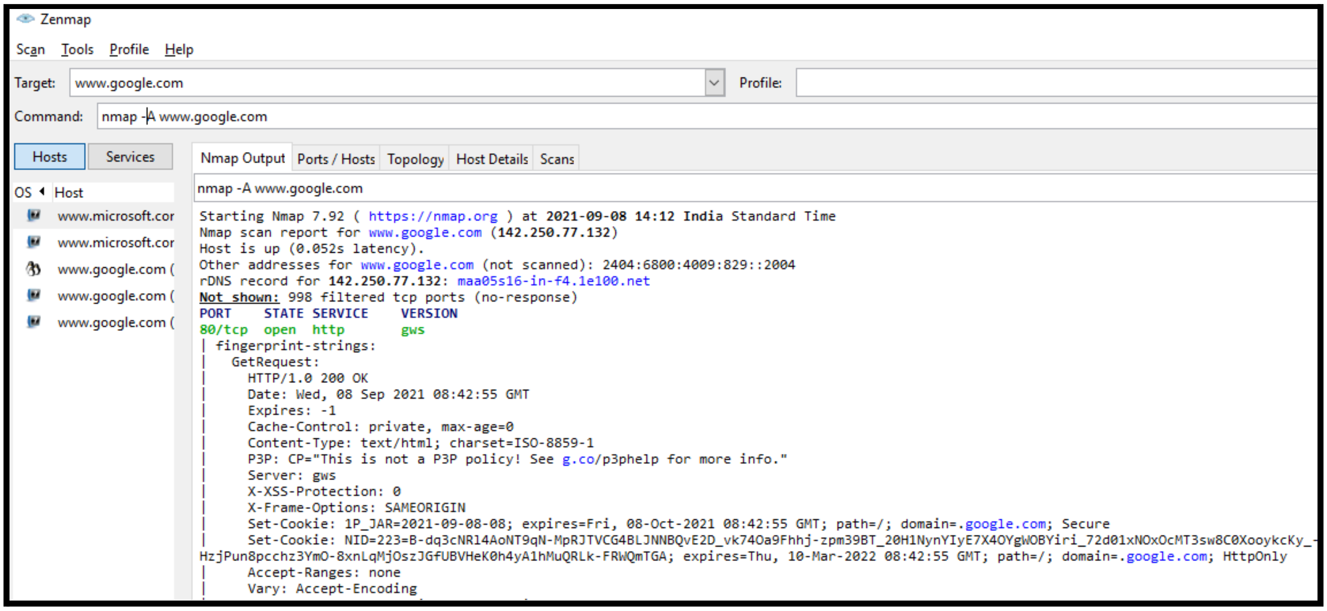
14. Determining Service/Version information:



Command: nmap -sV www.google.com

```
nmap -sV www.google.com

Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 14:08 India Standard Time
Nmap scan report for www.google.com (142.250.77.132)
Host is up (0.038s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:829::2004
rDNS record for 142.250.77.132: maa05s16-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      gws
443/tcp open  ssl/https gws
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-
service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.92%I=7%D=9/8%Time=613876A7%P=i686-pc-windows-windows%r(G
SF:etRequest,4204,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Wed,\x2008\x20Sep\x2
SF:02021\x2008:39:01\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20private
SF:,\x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\n
SF:P3P:\x20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p
SF:3phelp\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection
SF::\x200\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x201P_JAR=2021-
SF:09-08-08;\x20expires=Fri,\x2008-Oct-2021\x2008:39:01\x20GMT;\x20path=/;
SF:\x20domain=\.google\.com;\x20Secure\r\nSet-Cookie:\x20NID=223=sSsTMCHkA
SF:CIyPSjrjGHYwxMPieHAxRcVnbmFV2hOS_zn9o-DBENfXxXDxwX3eDEwXx9YMiKgd56nLnOA
SF:Avs2zmShIcOzdGapLZ4pAcdTBTghvSwsq7-z8vtxfU8kgFiFeXOZ9-5FtleIznSMiVIHXJH
SF:zpsZ1cyA9OpWWuD9AocM;\x20expires=Thu,\x2010-Mar-2022\x2008:39:01\x20GMT
SF:;\x20path=/;\x20domain=\.google\.com;\x20HttpOnly\r\nAccept-Ranges:\x20
SF:none\r\nVary:\x20Accept-Encoding\r\n\r\n<!doctype\x20html><html\x20item
SF:scope=\"\"\x20itemtype=\"http://schema\.org/WebPage\"\x20lang=\"en-IN\"
SF:><head><meta\x20content=\"text/html;\x20charset=UTF-8\"\x20http-equiv=\
SF:"Content-Type\"><meta\x20content=\"/logos/doodles/2021/tim-")%r(HTTPOpt
SF:ions,70F,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\nAllow:\x20GET
SF:,\x20HEAD\r\nDate:\x20Wed,\x2008\x20Sep\x202021\x2008:39:02\x20GMT\r\nC
SF:ontent-Type:\x20text/html;\x20charset=UTF-8\r\nServer:\x20gws\r\nConten
SF:t-Length:\x201592\r\nX-XSS-Protection:\x200\r\nX-Frame-Options:\x20SAME
SF:ORIGIN\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=en>\n\x20\x20<meta\x20c
SF:harset=utf-8>\n\x20\x20<meta\x20name=viewport\x20content=\"initial-scal
SF:e=1,\x20minimum-scale=1,\x20width=device-width\">\n\x20\x20<title>Error
SF:\x20405\x20\(Method\x20Not\x20Allowed\)!!1</title>\n\x20\x20<style>\n\x
SF:20\x20\x20\x20\*{margin:0;padding:0}html,code{font:15px/22px\x20arial,s
SF:ans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7%\x
```

