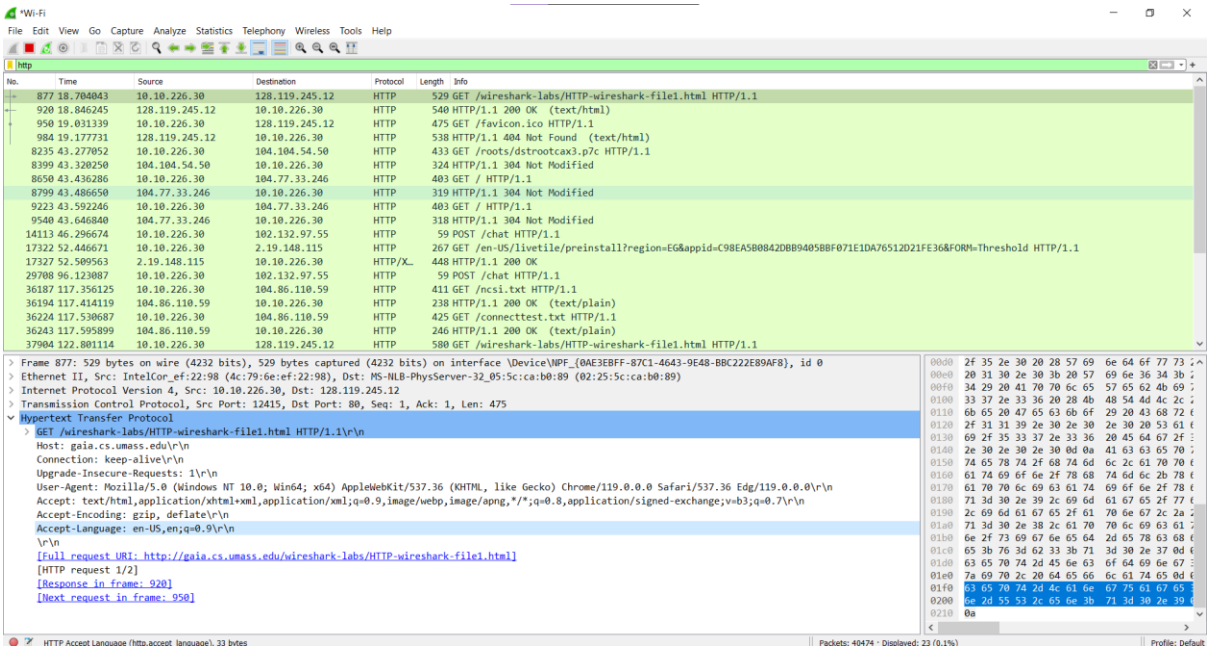
1. HTTP protocol:

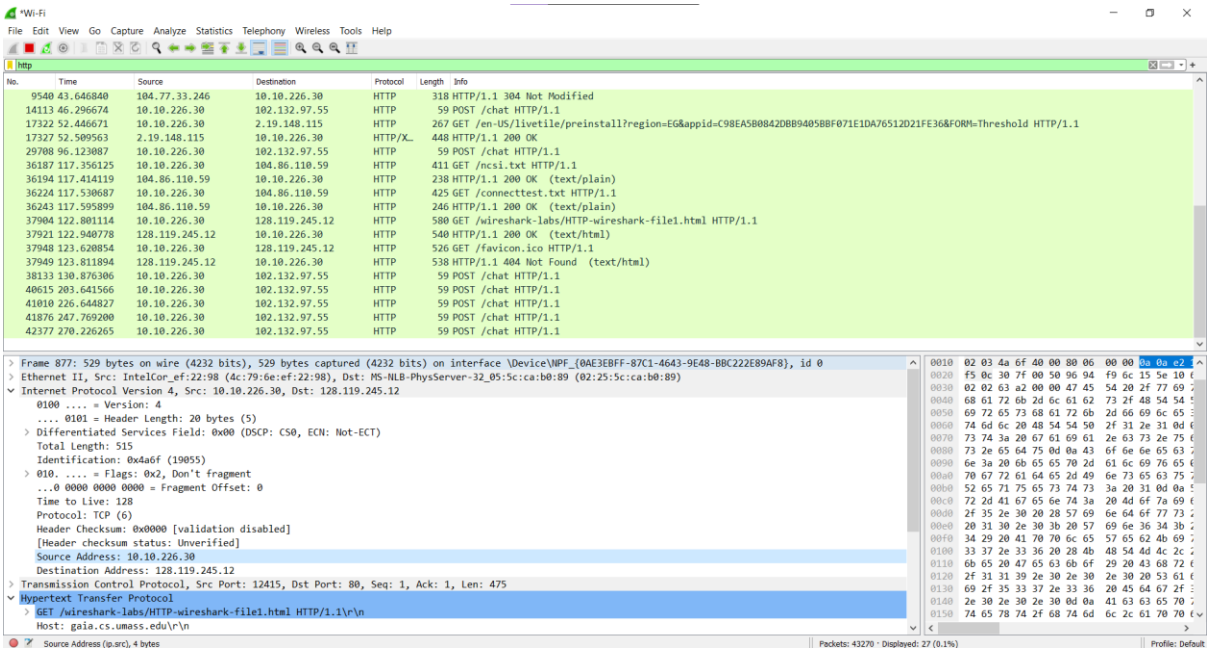
- Using this link http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

