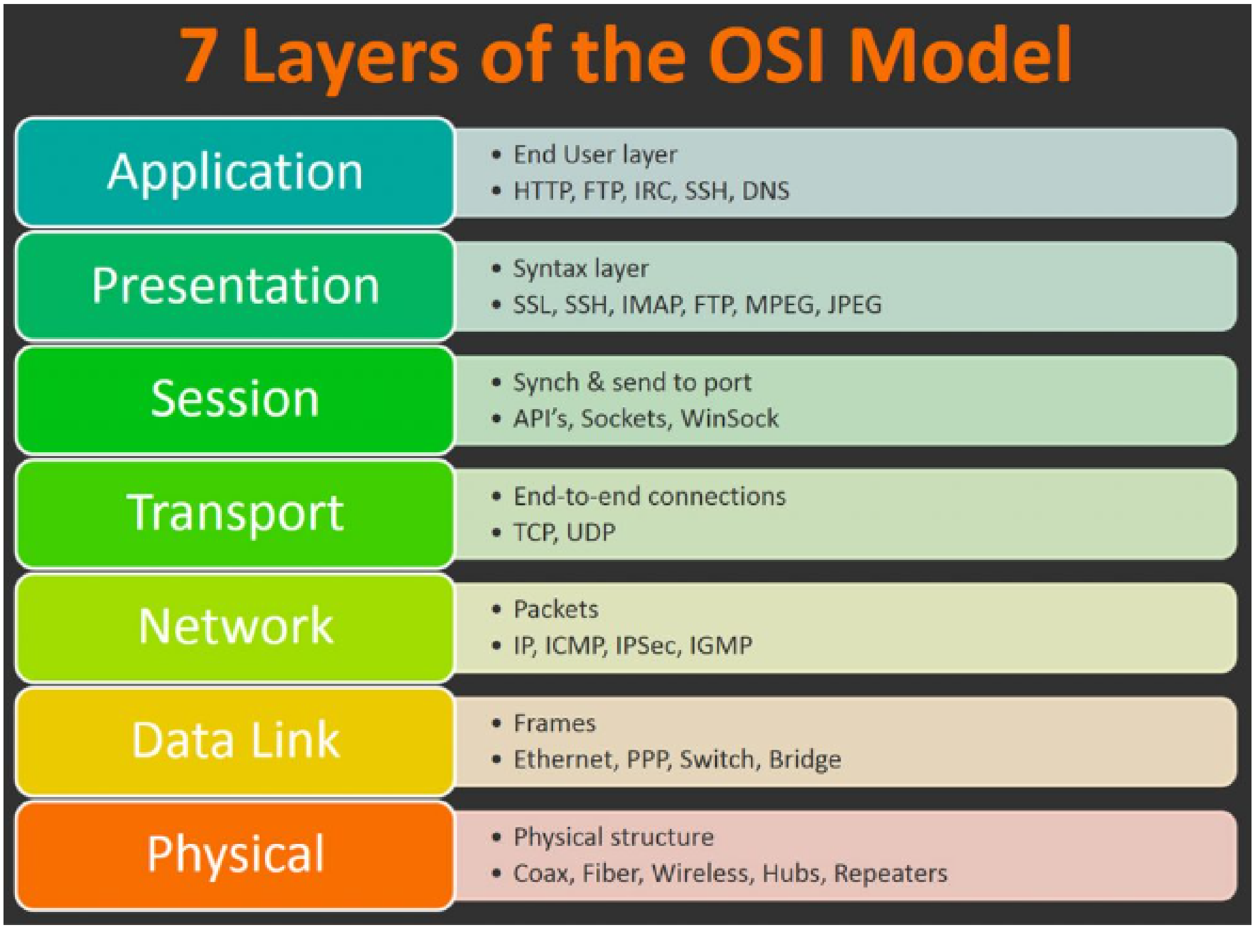
Wireshark

wireshark: wireshark is a network analyzing tool that is used for analysis of packet capture file or .pcap extension log file.

Download wireshark : Wireshark

Packet : Packets consist of two portions: **the header and the payload**. The header contains information about the packet, such as its origin and destination IP addresses (an IP address is like a computer's mailing address). The payload is the actual data.

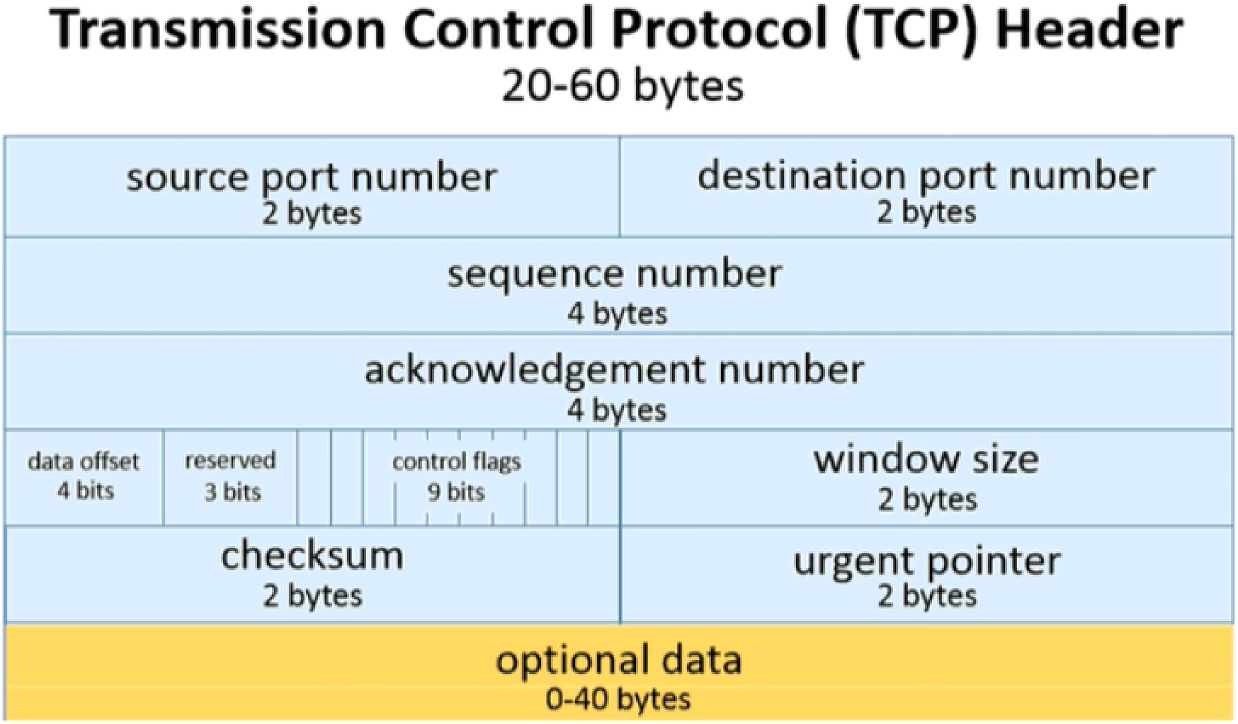
OSI 7 Layers



7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Example : TCP



Transmission Control Protocol (TCP) Header

20-60 bytes

source port number 2 bytes | destination port number 2 bytes

sequence number 4 bytes

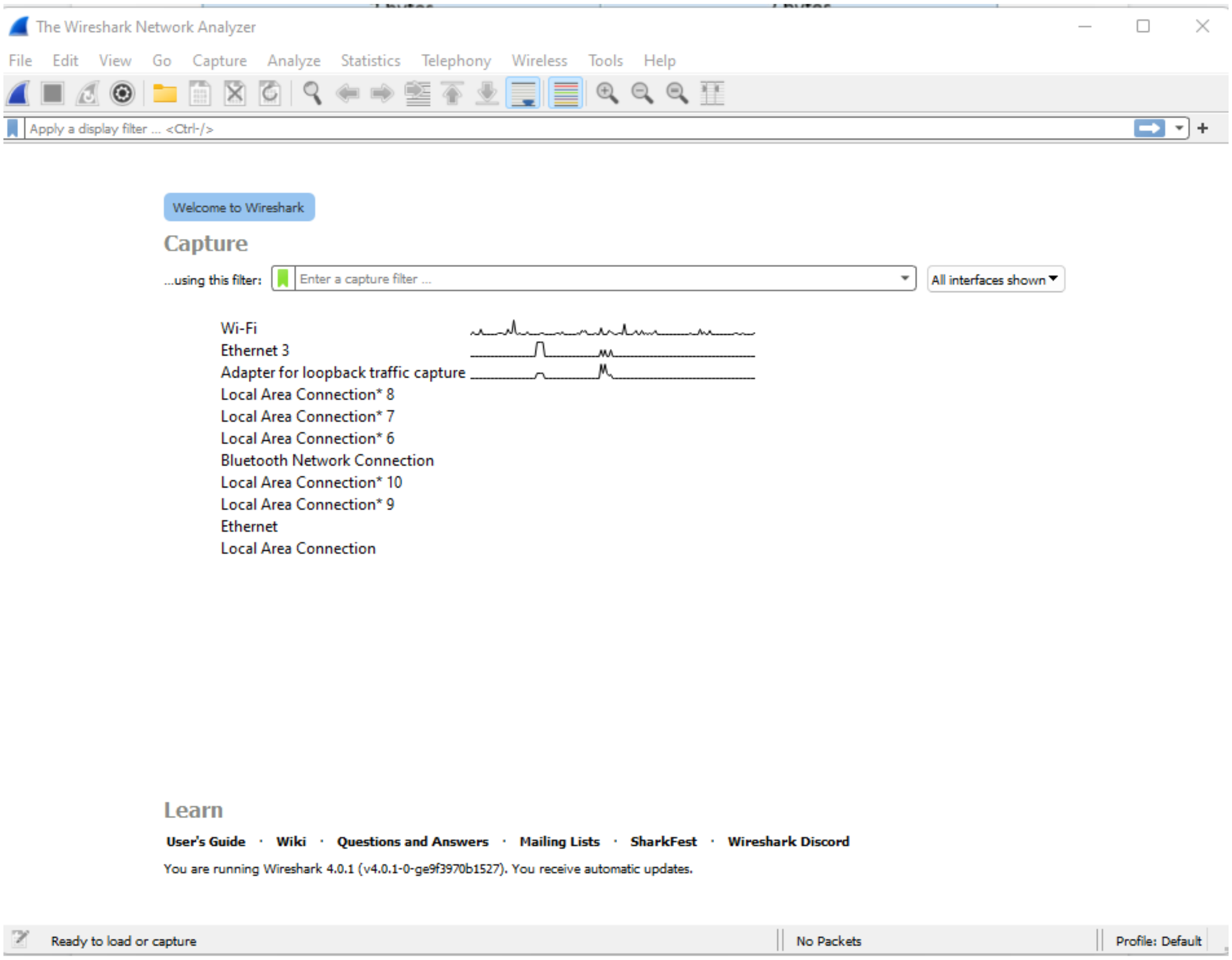
acknowledgement number 4 bytes

data offset 4 bits | reserved 3 bits | control flags 9 bits | window size 2 bytes

checksum 2 bytes | urgent pointer 2 bytes

optional data 0-40 bytes

Step 1 : After running wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
All interfaces shown
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord

Capture

...using this filter: Enter a capture filter ...