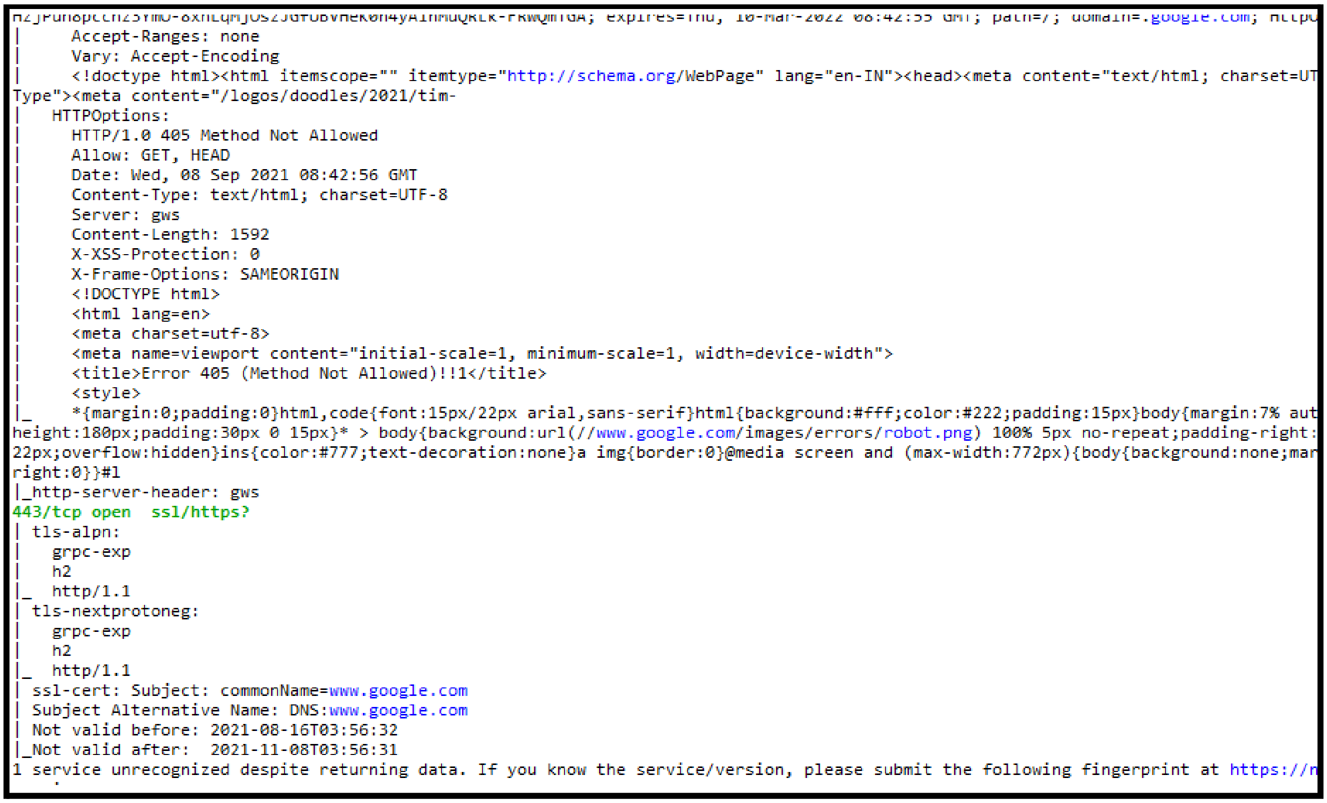
15. OS detection, version detection, script scanning and traceroute:



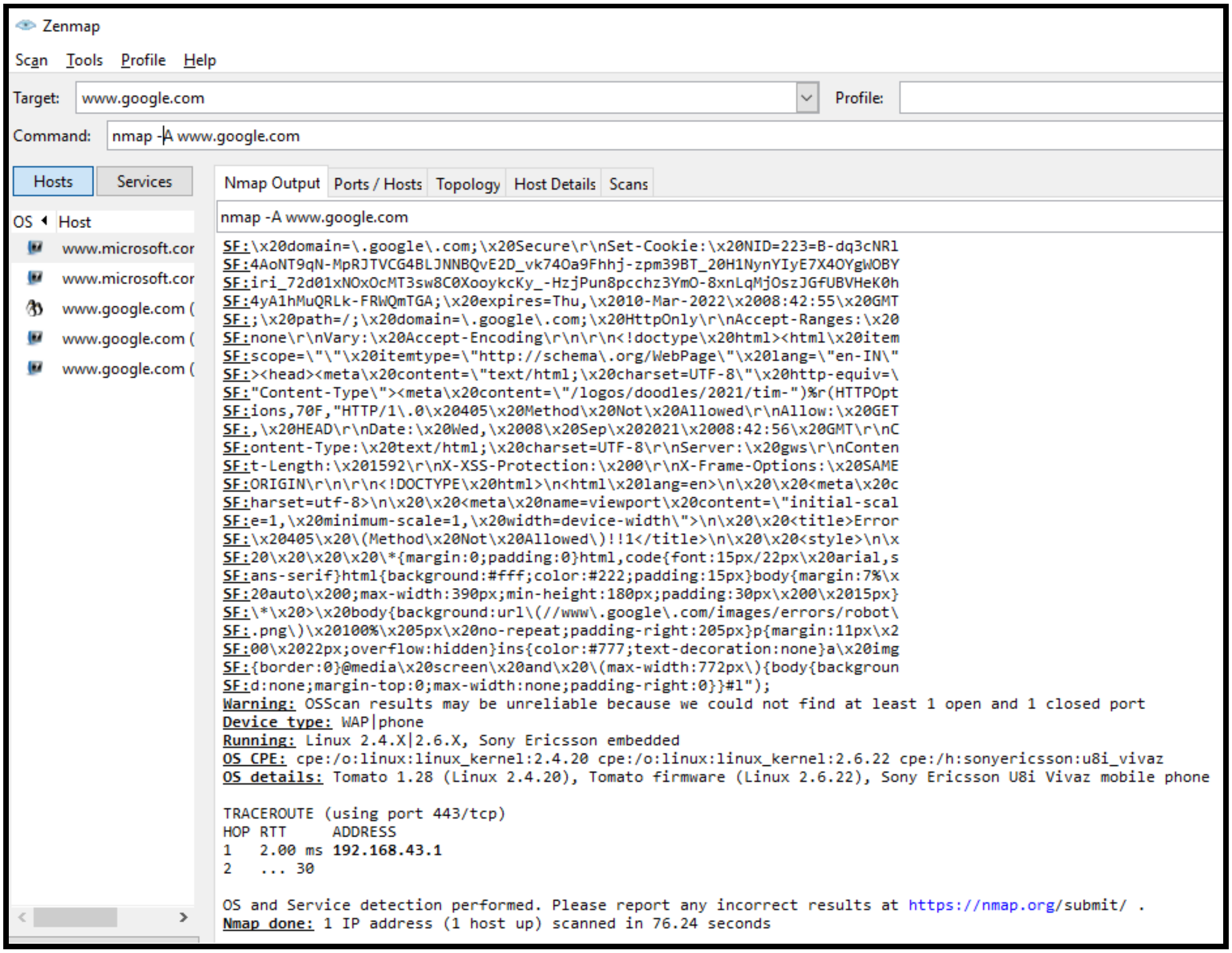
Target: www.google.com

Command: nmap -A www.google.com

```
nmap -A www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-08 14:12 India Standard Time
Nmap scan report for www.google.com (142.250.77.132)
Host is up (0.052s latency).
Other addresses for www.google.com (not scanned): 2404:6800:4009:829::2004
rDNS record for 142.250.77.132: maa05s16-in-f4.1e100.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  http       gws
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 200 OK
|     Date: Wed, 08 Sep 2021 08:42:55 GMT
|     Expires: -1
|     Cache-Control: private, max-age=0
|     Content-Type: text/html; charset=ISO-8859-1
|     P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
|     Server: gws
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     Set-Cookie: 1P_JAR=2021-09-08-08; expires=Fri, 08-Oct-2021 08:42:55 GMT; path=/; domain=.google.com; Secure
|     Set-Cookie: NID=223=B-dq3cNR14AoNT9qN-MpRJTVCG4BLJNNBQvE2D_vk74Oa9Fhhj-zpm39BT_20H1NynYIyE7X4OYgWOBYiri_72d01xNOxOcMT3sw8C0XooykcKy_-
HzjPun8pcchz3YmO-8xnLqMjOszJGfUBVHeK0h4yA1hMuQRLk-FRWQmTGA; expires=Thu, 10-Mar-2022 08:42:55 GMT; path=/; domain=.google.com; HttpOnly
|     Accept-Ranges: none
|     Vary: Accept-Encoding
```



```
HzjPun8pcchz3YmO-8xnLqMjOszJGfUBVHeK0h4yA1hMuQRLk-FRWQmTGA; expires=Thu, 10-Mar-2022 08:42:55 GMT; path=/; domain=.google.com; HttpO
|     Accept-Ranges: none
|     Vary: Accept-Encoding
|     <!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-IN"><head><meta content="text/html; charset=UT
Type"><meta content="/logos/doodles/2021/tim-
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: GET, HEAD
|     Date: Wed, 08 Sep 2021 08:42:56 GMT
|     Content-Type: text/html; charset=UTF-8
|     Server: gws
|     Content-Length: 1592
|     X-XSS-Protection: 0
|     X-Frame-Options: SAMEORIGIN
|     <!DOCTYPE html>
|     <html lang=en>
|     <meta charset=utf-8>
|     <meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
|     <title>Error 405 (Method Not Allowed)!!1</title>
|     <style>
|_    *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% aut
height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:
22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;mar
right:0}}#1
|_http-server-header: gws
443/tcp open  ssl/https?
| tls-alpn:
|   grpc-exp
|   h2
|_  http/1.1
| tls-nextprotoneg:
|   grpc-exp
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=www.google.com