1. Accept language:



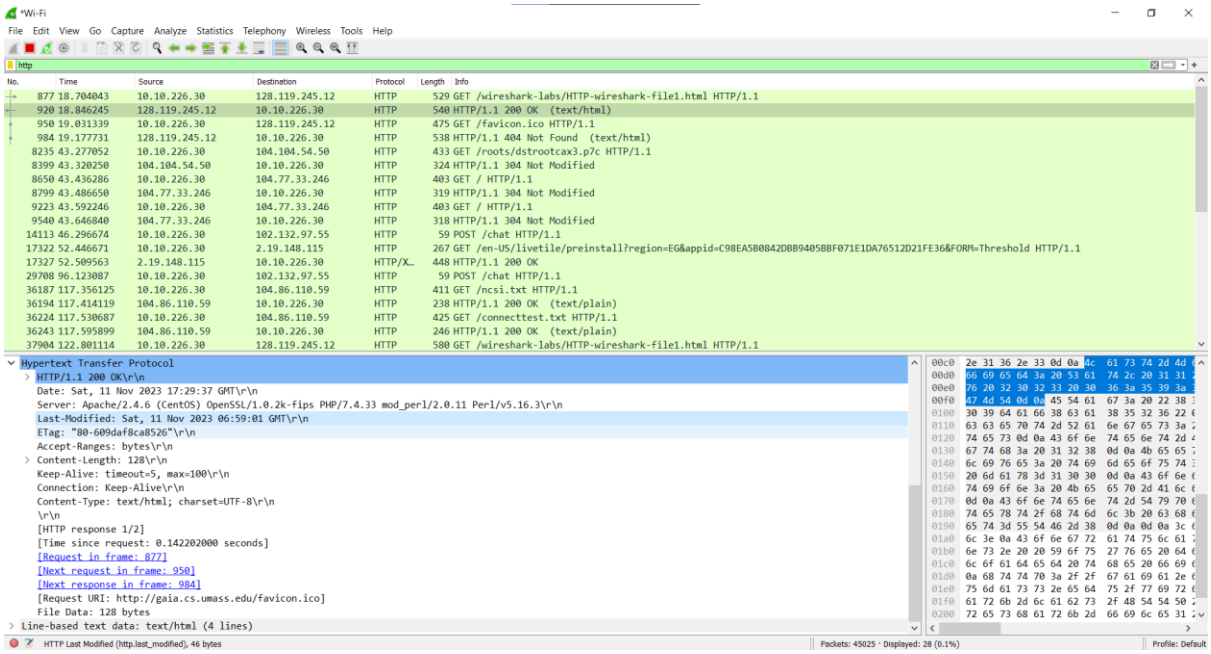
2. Ip address:

Source Address: 10.10.226.30



3. Last modified :

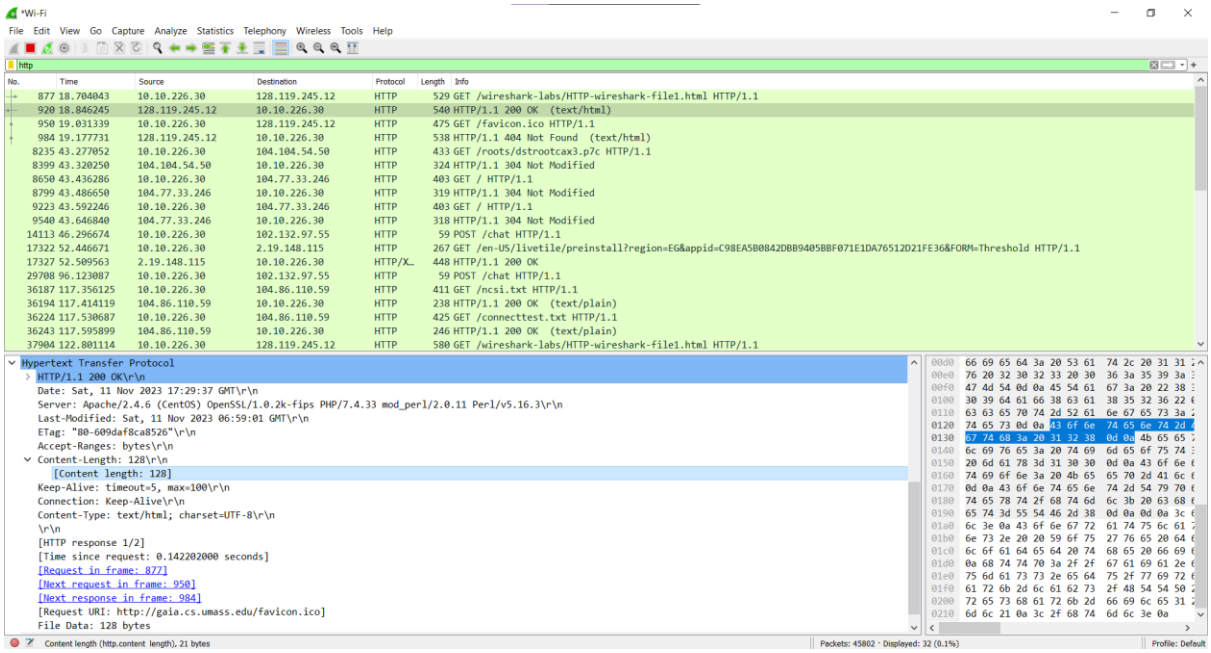
Last-Modified: Sat, 11 Nov 2023 06:59:01 GMT\r\n



4. Number of bytes of content are being returned to the browser:

Content-Length: 128\r\n

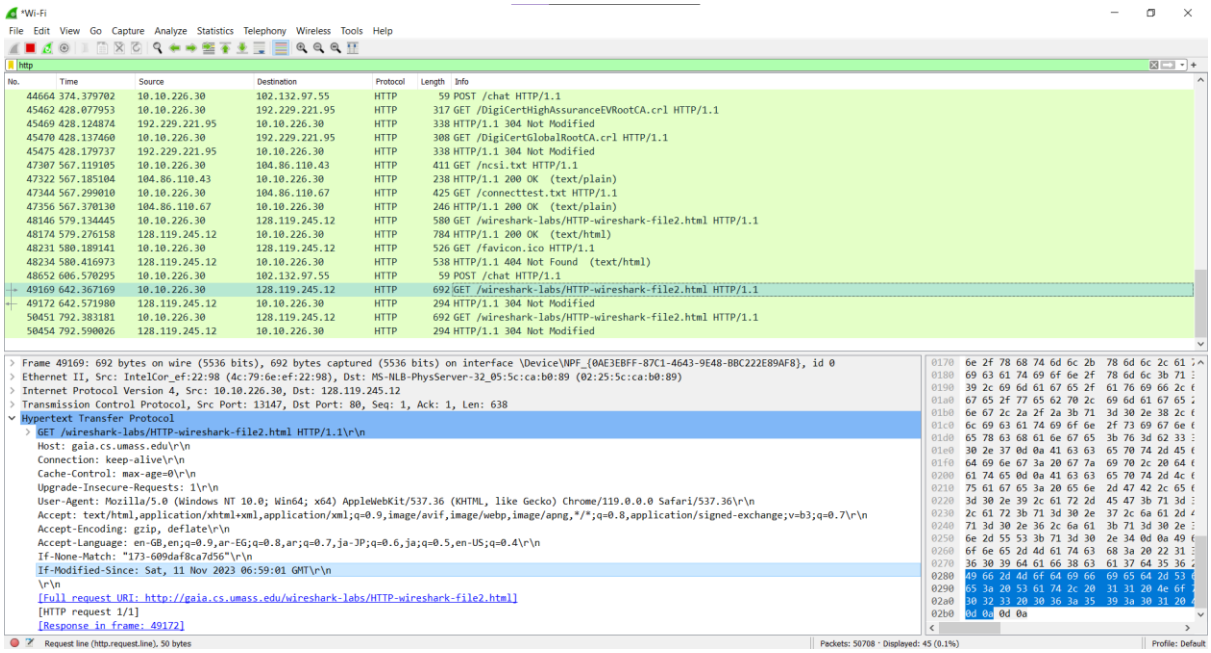
[Content length: 128]