Wi-Fi
Ethernet 3
Adapter for loopback traffic capture
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 6
Bluetooth Network Connection
Local Area Connection* 10
Local Area Connection* 9
Ethernet
Local Area Connection

Learn

You are running Wireshark 4.0.1 (v4.0.1-0-ge9f3970b1527). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

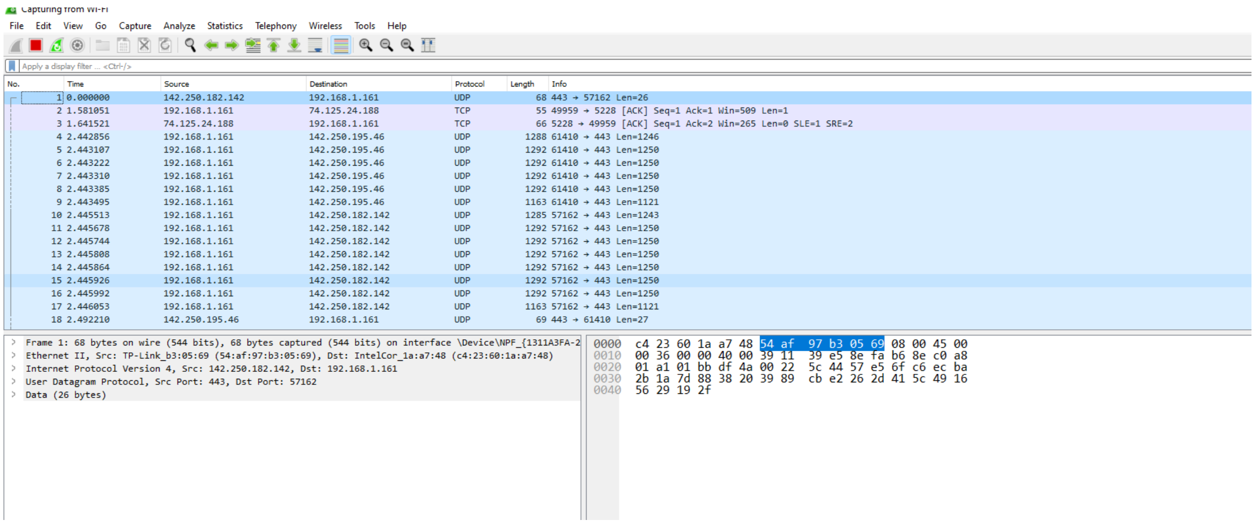
We are finding 3 default packets.

Step 2 : Check that wifi default packet .

- Click on wifi

Wi-Fi

- Check that all packets are running


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

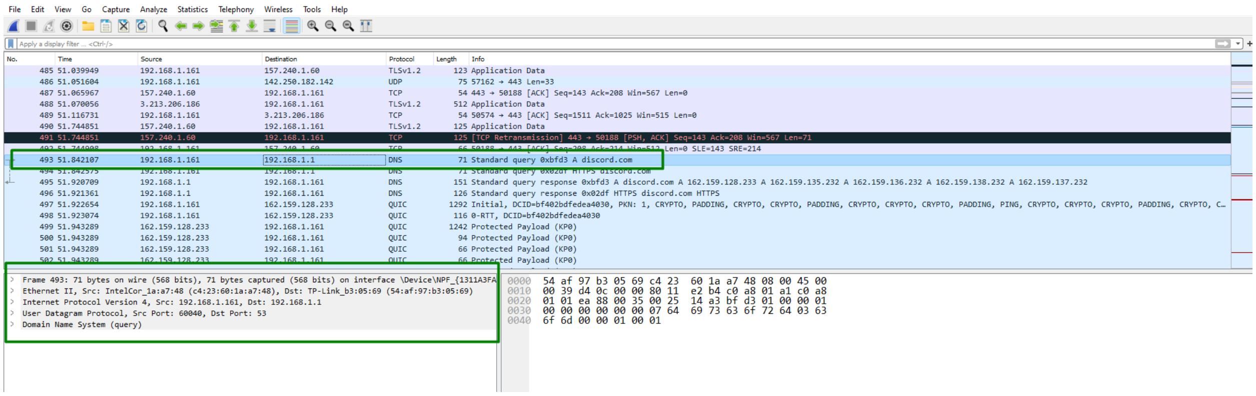
```
No.   Time       Source            Destination       Protocol  Length Info
    1 0.000000   142.250.182.142   192.168.1.161     UDP           68 443 → 57162 Len=26
    2 1.581051   192.168.1.161     74.125.24.188     TCP           55 49959 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
    3 1.641521   74.125.24.188     192.168.1.161     TCP           66 5228 → 49959 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
    4 2.442856   192.168.1.161     142.250.195.46    UDP         1288 61410 → 443 Len=1246
    5 2.443107   192.168.1.161     142.250.195.46    UDP         1292 61410 → 443 Len=1250
    6 2.443222   192.168.1.161     142.250.195.46    UDP         1292 61410 → 443 Len=1250
    7 2.443310   192.168.1.161     142.250.195.46    UDP         1292 61410 → 443 Len=1250
    8 2.443385   192.168.1.161     142.250.195.46    UDP         1292 61410 → 443 Len=1250
    9 2.443495   192.168.1.161     142.250.195.46    UDP         1163 61410 → 443 Len=1121
   10 2.445513   192.168.1.161     142.250.182.142   UDP         1285 57162 → 443 Len=1243
   11 2.445678   192.168.1.161     142.250.182.142   UDP         1292 57162 → 443 Len=1250
   12 2.445744   192.168.1.161     142.250.182.142   UDP         1292 57162 → 443 Len=1250
   13 2.445808   192.168.1.161     142.250.182.142   UDP         1292 57162 → 443 Len=1250
   14 2.445864   192.168.1.161     142.250.182.142   UDP         1292 57162 → 443 Len=1250
   15 2.445926   192.168.1.161     142.250.182.142   UDP         1292 57162 → 443 Len=1250
   16 2.445992   192.168.1.161     142.250.182.142   UDP         1292 57162 → 443 Len=1250
   17 2.446053   192.168.1.161     142.250.182.142   UDP         1163 57162 → 443 Len=1121
   18 2.492210   142.250.195.46    192.168.1.161     UDP           69 443 → 61410 Len=27
```

```
> Frame 1: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{1311A3FA-2
> Ethernet II, Src: TP-Link_b3:05:69 (54:af:97:b3:05:69), Dst: IntelCor_1a:a7:48 (c4:23:60:1a:a7:48)
> Internet Protocol Version 4, Src: 142.250.182.142, Dst: 192.168.1.161
> User Datagram Protocol, Src Port: 443, Dst Port: 57162
> Data (26 bytes)
```

```
0000  c4 23 60 1a a7 48 54 af  97 b3 05 69 08 00 45 00
0010  00 36 00 00 40 00 39 11  39 e5 8e fa b6 8e c0 a8
0020  01 a1 01 bb df 4a 00 22  5c 44 57 e5 6f c6 ec ba
0030  2b 1a 7d 88 38 20 39 89  cb e2 26 2d 41 5c 49 16
0040  56 29 19 2f
```