| Subject Alternative Name: DNS:www.google.com
| Not valid before: 2021-08-16T03:56:32
|_Not valid after:  2021-11-08T03:56:31
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://n
```



Target: www.google.com

Profile:

Command: nmap -A www.google.com

OS Host
www.microsoft.cor
www.microsoft.cor
www.google.com (
www.google.com (
www.google.com (

```
nmap -A www.google.com
SF:\x20domain=\.google\.com;\x20Secure\r\nSet-Cookie:\x20NID=223=B-dq3cNRl
SF:4AoNT9qN-MpRJTVCG4BLJNNBQvE2D_vk74Oa9Fhhj-zpm39BT_20H1NynYIyE7X4OYgWOBY
SF:iri_72d01xNOxOcMT3sw8C0XooykcKy_-HzjPun8pcchz3YmO-8xnLqMjOszJGfUBVHeK0h
SF:4yA1hMuQRLk-FRWQmTGA;\x20expires=Thu,\x2010-Mar-2022\x2008:42:55\x20GMT
SF:;\x20path=/;\x20domain=\.google\.com;\x20HttpOnly\r\nAccept-Ranges:\x20
SF:none\r\nVary:\x20Accept-Encoding\r\n\r\n<!doctype\x20html><html\x20item
SF:scope=\"\"\x20itemtype=\"http://schema\.org/WebPage\"\x20lang=\"en-IN\"
SF:><head><meta\x20content=\"text/html;\x20charset=UTF-8\"\x20http-equiv=\
SF:"Content-Type\"><meta\x20content=\"/logos/doodles/2021/tim-")%r(HTTPOpt
SF:ions,70F,"HTTP/1\.0\x20405\x20Method\x20Not\x20Allowed\r\nAllow:\x20GET
SF:,\x20HEAD\r\nDate:\x20Wed,\x2008\x20Sep\x202021\x2008:42:56\x20GMT\r\nC
SF:ontent-Type:\x20text/html;\x20charset=UTF-8\r\nServer:\x20gws\r\nConten
SF:t-Length:\x201592\r\nX-XSS-Protection:\x200\r\nX-Frame-Options:\x20SAME
SF:ORIGIN\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=en>\n\x20\x20<meta\x20c
SF:harset=utf-8>\n\x20\x20<meta\x20name=viewport\x20content=\"initial-scal
SF:e=1,\x20minimum-scale=1,\x20width=device-width\">\n\x20\x20<title>Error
SF:\x20405\x20\(Method\x20Not\x20Allowed\)!!1</title>\n\x20\x20<style>\n\x
SF:20\x20\x20\x20\*{margin:0;padding:0}html,code{font:15px/22px\x20arial,s
SF:ans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7%\x
SF:20auto\x200;max-width:390px;min-height:180px;padding:30px\x200\x2015px}
SF:\*\x20>\x20body{background:url\(//www\.google\.com/images/errors/robot\
SF:.png\)\x20100%\x205px\x20no-repeat;padding-right:205px}p{margin:11px\x2
SF:00\x2022px;overflow:hidden}ins{color:#777;text-decoration:none}a\x20img
SF:{border:0}@media\x20screen\x20and\x20\(max-width:772px\){body{backgroun
SF:d:none;margin-top:0;max-width:none;padding-right:0}}#1");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 443/tcp)
HOP RTT     ADDRESS
1   2.00 ms 192.168.43.1
2   ... 30

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.24 seconds
```

=========================END OF FILE======================================