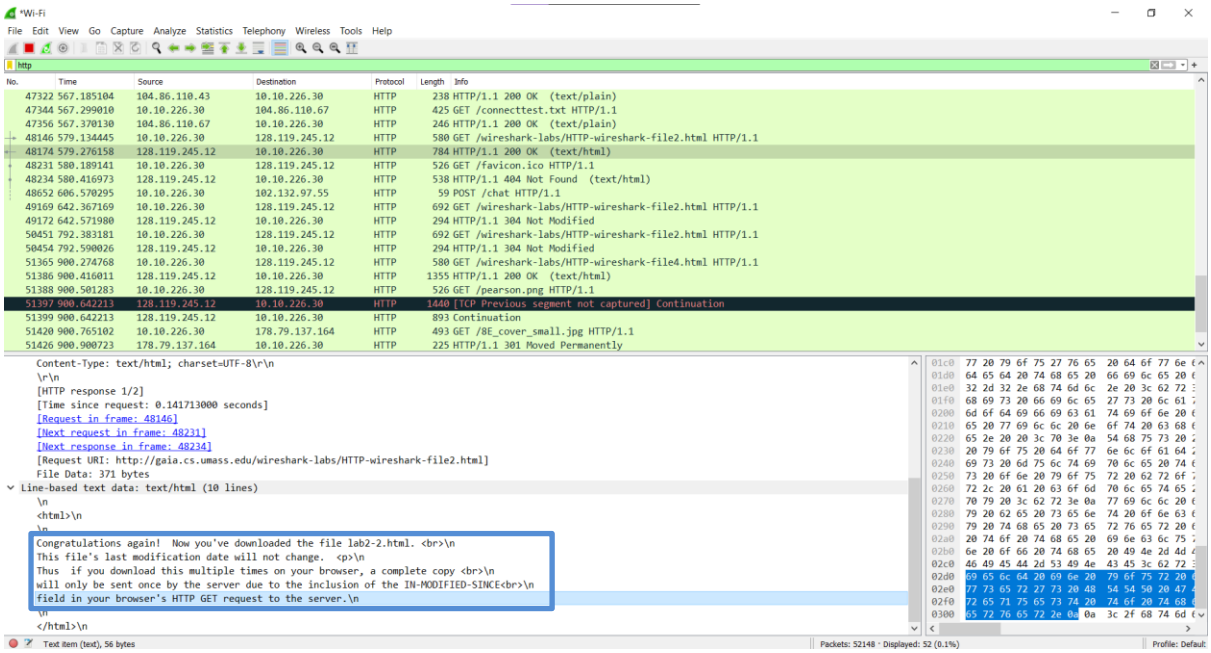
- Using this link http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html

1. “IF-MODIFIED-SINCE” line in the HTTP GET:

   If-Modified-Since: Sat, 11 Nov 2023 06:59:01 GMT\r\n

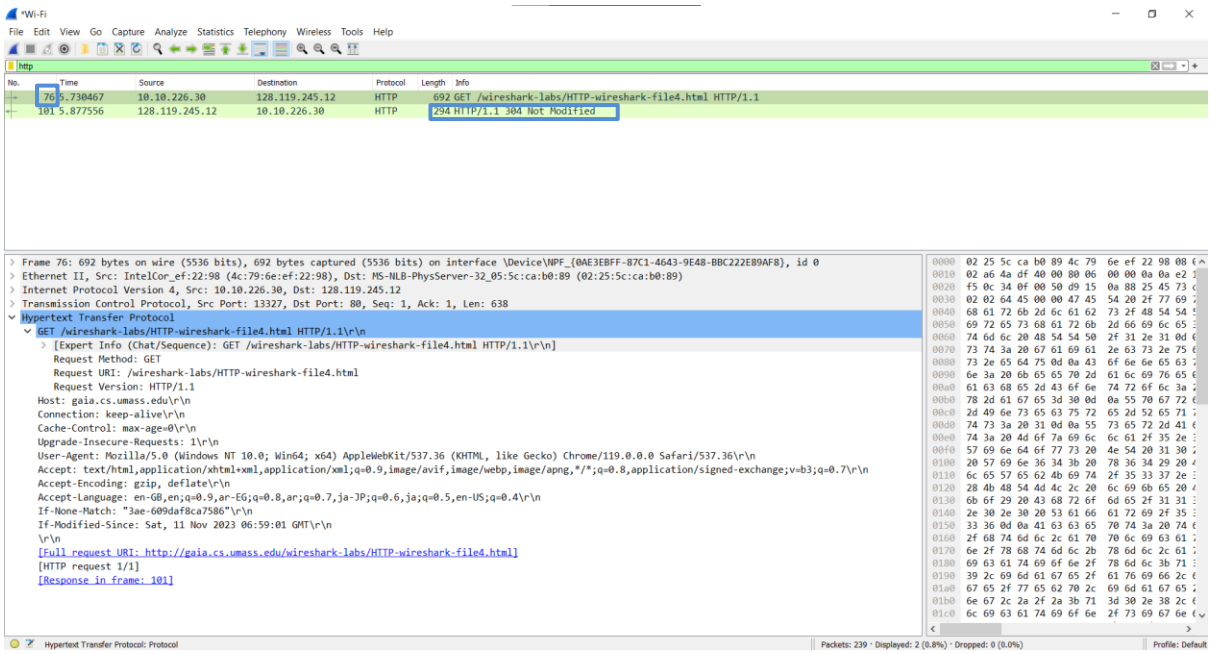


2. The contents of the server response:

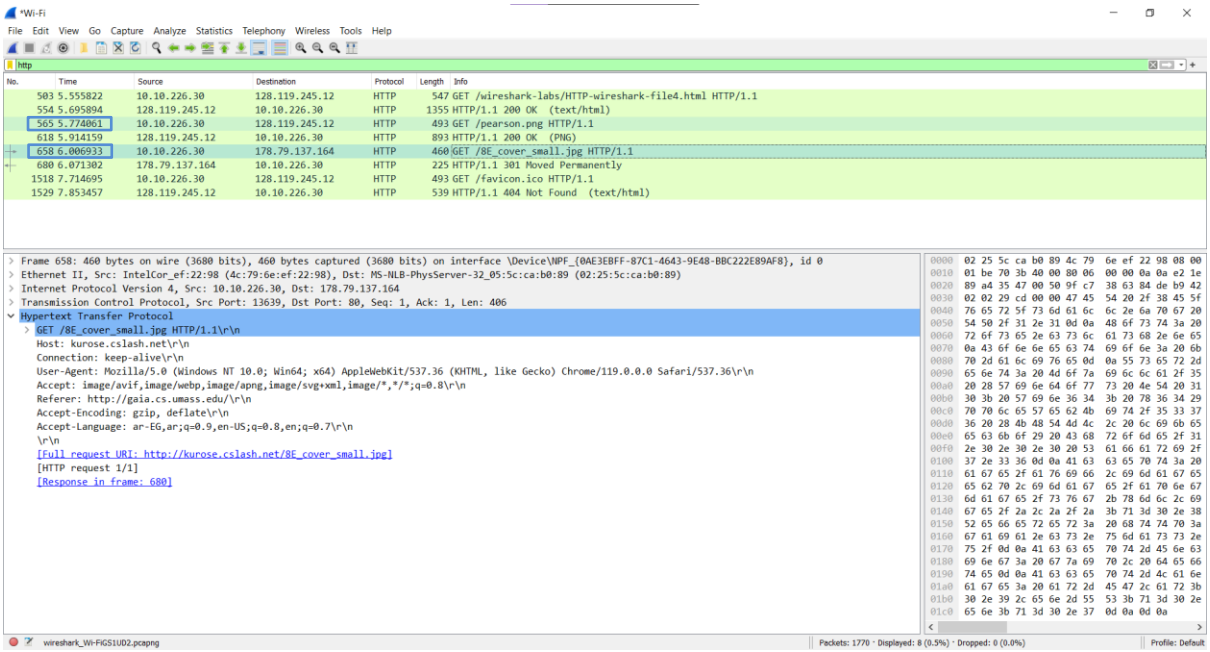


- Using this link