We are finding No ,Time, Source, Destination ,protocol,Length,Info

- Click on Stop capturing packets
- Check that a protocol

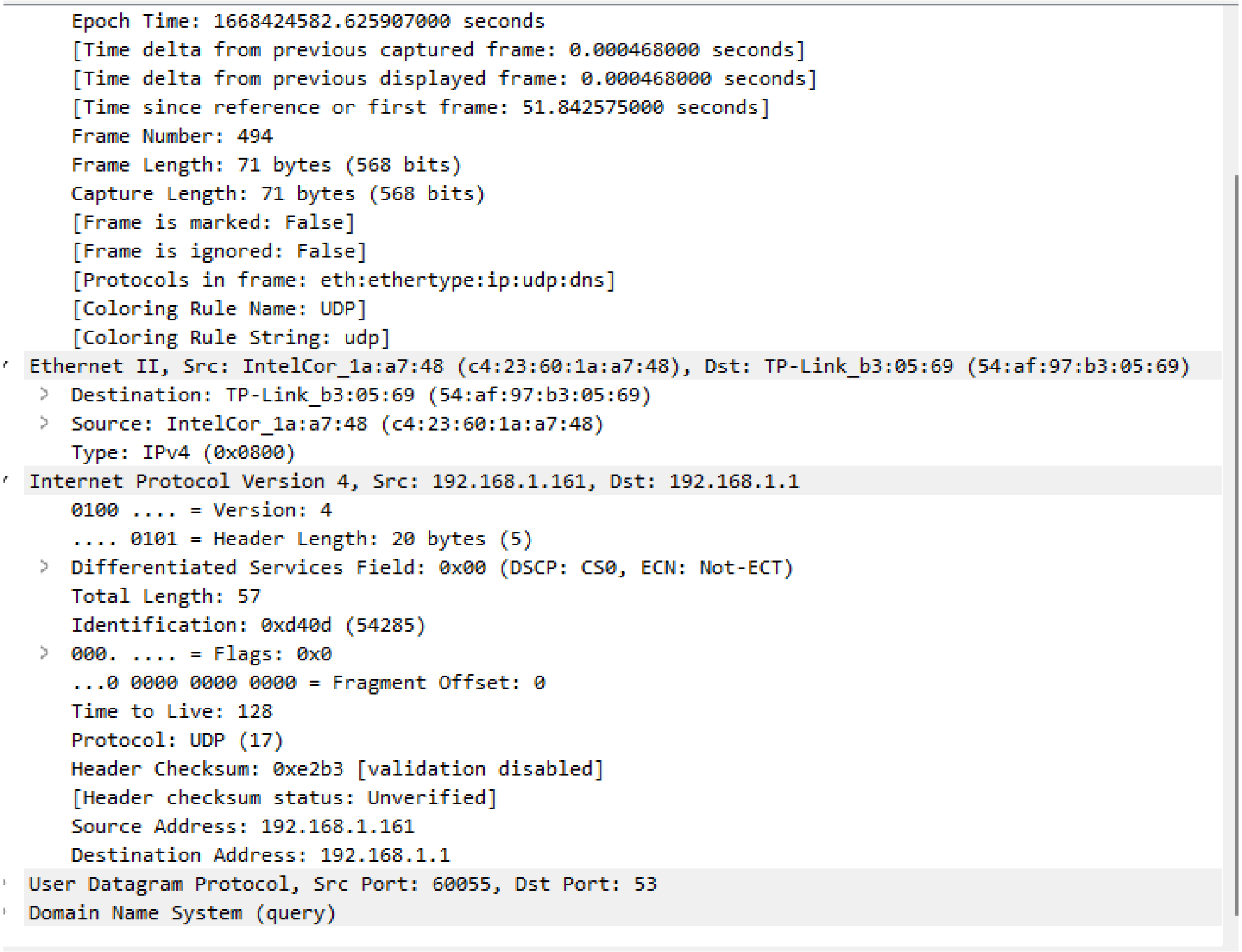

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time        Source            Destination       Protocol  Length Info
  485 51.039949   192.168.1.161     157.240.1.60      TLSv1.2      123 Application Data
  486 51.051604   192.168.1.161     142.250.182.142   UDP           75 57162 → 443 Len=33
  487 51.065967   157.240.1.60      192.168.1.161     TCP           54 443 → 50188 [ACK] Seq=143 Ack=208 Win=567 Len=0
  488 51.070056   3.213.206.186     192.168.1.161     TLSv1.2      512 Application Data
  489 51.116731   192.168.1.161     3.213.206.186     TCP           54 50574 → 443 [ACK] Seq=1511 Ack=1025 Win=515 Len=0
  490 51.744851   157.240.1.60      192.168.1.161     TLSv1.2      125 Application Data
  491 51.744851   157.240.1.60      192.168.1.161     TCP          125 [TCP Retransmission] 443 → 50188 [PSH, ACK] Seq=143 Ack=208 Win=567 Len=71
  492 51.744908   192.168.1.161     157.240.1.60      TCP           66 50188 → 443 [ACK] Seq=208 Ack=214 Win=512 Len=0 SLE=143 SRE=214
  493 51.842107   192.168.1.161     192.168.1.1       DNS           71 Standard query 0xbfd3 A discord.com
  494 51.842575   192.168.1.161     192.168.1.1       DNS           71 Standard query 0x02df HTTPS discord.com
  495 51.920709   192.168.1.1       192.168.1.161     DNS          151 Standard query response 0xbfd3 A discord.com A 162.159.128.233 A 162.159.135.232 A 162.159.136.232 A 162.159.138.232 A 162.159.137.232
  496 51.921361   192.168.1.1       192.168.1.161     DNS          126 Standard query response 0x02df HTTPS discord.com HTTPS
  497 51.922654   192.168.1.161     162.159.128.233   QUIC        1292 Initial, DCID=bf402bdfedea4030, PKN: 1, CRYPTO, PADDING, CRYPTO, CRYPTO, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDING, PING, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, C…
  498 51.923074   192.168.1.161     162.159.128.233   QUIC         116 0-RTT, DCID=bf402bdfedea4030
  499 51.943289   162.159.128.233   192.168.1.161     QUIC        1242 Protected Payload (KP0)
  500 51.943289   162.159.128.233   192.168.1.161     QUIC          94 Protected Payload (KP0)
  501 51.943289   162.159.128.233   192.168.1.161     QUIC          66 Protected Payload (KP0)
  502 51.943289   162.159.128.233   192.168.1.161     QUIC          66 Protected Payload (KP0)
```

```
> Frame 493: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{1311A3FA
> Ethernet II, Src: IntelCor_1a:a7:48 (c4:23:60:1a:a7:48), Dst: TP-Link_b3:05:69 (54:af:97:b3:05:69)
> Internet Protocol Version 4, Src: 192.168.1.161, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 60040, Dst Port: 53
> Domain Name System (query)
```

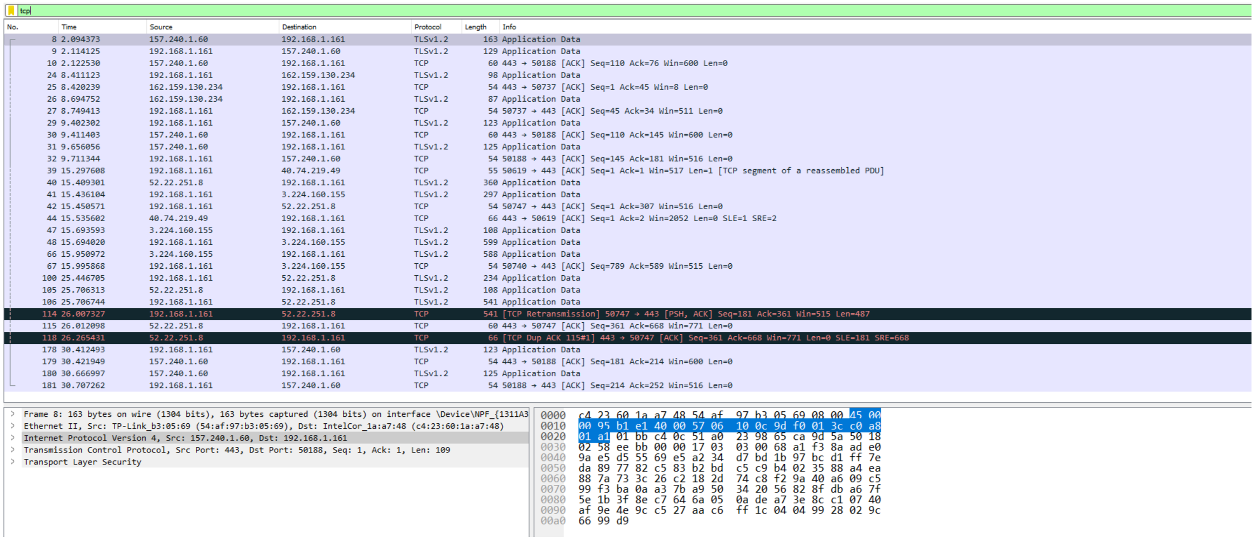
```
0000  54 af 97 b3 05 69 c4 23  60 1a a7 48 08 00 45 00
0010  00 39 d4 0c 00 00 80 11  e2 b4 c0 a8 01 a1 c0 a8
0020  01 01 ea 88 00 35 00 25  14 a3 bf d3 01 00 00 01
0030  00 00 00 00 00 00 07 64  69 73 63 6f 72 64 03 63
0040  6f 6d 00 00 01 00 01
```

- Check that protocol deatials (Frame,Ethernet,internet,user datagram protocol,src port, Domain name system)



```
      Epoch Time: 1668424582.625907000 seconds
      [Time delta from previous captured frame: 0.000468000 seconds]
      [Time delta from previous displayed frame: 0.000468000 seconds]
      [Time since reference or first frame: 51.842575000 seconds]
      Frame Number: 494
      Frame Length: 71 bytes (568 bits)
      Capture Length: 71 bytes (568 bits)
      [Frame is marked: False]
      [Frame is ignored: False]
      [Protocols in frame: eth:ethertype:ip:udp:dns]
      [Coloring Rule Name: UDP]
      [Coloring Rule String: udp]
  Ethernet II, Src: IntelCor_1a:a7:48 (c4:23:60:1a:a7:48), Dst: TP-Link_b3:05:69 (54:af:97:b3:05:69)
    > Destination: TP-Link_b3:05:69 (54:af:97:b3:05:69)
    > Source: IntelCor_1a:a7:48 (c4:23:60:1a:a7:48)
      Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.1.161, Dst: 192.168.1.1
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 57
      Identification: 0xd40d (54285)
    > 000. .... = Flags: 0x0
      ...0 0000 0000 0000 = Fragment Offset: 0
      Time to Live: 128
      Protocol: UDP (17)
      Header Checksum: 0xe2b3 [validation disabled]
      [Header checksum status: Unverified]
      Source Address: 192.168.1.161
      Destination Address: 192.168.1.1
  User Datagram Protocol, Src Port: 60055, Dst Port: 53
  Domain Name System (query)
```

Step 3 : Searching result — TCP



tcp

```
No.   Time       Source           Destination      Protocol  Length Info
    8 2.094373   157.240.1.60     192.168.1.161    TLSv1.2   163 Application Data
    9 2.114125   192.168.1.161    157.240.1.60     TLSv1.2   129 Application Data
   10 2.122530   157.240.1.60     192.168.1.161    TCP        60 443 → 50188 [ACK] Seq=110 Ack=76 Win=600 Len=0
   24 8.411123   192.168.1.161    162.159.130.234  TLSv1.2    98 Application Data
   25 8.420239   162.159.130.234  192.168.1.161    TCP        54 443 → 50737 [ACK] Seq=1 Ack=45 Win=8 Len=0
   26 8.694752   162.159.130.234  192.168.1.161    TLSv1.2    87 Application Data
   27 8.749413   192.168.1.161    162.159.130.234  TCP        54 50737 → 443 [ACK] Seq=45 Ack=34 Win=511 Len=0
   29 9.402302   192.168.1.161    157.240.1.60     TLSv1.2   123 Application Data
   30 9.411403   157.240.1.60     192.168.1.161    TCP        60 443 → 50188 [ACK] Seq=110 Ack=145 Win=600 Len=0
   31 9.656056   157.240.1.60     192.168.1.161    TLSv1.2   125 Application Data
   32 9.711344   192.168.1.161    157.240.1.60     TCP        54 50188 → 443 [ACK] Seq=145 Ack=181 Win=516 Len=0
   39 15.297608  192.168.1.161    40.74.219.49     TCP        55 50619 → 443 [ACK] Seq=1 Ack=1 Win=517 Len=1 [TCP segment of a reassembled PDU]
   40 15.409301  52.22.251.8      192.168.1.161    TLSv1.2   360 Application Data
   41 15.436104  192.168.1.161    3.224.160.155    TLSv1.2   297 Application Data
   42 15.450571  192.168.1.161    52.22.251.8      TCP        54 50747 → 443 [ACK] Seq=1 Ack=307 Win=516 Len=0
   44 15.535602  40.74.219.49     192.168.1.161    TCP        66 443 → 50619 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2
   47 15.693593  3.224.160.155    192.168.1.161    TLSv1.2   108 Application Data
   48 15.694020  192.168.1.161    3.224.160.155    TLSv1.2   599 Application Data
   66 15.950972  3.224.160.155    192.168.1.161    TLSv1.2   588 Application Data
   67 15.995868  192.168.1.161    3.224.160.155    TCP        54 50740 → 443 [ACK] Seq=789 Ack=589 Win=515 Len=0
  100 25.446705  192.168.1.161    52.22.251.8      TLSv1.2   234 Application Data
  105 25.706313  52.22.251.8      192.168.1.161    TLSv1.2   108 Application Data
  106 25.706744  192.168.1.161    52.22.251.8      TLSv1.2   541 Application Data
  114 26.007327  192.168.1.161    52.22.251.8      TCP       541 [TCP Retransmission] 50747 → 443 [PSH, ACK] Seq=181 Ack=361 Win=515 Len=487
  115 26.012098  52.22.251.8      192.168.1.161    TCP        60 443 → 50747 [ACK] Seq=361 Ack=668 Win=771 Len=0
  118 26.265431  52.22.251.8      192.168.1.161    TCP        66 [TCP Dup ACK 115#1] 443 → 50747 [ACK] Seq=361 Ack=668 Win=771 Len=0 SLE=181 SRE=668
  178 30.412493  192.168.1.161    157.240.1.60     TLSv1.2   123 Application Data
  179 30.421949  157.240.1.60     192.168.1.161    TCP        54 443 → 50188 [ACK] Seq=181 Ack=214 Win=600 Len=0
  180 30.666997  157.240.1.60     192.168.1.161    TLSv1.2   125 Application Data
  181 30.707262  192.168.1.161    157.240.1.60     TCP        54 50188 → 443 [ACK] Seq=214 Ack=252 Win=516 Len=0
```

```
> Frame 8: 163 bytes on wire (1304 bits), 163 bytes captured (1304 bits) on interface \Device\NPF_{1311A3
> Ethernet II, Src: TP-Link_b3:05:69 (54:af:97:b3:05:69), Dst: IntelCor_1a:a7:48 (c4:23:60:1a:a7:48)
> Internet Protocol Version 4, Src: 157.240.1.60, Dst: 192.168.1.161
> Transmission Control Protocol, Src Port: 443, Dst Port: 50188, Seq: 1, Ack: 1, Len: 109
> Transport Layer Security
```

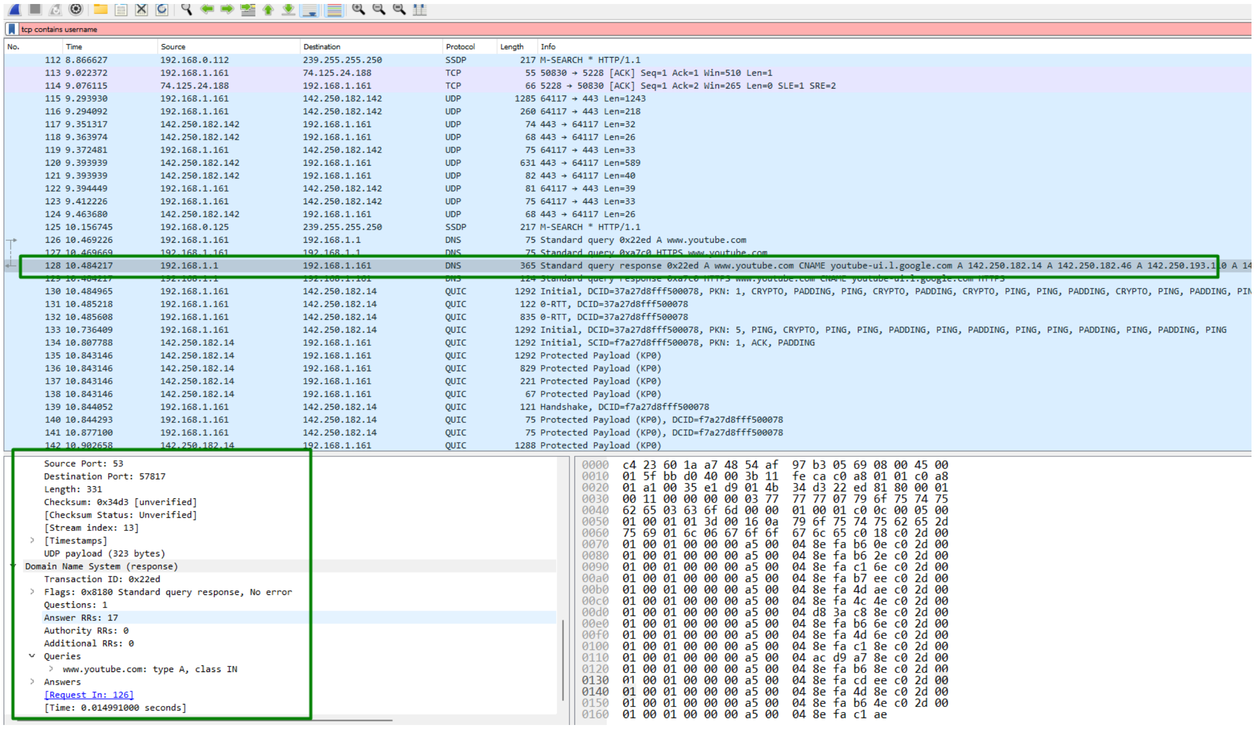
```
0000  c4 23 60 1a a7 48 54 af  97 b3 05 69 08 00 45 00
0010  00 95 b1 e1 40 00 57 06  10 0c 9d f0 01 3c c0 a8
0020  01 a1 01 bb c4 0c 51 a0  23 98 65 ca 9d 5a 50 18
0030  02 58 ee bb 00 00 17 03  03 00 68 a1 f3 8a ad e0
0040  9a e5 d5 55 69 e5 a2 34  d7 bd 1b 97 bc d1 ff 7e
0050  da 89 77 82 c5 83 b2 bd  c5 c9 b4 02 35 88 a4 ea
0060  88 7a 73 3c 26 c2 18 2d  74 c8 f2 9a 40 a6 09 c5
0070  99 f3 ba 0a a3 7b a9 50  34 20 56 82 8f db a6 7f
0080  5e 1b 3f 8e c7 64 6a 05  0a de a7 3e 8c c1 07 40
0090  af 9e 4e 9c c5 27 aa c6  ff 1c 04 04 99 28 02 9c
00a0  66 99 d9
```

We are finding all tcp details .

Now check website Details :

1 . Youtube

- □ Search result :



tcp contains username

```
No.    Time        Source            Destination       Protocol  Length Info
   112 8.866627    192.168.0.112     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
   113 9.022372    192.168.1.161     74.125.24.188     TCP        55 50830 → 5228 [ACK] Seq=1 Ack=1 Win=510 Len=1
   114 9.076115    74.125.24.188     192.168.1.161     TCP        66 5228 → 50830 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
   115 9.293930    192.168.1.161     142.250.182.142   UDP      1285 64117 → 443 Len=1243
   116 9.294092    192.168.1.161     142.250.182.142   UDP       260 64117 → 443 Len=218
   117 9.351317    142.250.182.142   192.168.1.161     UDP        74 443 → 64117 Len=32
   118 9.363974    142.250.182.142   192.168.1.161     UDP        68 443 → 64117 Len=26
   119 9.372481    192.168.1.161     142.250.182.142   UDP        75 64117 → 443 Len=33
   120 9.393939    142.250.182.142   192.168.1.161     UDP       631 443 → 64117 Len=589
   121 9.393939    142.250.182.142   192.168.1.161     UDP        82 443 → 64117 Len=40
   122 9.394449    192.168.1.161     142.250.182.142   UDP        81 64117 → 443 Len=39
   123 9.412226    192.168.1.161     142.250.182.142   UDP        75 64117 → 443 Len=33
   124 9.463680    142.250.182.142   192.168.1.161     UDP        68 443 → 64117 Len=26
   125 10.156745   192.168.0.125     239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
   126 10.469226   192.168.1.161     192.168.1.1       DNS        75 Standard query 0x22ed A www.youtube.com
   127 10.469669   192.168.1.161     192.168.1.1       DNS        75 Standard query 0xa7c0 HTTPS www.youtube.com
   128 10.484217   192.168.1.1       192.168.1.161     DNS       365 Standard query response 0x22ed A www.youtube.com CNAME youtube-ui.l.google.com A 142.250.182.14 A 142.250.182.46 A 142.250.193.110 A 14
   129 10.484217   192.168.1.1       192.168.1.161     DNS       124 Standard query response 0xa7c0 HTTPS www.youtube.com CNAME youtube-ui.l.google.com HTTPS
   130 10.484965   192.168.1.161     142.250.182.14    QUIC     1292 Initial, DCID=37a27d8fff500078, PKN: 1, CRYPTO, PADDING, PING, CRYPTO, PADDING, CRYPTO, PING, PING, PADDING, CRYPTO, PING, PADDING, PIN
   131 10.485218   192.168.1.161     142.250.182.14    QUIC      122 0-RTT, DCID=37a27d8fff500078
   132 10.485608   192.168.1.161     142.250.182.14    QUIC      835 0-RTT, DCID=37a27d8fff500078
   133 10.736409   192.168.1.161     142.250.182.14    QUIC     1292 Initial, DCID=37a27d8fff500078, PKN: 5, PING, CRYPTO, PING, PING, PADDING, PING, PADDING, PING, PING, PADDING, PING, PADDING, PING
   134 10.807788   142.250.182.14    192.168.1.161     QUIC     1292 Initial, SCID=f7a27d8fff500078, PKN: 1, ACK, PADDING
   135 10.843146   142.250.182.14    192.168.1.161     QUIC     1292 Protected Payload (KP0)
   136 10.843146   142.250.182.14    192.168.1.161     QUIC      829 Protected Payload (KP0)
   137 10.843146   142.250.182.14    192.168.1.161     QUIC      221 Protected Payload (KP0)
   138 10.843146   142.250.182.14    192.168.1.161     QUIC       67 Protected Payload (KP0)
   139 10.844052   192.168.1.161     142.250.182.14    QUIC      121 Handshake, DCID=f7a27d8fff500078
   140 10.844293   192.168.1.161     142.250.182.14    QUIC       75 Protected Payload (KP0), DCID=f7a27d8fff500078
   141 10.877100   192.168.1.161     142.250.182.14    QUIC       75 Protected Payload (KP0), DCID=f7a27d8fff500078
   142 10.902658   142.250.182.14    192.168.1.161     QUIC     1288 Protected Payload (KP0)
```

```
    Source Port: 53
    Destination Port: 57817
    Length: 331
    Checksum: 0x34d3 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 13]
  > [Timestamps]
    UDP payload (323 bytes)
v Domain Name System (response)
    Transaction ID: 0x22ed
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 17
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    > www.youtube.com: type A, class IN
  > Answers
    [Request In: 126]
    [Time: 0.014991000 seconds]
```

```
0000  c4 23 60 1a a7 48 54 af  97 b3 05 69 08 00 45 00
0010  01 5f bb d0 40 00 3b 11  fe ca c0 a8 01 01 c0 a8
0020  01 a1 00 35 e1 d9 01 4b  34 d3 22 ed 81 80 00 01
0030  00 11 00 00 00 00 03 77  77 77 07 79 6f 75 74 75
0040  62 65 03 63 6f 6d 00 00  01 00 01 c0 0c 00 05 00
0050  01 00 01 01 3d 00 16 0a  79 6f 75 74 75 62 65 2d
0060  75 69 01 6c 06 67 6f 6f  67 6c 65 c0 18 c0 2d 00
0070  01 00 01 00 00 00 a5 00  04 8e fa b6 0e c0 2d 00
0080  01 00 01 00 00 00 a5 00  04 8e fa b6 2e c0 2d 00
0090  01 00 01 00 00 00 a5 00  04 8e fa c1 6e c0 2d 00
00a0  01 00 01 00 00 00 a5 00  04 8e fa b7 ee c0 2d 00
00b0  01 00 01 00 00 00 a5 00  04 8e fa 4d ae c0 2d 00
00c0  01 00 01 00 00 00 a5 00  04 8e fa 4c 4e c0 2d 00
00d0  01 00 01 00 00 00 a5 00  04 d8 3a c8 8e c0 2d 00
00e0  01 00 01 00 00 00 a5 00  04 8e fa b6 6e c0 2d 00
00f0  01 00 01 00 00 00 a5 00  04 8e fa 4d 6e c0 2d 00
0100  01 00 01 00 00 00 a5 00  04 8e fa c1 8e c0 2d 00
0110  01 00 01 00 00 00 a5 00  04 ac d9 a7 8e c0 2d 00
0120  01 00 01 00 00 00 a5 00  04 8e fa b6 8e c0 2d 00
0130  01 00 01 00 00 00 a5 00  04 8e fa cd ee c0 2d 00
0140  01 00 01 00 00 00 a5 00  04 8e fa 4d 8e c0 2d 00
0150  01 00 01 00 00 00 a5 00  04 8e fa b6 4e c0 2d 00
0160  01 00 01 00 00 00 a5 00  04 8e fa c1 ae
```

- □ We can save fail (pcap fail)

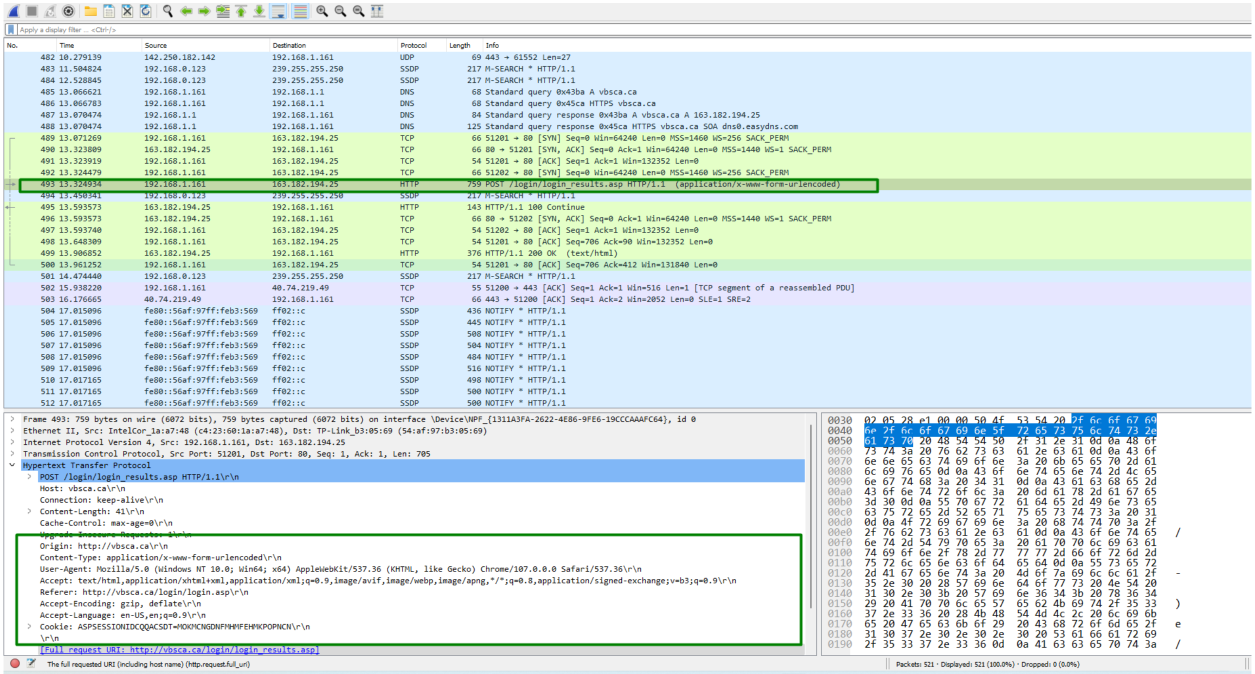
  Fail>Save>Name

- □ We can also open fail .

  Fail>Open> .pcap fail >open

2. http://vbsca.ca/login/login_results.asp

☐ Search result :