http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html

1. HTTP GET request messages number:
    - 1 message
    - GET 76

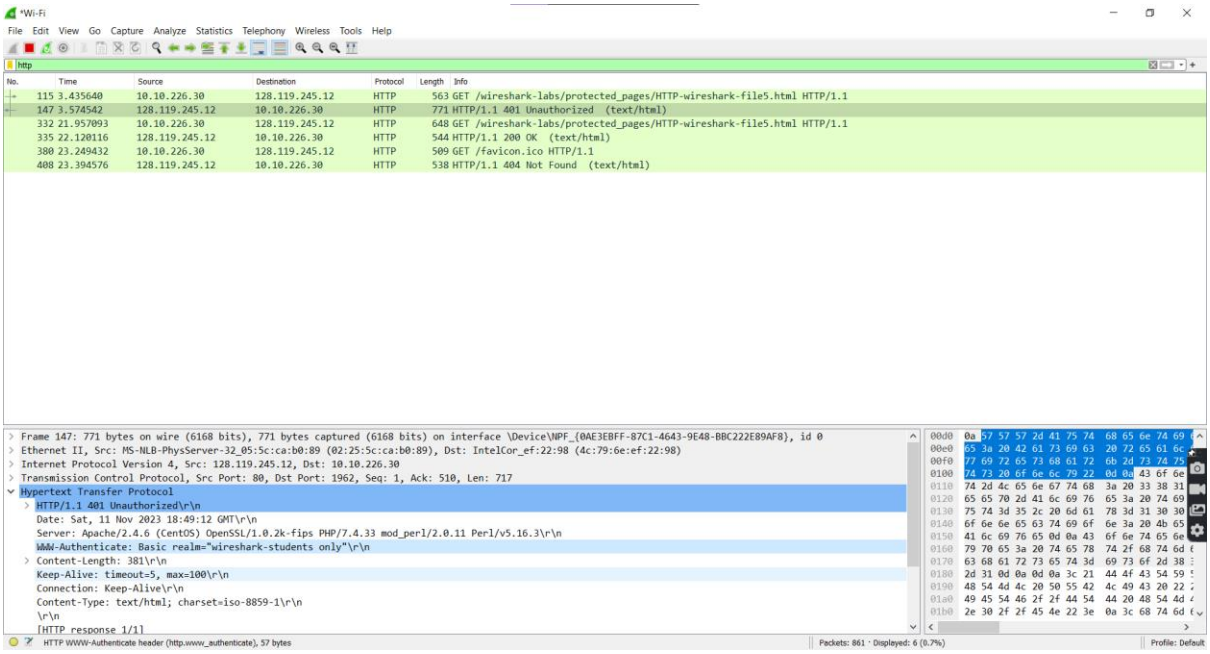


2. They were downloaded serially in different timestamp