```
Apply a display filter ... <Ctrl-/>

No.   Time       Source                      Destination       Protocol Length Info
  482 10.279139  142.250.182.142             192.168.1.161     UDP        69 443 → 61552 Len=27
  483 11.504824  192.168.0.123               239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
  484 12.528845  192.168.0.123               239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
  485 13.066621  192.168.1.161               192.168.1.1       DNS        68 Standard query 0x43ba A vbsca.ca
  486 13.066783  192.168.1.161               192.168.1.1       DNS        68 Standard query 0x45ca HTTPS vbsca.ca
  487 13.070474  192.168.1.1                 192.168.1.161     DNS        84 Standard query response 0x43ba A vbsca.ca A 163.182.194.25
  488 13.070474  192.168.1.1                 192.168.1.161     DNS       125 Standard query response 0x45ca HTTPS vbsca.ca SOA dns0.easydns.com
  489 13.071269  192.168.1.161               163.182.194.25    TCP        66 51201 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  490 13.323809  163.182.194.25              192.168.1.161     TCP        66 80 → 51201 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 WS=1 SACK_PERM
  491 13.323919  192.168.1.161               163.182.194.25    TCP        54 51201 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  492 13.324479  192.168.1.161               163.182.194.25    TCP        66 51202 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  493 13.324934  192.168.1.161               163.182.194.25    HTTP      759 POST /login/login_results.asp HTTP/1.1  (application/x-www-form-urlencoded)
  494 13.450341  192.168.0.123               239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
  495 13.593573  163.182.194.25              192.168.1.161     HTTP      143 HTTP/1.1 100 Continue
  496 13.593573  163.182.194.25              192.168.1.161     TCP        66 80 → 51202 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 WS=1 SACK_PERM
  497 13.593740  192.168.1.161               163.182.194.25    TCP        54 51202 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
  498 13.648309  192.168.1.161               163.182.194.25    TCP        54 51201 → 80 [ACK] Seq=706 Ack=90 Win=132352 Len=0
  499 13.906852  163.182.194.25              192.168.1.161     HTTP      376 HTTP/1.1 200 OK  (text/html)
  500 13.961252  192.168.1.161               163.182.194.25    TCP        54 51201 → 80 [ACK] Seq=706 Ack=412 Win=131840 Len=0
  501 14.474440  192.168.0.123               239.255.255.250   SSDP      217 M-SEARCH * HTTP/1.1
  502 15.938220  192.168.1.161               40.74.219.49      TCP        55 51200 → 443 [ACK] Seq=1 Ack=1 Win=516 Len=1 [TCP segment of a reassembled PDU]
  503 16.176665  40.74.219.49                192.168.1.161     TCP        66 443 → 51200 [ACK] Seq=1 Ack=2 Win=2052 Len=0 SLE=1 SRE=2
  504 17.015096  fe80::56af:97ff:feb3:569    ff02::c           SSDP      436 NOTIFY * HTTP/1.1
  505 17.015096  fe80::56af:97ff:feb3:569    ff02::c           SSDP      445 NOTIFY * HTTP/1.1
  506 17.015096  fe80::56af:97ff:feb3:569    ff02::c           SSDP      508 NOTIFY * HTTP/1.1
  507 17.015096  fe80::56af:97ff:feb3:569    ff02::c           SSDP      504 NOTIFY * HTTP/1.1
  508 17.015096  fe80::56af:97ff:feb3:569    ff02::c           SSDP      484 NOTIFY * HTTP/1.1
  509 17.015096  fe80::56af:97ff:feb3:569    ff02::c           SSDP      516 NOTIFY * HTTP/1.1
  510 17.017165  fe80::56af:97ff:feb3:569    ff02::c           SSDP      498 NOTIFY * HTTP/1.1
  511 17.017165  fe80::56af:97ff:feb3:569    ff02::c           SSDP      500 NOTIFY * HTTP/1.1
  512 17.017165  fe80::56af:97ff:feb3:569    ff02::c           SSDP      500 NOTIFY * HTTP/1.1
```

```
> Frame 493: 759 bytes on wire (6072 bits), 759 bytes captured (6072 bits) on interface \Device\NPF_{1311A3FA-2622-4E86-9FE6-19CCCAAAFC64}, id 0
> Ethernet II, Src: IntelCor_1a:a7:48 (c4:23:60:1a:a7:48), Dst: TP-Link_b3:05:69 (54:af:97:b3:05:69)
> Internet Protocol Version 4, Src: 192.168.1.161, Dst: 163.182.194.25
> Transmission Control Protocol, Src Port: 51201, Dst Port: 80, Seq: 1, Ack: 1, Len: 705
v Hypertext Transfer Protocol
  > POST /login/login_results.asp HTTP/1.1\r\n
    Host: vbsca.ca\r\n
    Connection: keep-alive\r\n
  > Content-Length: 41\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Origin: http://vbsca.ca\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Referer: http://vbsca.ca/login/login.asp\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  > Cookie: ASPSESSIONIDCQQACSDT=MOKMCNGDNFMHMFEHMKPOPNCN\r\n
    \r\n
    [Full request URI: http://vbsca.ca/login/login_results.asp]
```

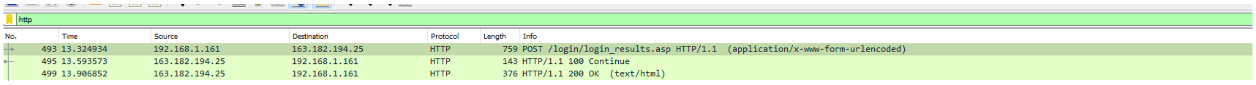
```
0030  02 05 28 e1 00 00 50 4f  53 54 20 2f 6c 6f 67 69
0040  6e 2f 6c 6f 67 69 6e 5f  72 65 73 75 6c 74 73 2e
0050  61 73 70 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f
0060  73 74 3a 20 76 62 73 63  61 2e 63 61 0d 0a 43 6f
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65
0090  6e 67 74 68 3a 20 34 31  0d 0a 43 61 63 68 65 2d
00a0  43 6f 6e 74 72 6f 6c 3a  20 6d 61 78 2d 61 67 65
00b0  3d 30 0d 0a 55 70 67 72  61 64 65 2d 49 6e 73 65
00c0  63 75 72 65 2d 52 65 71  75 65 73 74 73 3a 20 31
00d0  0d 0a 4f 72 69 67 69 6e  3a 20 68 74 74 70 3a 2f
00e0  2f 76 62 73 63 61 2e 63  61 0d 0a 43 6f 6e 74 65   /
00f0  6e 74 2d 54 79 70 65 3a  20 61 70 70 6c 69 63 61
0100  74 69 6f 6e 2f 78 2d 77  77 77 2d 66 6f 72 6d 2d
0110  75 72 6c 65 6e 63 6f 64  65 64 0d 0a 55 73 65 72
0120  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -
0130  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20
0140  31 30 2e 30 3b 20 57 69  6e 36 34 3b 20 78 36 34
0150  29 20 41 70 70 6c 65 57  65 62 4b 69 74 2f 35 33   )
0160  37 2e 33 36 20 28 4b 48  54 4d 4c 2c 20 6c 69 6b
0170  65 20 47 65 63 6b 6f 29  20 43 68 72 6f 6d 65 2f   e
0180  31 30 37 2e 30 2e 30 2e  30 20 53 61 66 61 72 69
0190  2f 35 33 37 2e 33 36 0d  0a 41 63 63 65 70 74 3a   /
```

The full requested URI (including host name) (http.request.full_uri)

Packets: 521 · Displayed: 521 (100.0%) · Dropped: 0 (0.0%)

Now we are filtering .

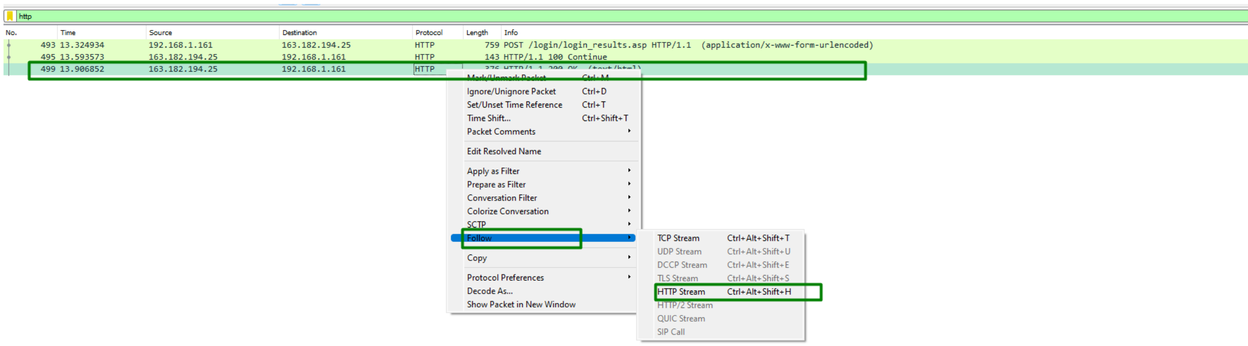
☐ Http :