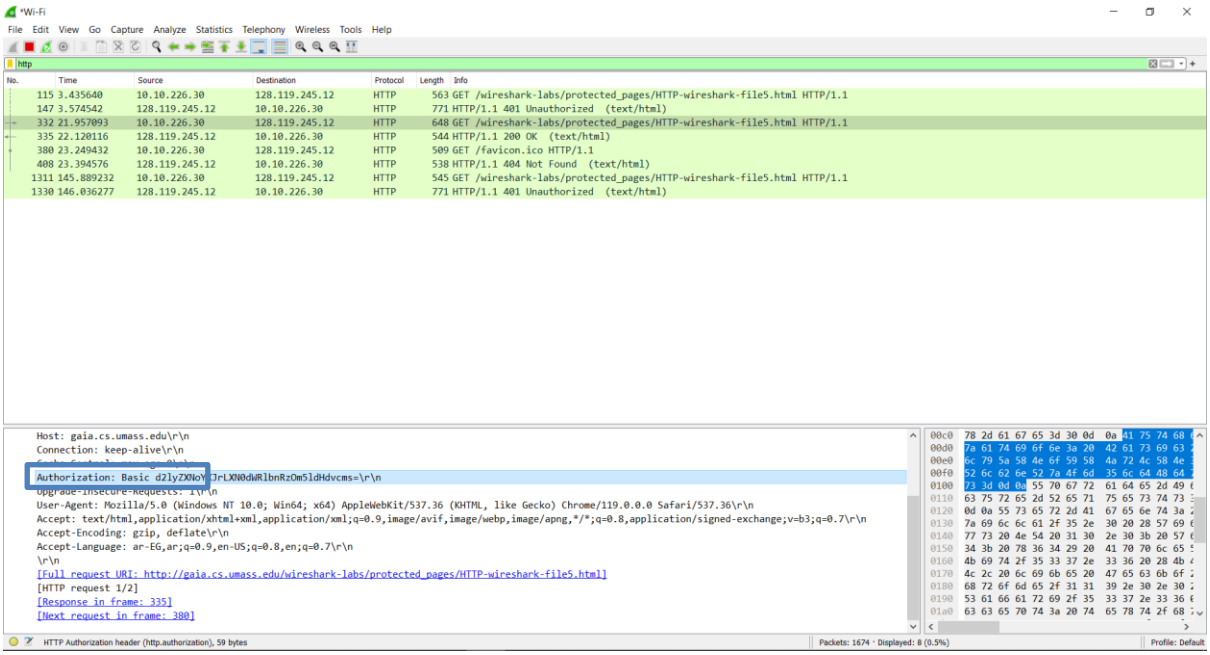


Using this link http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

1.



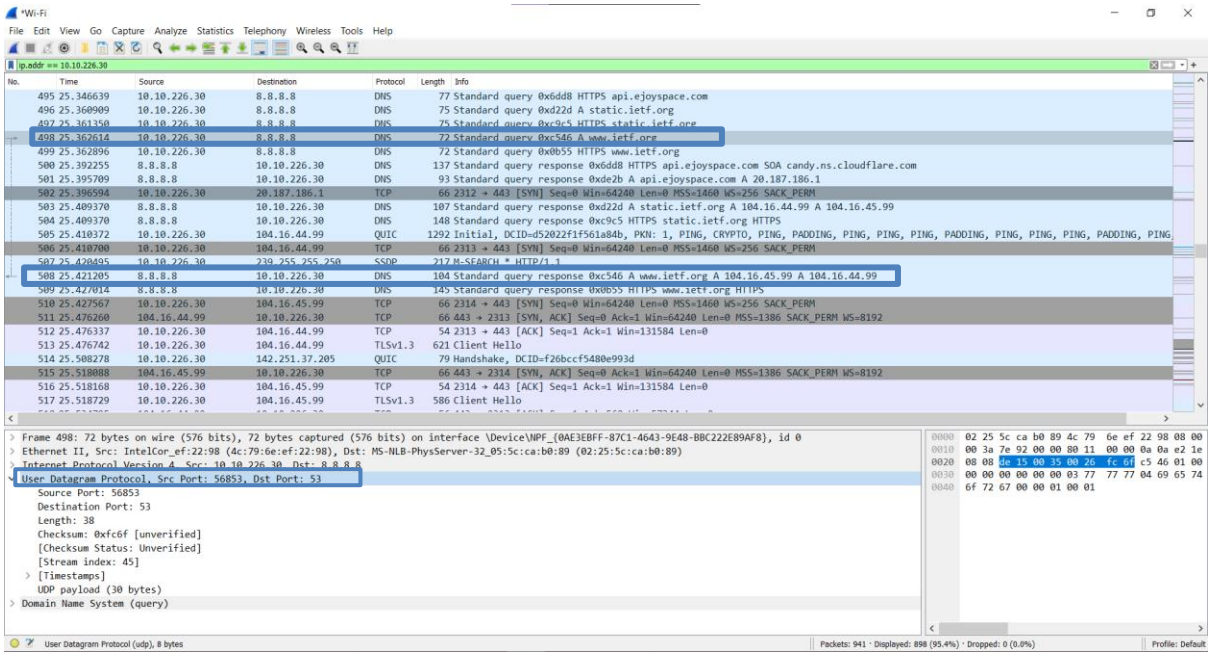
2. Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n