```
http

No.   Time       Source           Destination      Protocol Length Info
  493 13.324934  192.168.1.161    163.182.194.25   HTTP      759 POST /login/login_results.asp HTTP/1.1  (application/x-www-form-urlencoded)
  495 13.593573  163.182.194.25   192.168.1.161    HTTP      143 HTTP/1.1 100 Continue
  499 13.906852  163.182.194.25   192.168.1.161    HTTP      376 HTTP/1.1 200 OK  (text/html)
```

- How can we read this data?

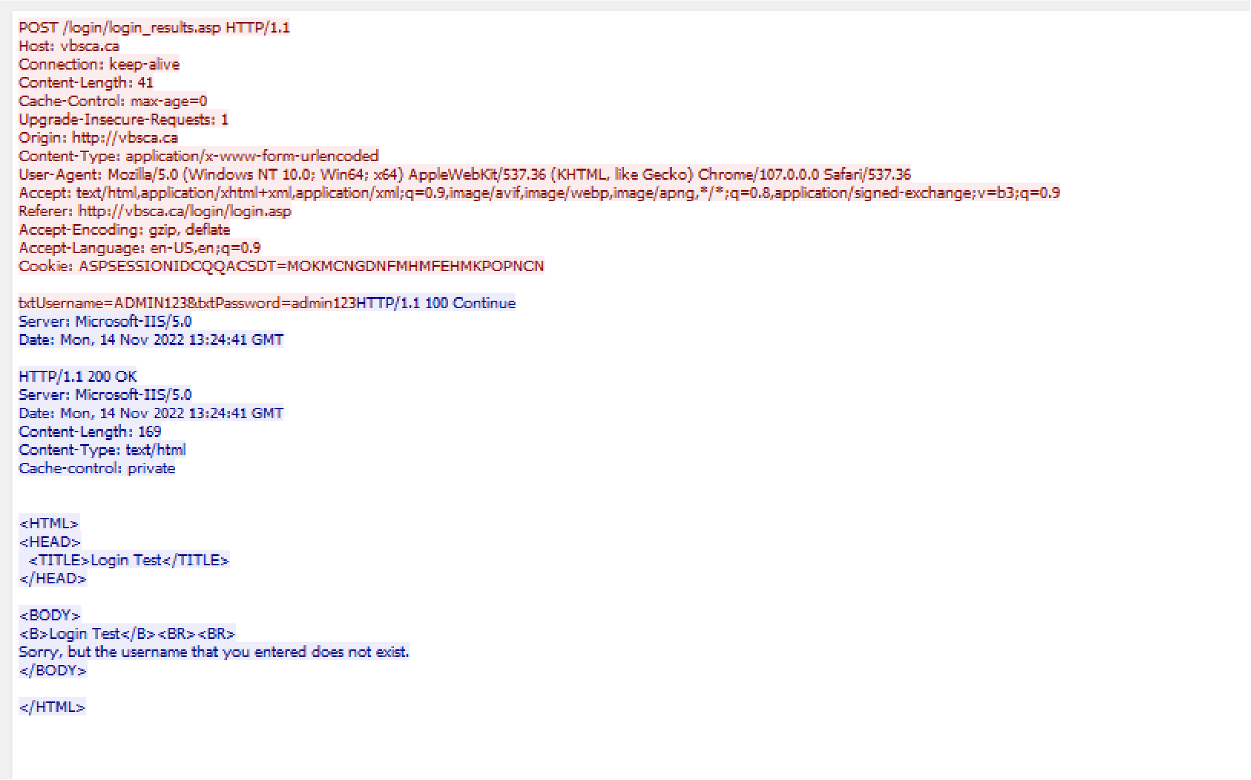
☐ Right Click > Follow > http stream



```
http

No.   Time       Source           Destination      Protocol Length Info
  493 13.324934  192.168.1.161    163.182.194.25   HTTP      759 POST /login/login_results.asp HTTP/1.1  (application/x-www-form-urlencoded)
  495 13.593573  163.182.194.25   192.168.1.161    HTTP      143 HTTP/1.1 100 Continue
  499 13.906852  163.182.194.25   192.168.1.161    HTTP      376 HTTP/1.1 200 OK  (text/html)
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call

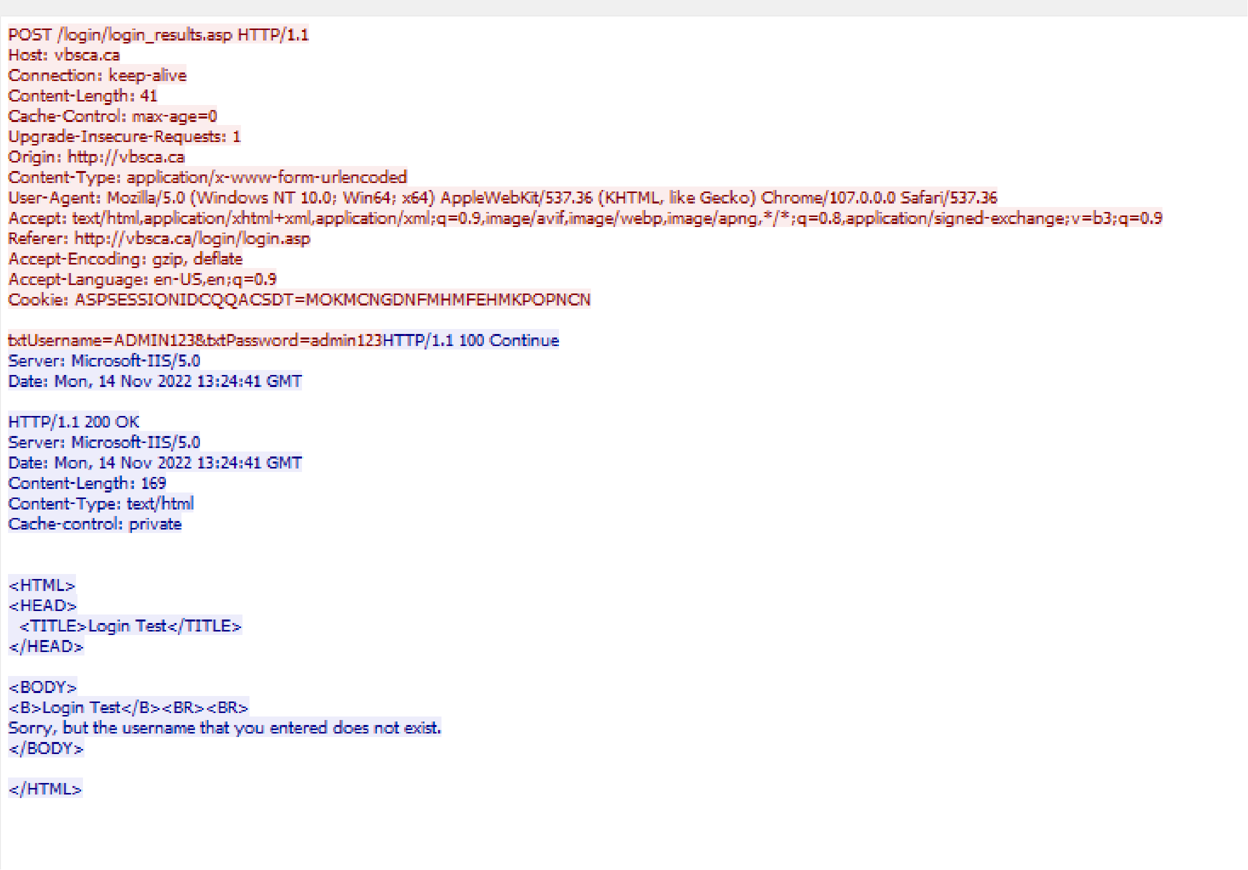
- **Http Result —**



```
POST /login/login_results.asp HTTP/1.1
Host: vbsca.ca
Connection: keep-alive
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vbsca.ca
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://vbsca.ca/login/login.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASPSESSIONIDCQQACSDT=MOKMCNGDNFMHMFEHMKPOPNCN

txtUsername=ADMIN123&txtPassword=admin123HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Mon, 14 Nov 2022 13:24:41 GMT

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 14 Nov 2022 13:24:41 GMT
Content-Length: 169
Content-Type: text/html
Cache-control: private


<HTML>
<HEAD>
 <TITLE>Login Test</TITLE>
</HEAD>

<BODY>
<B>Login Test</B><BR><BR>
Sorry, but the username that you entered does not exist.
</BODY>

</HTML>
```

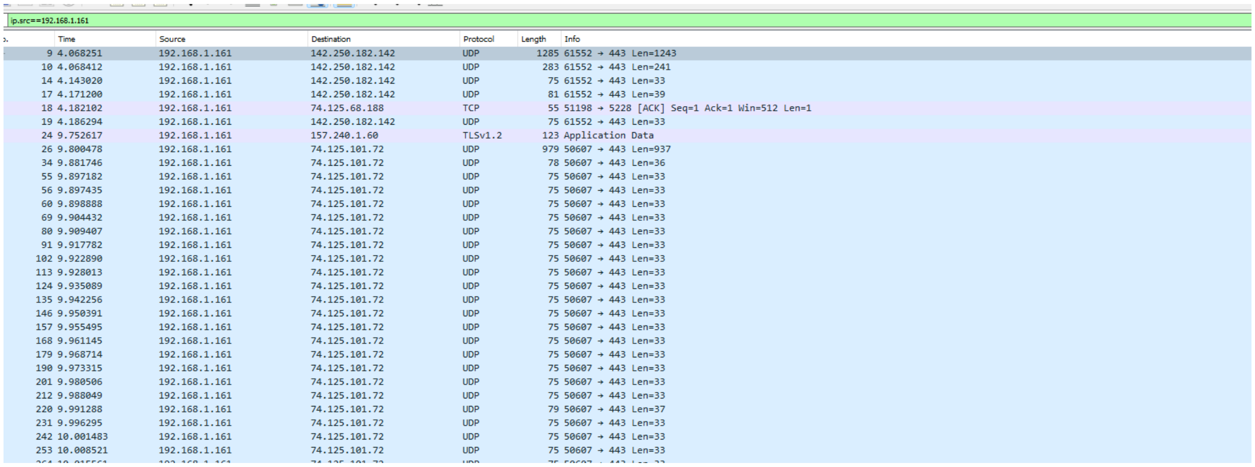
☐ Right Click > Follow > TCP stream

- **TCP Result :**



```
POST /login/login_results.asp HTTP/1.1
Host: vbsca.ca
Connection: keep-alive
Content-Length: 41
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://vbsca.ca
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://vbsca.ca/login/login.asp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: ASPSESSIONIDCQQACSDT=MOKMCNGDNFMHMFEHMKPOPNCN

txtUsername=ADMIN123&txtPassword=admin123HTTP/1.1 100 Continue
Server: Microsoft-IIS/5.0
Date: Mon, 14 Nov 2022 13:24:41 GMT

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Mon, 14 Nov 2022 13:24:41 GMT
Content-Length: 169
Content-Type: text/html
Cache-control: private


<HTML>
<HEAD>
  <TITLE>Login Test</TITLE>
</HEAD>

<BODY>
<B>Login Test</B><BR><BR>
Sorry, but the username that you entered does not exist.
</BODY>

</HTML>
```

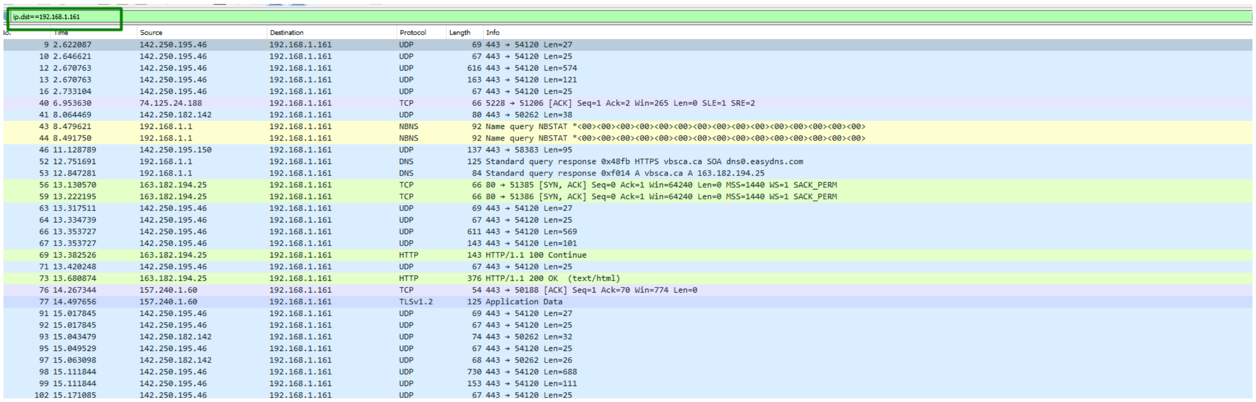
☐ **source =** ip.src==192.168.1.161



ip.src==192.168.1.161

o.	Time	Source	Destination	Protocol	Length	Info
9	4.068251	192.168.1.161	142.250.182.142	UDP	1285	61552 → 443 Len=1243
10	4.068412	192.168.1.161	142.250.182.142	UDP	283	61552 → 443 Len=241
14	4.143020	192.168.1.161	142.250.182.142	UDP	75	61552 → 443 Len=33
17	4.171200	192.168.1.161	142.250.182.142	UDP	81	61552 → 443 Len=39
18	4.182102	192.168.1.161	74.125.68.188	TCP	55	51198 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1
19	4.186294	192.168.1.161	142.250.182.142	UDP	75	61552 → 443 Len=33
24	9.752617	192.168.1.161	157.240.1.60	TLSv1.2	123	Application Data
26	9.800478	192.168.1.161	74.125.101.72	UDP	979	50607 → 443 Len=937
34	9.881746	192.168.1.161	74.125.101.72	UDP	78	50607 → 443 Len=36
55	9.897182	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
56	9.897435	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
60	9.898888	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
69	9.904432	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
80	9.909407	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
91	9.917782	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
102	9.922890	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
113	9.928013	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
124	9.935089	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
135	9.942256	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
146	9.950391	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
157	9.955495	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
168	9.961145	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
179	9.968714	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
190	9.973315	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
201	9.980506	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
212	9.988049	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
220	9.991288	192.168.1.161	74.125.101.72	UDP	79	50607 → 443 Len=37
231	9.996295	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
242	10.001483	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33
253	10.008521	192.168.1.161	74.125.101.72	UDP	75	50607 → 443 Len=33

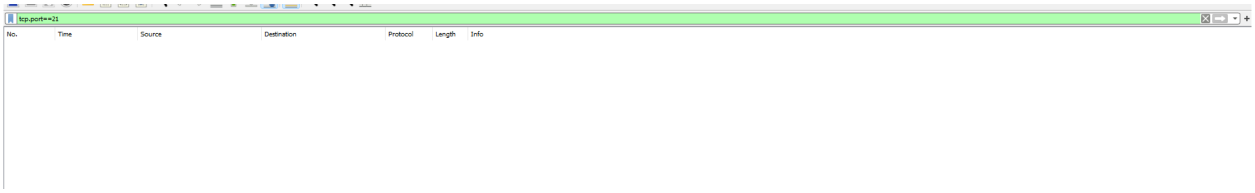
☐ Destination : ip.dst==192.168.1.162



```
ip.dst==192.168.1.161

No.  Time        Source            Destination     Protocol  Length  Info
  9 2.622087     142.250.195.46    192.168.1.161   UDP         69 443 → 54120 Len=27
 10 2.646621     142.250.195.46    192.168.1.161   UDP         67 443 → 54120 Len=25
 12 2.670763     142.250.195.46    192.168.1.161   UDP        616 443 → 54120 Len=574
 13 2.670763     142.250.195.46    192.168.1.161   UDP        163 443 → 54120 Len=121
 16 2.733104     142.250.195.46    192.168.1.161   UDP         67 443 → 54120 Len=25
 40 6.953630     74.125.24.188     192.168.1.161   TCP         66 5228 → 51206 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
 41 8.064469     142.250.182.142   192.168.1.161   UDP         80 443 → 50262 Len=38
 43 8.479621     192.168.1.1       192.168.1.161   NBNS        92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 44 8.491750     192.168.1.1       192.168.1.161   NBNS        92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00><00><00><00><00><00>
 46 11.128789    142.250.195.150   192.168.1.161   UDP        137 443 → 58383 Len=95
 52 12.751691    192.168.1.1       192.168.1.161   DNS        125 Standard query response 0x48fb HTTPS vbsca.ca SOA dns0.easydns.com
 53 12.847281    192.168.1.1       192.168.1.161   DNS         84 Standard query response 0xf014 A vbsca.ca A 163.182.194.25
 56 13.130570    163.182.194.25    192.168.1.161   TCP         66 80 → 51385 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 WS=1 SACK_PERM
 59 13.222195    163.182.194.25    192.168.1.161   TCP         66 80 → 51386 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 WS=1 SACK_PERM
 63 13.317511    142.250.195.46    192.168.1.161   UDP         69 443 → 54120 Len=27
 64 13.334739    142.250.195.46    192.168.1.161   UDP         67 443 → 54120 Len=25
 66 13.353727    142.250.195.46    192.168.1.161   UDP        611 443 → 54120 Len=569
 67 13.353727    142.250.195.46    192.168.1.161   UDP        143 443 → 54120 Len=101
 69 13.382526    163.182.194.25    192.168.1.161   HTTP       143 HTTP/1.1 100 Continue
 71 13.420248    142.250.195.46    192.168.1.161   UDP         67 443 → 54120 Len=25
 73 13.680874    163.182.194.25    192.168.1.161   HTTP       376 HTTP/1.1 200 OK  (text/html)
 76 14.267344    157.240.1.60      192.168.1.161   TCP         54 443 → 50188 [ACK] Seq=1 Ack=70 Win=774 Len=0
 77 14.497656    157.240.1.60      192.168.1.161   TLSv1.2    125 Application Data
 91 15.017845    142.250.195.46    192.168.1.161   UDP         69 443 → 54120 Len=27
 92 15.017845    142.250.195.46    192.168.1.161   UDP         67 443 → 54120 Len=25
 93 15.043479    142.250.182.142   192.168.1.161   UDP         74 443 → 50262 Len=32
 95 15.049529    142.250.195.46    192.168.1.161   UDP         67 443 → 54120 Len=25
 97 15.063098    142.250.182.142   192.168.1.161   UDP         68 443 → 50262 Len=26
 98 15.111844    142.250.195.46    192.168.1.161   UDP        730 443 → 54120 Len=688
 99 15.111844    142.250.195.46    192.168.1.161   UDP        153 443 → 54120 Len=111
102 15.171085    142.250.195.46    192.168.1.161   UDP         67 443 → 54120 Len=25
```

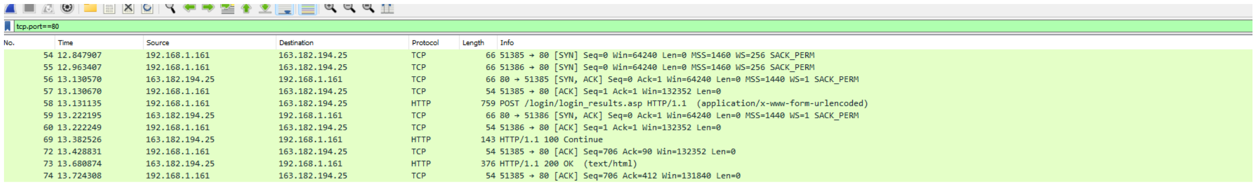
☐ Tcp port type :

tcp.port==21 (Prototype not built)



```
tcp.port==21

No.  Time  Source  Destination  Protocol  Length  Info
```

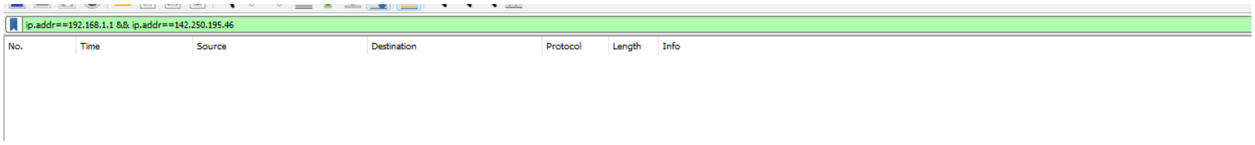
tcp.port==80(build)



```
tcp.port==80

No.  Time        Source            Destination       Protocol  Length  Info
 54 12.847907    192.168.1.161     163.182.194.25    TCP         66 51385 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 55 12.963407    192.168.1.161     163.182.194.25    TCP         66 51386 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 56 13.130570    163.182.194.25    192.168.1.161     TCP         66 80 → 51385 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 WS=1 SACK_PERM
 57 13.130670    192.168.1.161     163.182.194.25    TCP         54 51385 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
 58 13.131135    192.168.1.161     163.182.194.25    HTTP       759 POST /login/login_results.asp HTTP/1.1  (application/x-www-form-urlencoded)
 59 13.222195    163.182.194.25    192.168.1.161     TCP         66 80 → 51386 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 WS=1 SACK_PERM
 60 13.222249    192.168.1.161     163.182.194.25    TCP         54 51386 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
 69 13.382526    163.182.194.25    192.168.1.161     HTTP       143 HTTP/1.1 100 Continue
 72 13.428831    192.168.1.161     163.182.194.25    TCP         54 51385 → 80 [ACK] Seq=706 Ack=90 Win=132352 Len=0
 73 13.680874    163.182.194.25    192.168.1.161     HTTP       376 HTTP/1.1 200 OK  (text/html)
 74 13.724308    192.168.1.161     163.182.194.25    TCP         54 51385 → 80 [ACK] Seq=706 Ack=412 Win=131840 Len=0
```

☐ Two different ip address

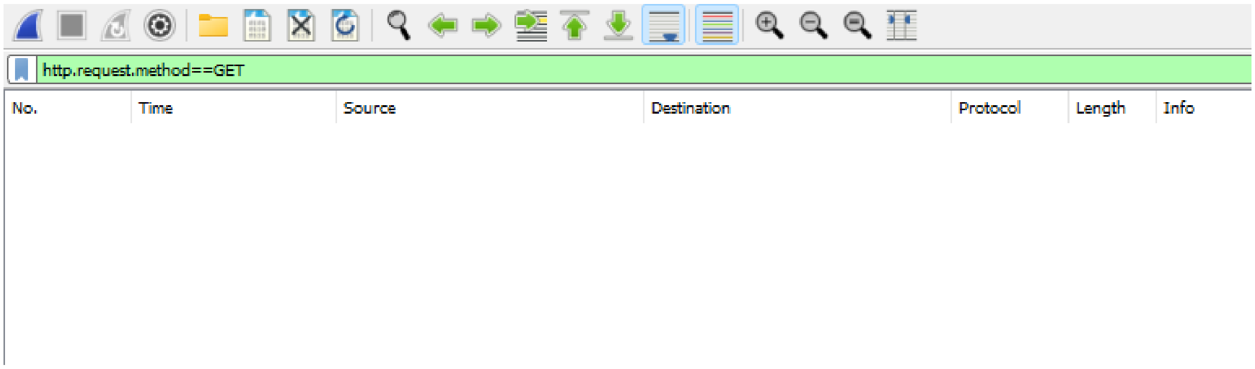
ip.addr==192.168.1.1 && ip.addr==142.250.195.46



```
ip.addr==192.168.1.1 && ip.addr==142.250.195.46

No.  Time  Source  Destination  Protocol  Length  Info
```

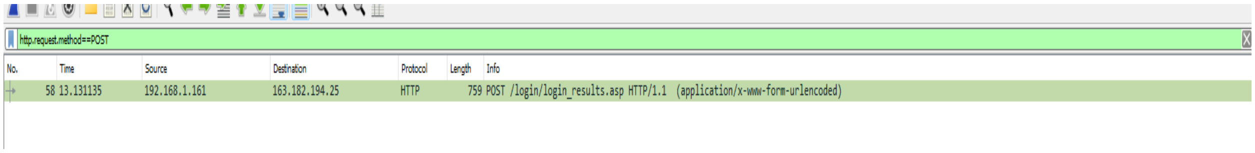
- □ **If we only wanted to see HTTP GET?POST request in our site or file**

>>http.request.method==GET



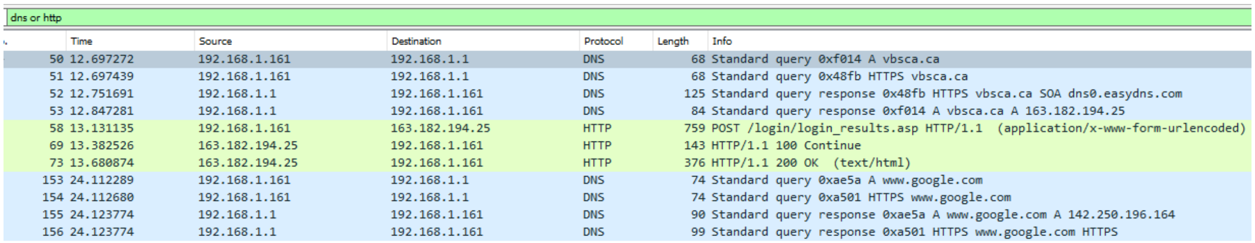
```
http.request.method==GET
No.    Time    Source    Destination    Protocol    Length    Info
```

>>>http.request.method== POST



```
http.request.method==POST
No.   Time          Source          Destination      Protocol   Length   Info
   58 13.131135     192.168.1.161   163.182.194.25   HTTP          759 POST /login/login_results.asp HTTP/1.1  (application/x-www-form-urlencoded)
```

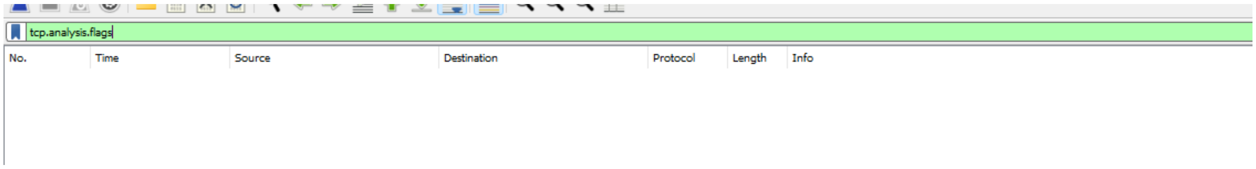
- □ **Two protocol in display >> dns or http**



```
dns or http
.       Time        Source            Destination       Protocol   Length Info
     50 12.697272   192.168.1.161     192.168.1.1       DNS            68 Standard query 0xf014 A vbsca.ca
     51 12.697439   192.168.1.161     192.168.1.1       DNS            68 Standard query 0x48fb HTTPS vbsca.ca
     52 12.751691   192.168.1.1       192.168.1.161     DNS           125 Standard query response 0x48fb HTTPS vbsca.ca SOA dns0.easydns.com
     53 12.847281   192.168.1.1       192.168.1.161     DNS            84 Standard query response 0xf014 A vbsca.ca A 163.182.194.25
     58 13.131135   192.168.1.161     163.182.194.25    HTTP          759 POST /login/login_results.asp HTTP/1.1  (application/x-www-form-urlencoded)
     69 13.382526   163.182.194.25    192.168.1.161     HTTP          143 HTTP/1.1 100 Continue
     73 13.680874   163.182.194.25    192.168.1.161     HTTP          376 HTTP/1.1 200 OK  (text/html)
    153 24.112289   192.168.1.161     192.168.1.1       DNS            74 Standard query 0xae5a A www.google.com
    154 24.112680   192.168.1.161     192.168.1.1       DNS            74 Standard query 0xa501 HTTPS www.google.com
    155 24.123774   192.168.1.1       192.168.1.161     DNS            90 Standard query response 0xae5a A www.google.com A 142.250.196.164
    156 24.123774   192.168.1.1       192.168.1.161     DNS            99 Standard query response 0xa501 HTTPS www.google.com HTTPS
```

- □ **Wireshark can flag TCP problems in the trace file.**

  >>tcp.analysis.flags



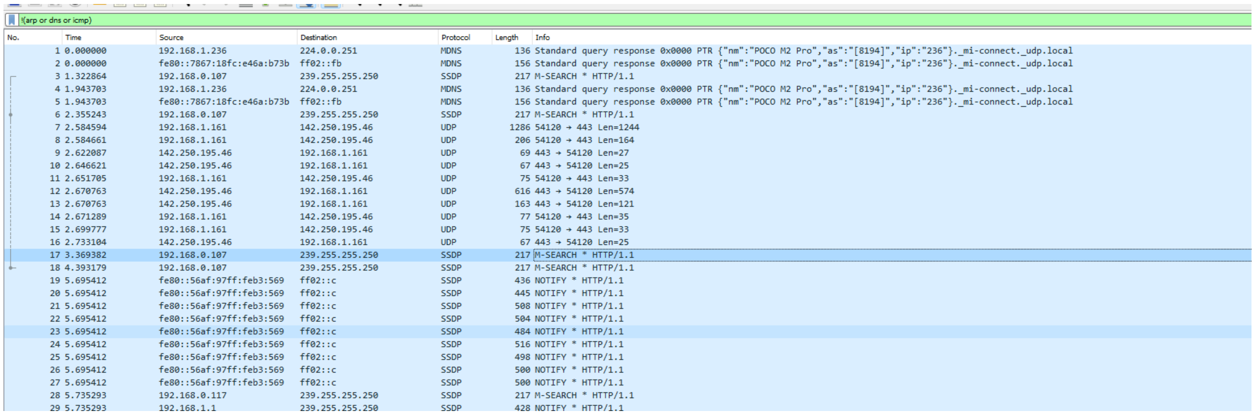
tcp.analysis.flags

No.	Time	Source	Destination	Protocol	Length	Info

>> If we have some duplicate acknowledgments of his mission a tcp previous segment not captured now all of those may indicate packet loss could be window problem or whatever those TCP issues are that wireshark has already flagged this is an excellent filter to use . If we're just trying to quickly identify whether a problem is rooted in the network or if it's rooted in the application the next filter we.re going to take a look at is how we can remove some of the noise and when we're looking in a trace file.

☐ **List of protocols or applications that were not in looking at so to do that to remove them from the trace file or to filter them out .**

>>> !(arp or dns or icmp)



!(arp or dns or icmp)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.236	224.0.0.251	MDNS	136	Standard query response 0x0000 PTR {"nm":"POCO M2 Pro","as":"[8194]","ip":"236"}._mi-connect._udp.local
2	0.000000	fe80::7867:18fc:e46a:b73b	ff02::fb	MDNS	156	Standard query response 0x0000 PTR {"nm":"POCO M2 Pro","as":"[8194]","ip":"236"}._mi-connect._udp.local
3	1.322864	192.168.0.107	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	1.943703	192.168.1.236	224.0.0.251	MDNS	136	Standard query response 0x0000 PTR {"nm":"POCO M2 Pro","as":"[8194]","ip":"236"}._mi-connect._udp.local
5	1.943703	fe80::7867:18fc:e46a:b73b	ff02::fb	MDNS	156	Standard query response 0x0000 PTR {"nm":"POCO M2 Pro","as":"[8194]","ip":"236"}._mi-connect._udp.local
6	2.355243	192.168.0.107	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
7	2.584594	192.168.1.161	142.250.195.46	UDP	1286	54120 → 443 Len=1244
8	2.584661	192.168.1.161	142.250.195.46	UDP	206	54120 → 443 Len=164
9	2.622087	142.250.195.46	192.168.1.161	UDP	69	443 → 54120 Len=27
10	2.646621	142.250.195.46	192.168.1.161	UDP	67	443 → 54120 Len=25
11	2.651705	192.168.1.161	142.250.195.46	UDP	75	54120 → 443 Len=33
12	2.670763	142.250.195.46	192.168.1.161	UDP	616	443 → 54120 Len=574
13	2.670763	142.250.195.46	192.168.1.161	UDP	163	443 → 54120 Len=121
14	2.671289	192.168.1.161	142.250.195.46	UDP	77	54120 → 443 Len=35
15	2.699777	192.168.1.161	142.250.195.46	UDP	75	54120 → 443 Len=33
16	2.733104	142.250.195.46	192.168.1.161	UDP	67	443 → 54120 Len=25
17	3.369382	192.168.0.107	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
18	4.393179	192.168.0.107	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
19	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	436	NOTIFY * HTTP/1.1
20	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	445	NOTIFY * HTTP/1.1
21	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	508	NOTIFY * HTTP/1.1
22	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	504	NOTIFY * HTTP/1.1
23	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	484	NOTIFY * HTTP/1.1
24	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	516	NOTIFY * HTTP/1.1
25	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	498	NOTIFY * HTTP/1.1
26	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	500	NOTIFY * HTTP/1.1
27	5.695412	fe80::56af:97ff:feb3:569	ff02::c	SSDP	500	NOTIFY * HTTP/1.1
28	5.735293	192.168.0.117	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
29	5.735293	192.168.1.1	239.255.255.250	SSDP	428	NOTIFY * HTTP/1.1