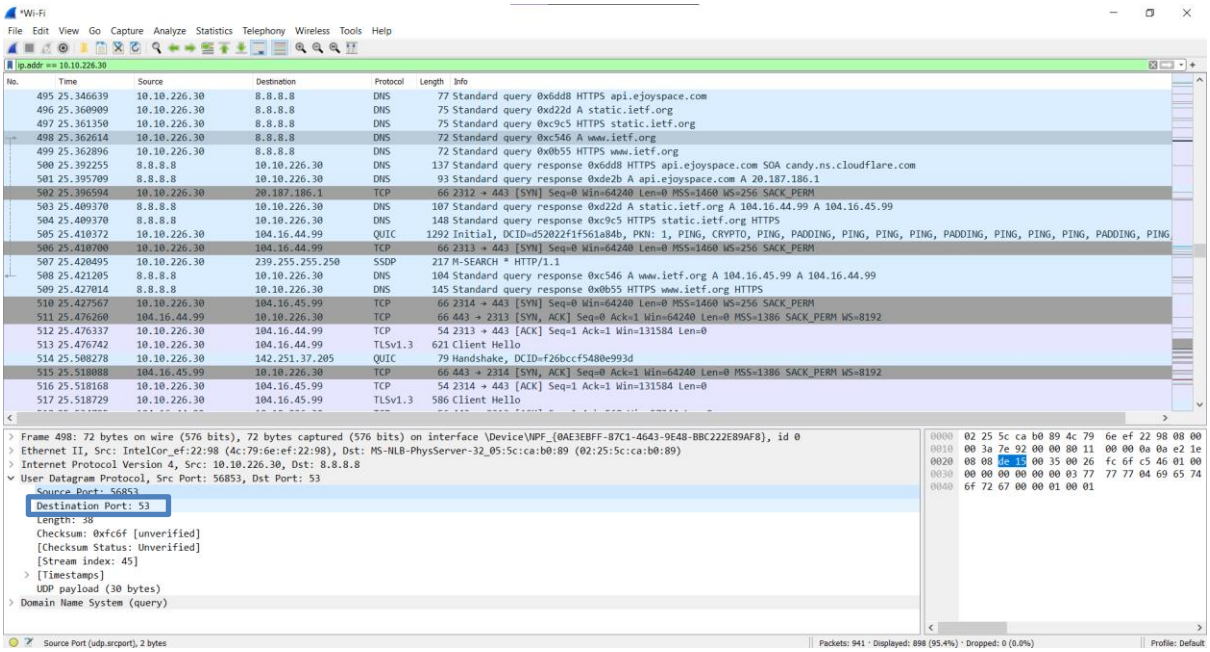
2.DNS Protocol:

```
Select Command Prompt
                                    fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 8:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 4C-79-6E-EF-22-99
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 4E-79-6E-EF-22-98
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : ejust.edu.eg
   Description . . . . . . . . . . . : Intel(R) Wireless-AC 9560
   Physical Address. . . . . . . . . : 4C-79-6E-EF-22-98
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::149e:f878:bb1d:c1c8%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.226.30(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Lease Obtained. . . . . . . . . . : Saturday, November 11, 2023 4:39:00 PM
   Lease Expires . . . . . . . . . . : Sunday, November 12, 2023 3:25:27 AM
   Default Gateway . . . . . . . . . : 10.10.224.1
   DHCP Server . . . . . . . . . . . : 10.10.10.23
   DHCPv6 IAID . . . . . . . . . . . : 55343470
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2B-76-A8-E9-4C-79-6E-EF-22-98
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 4C-79-6E-EF-22-9C
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

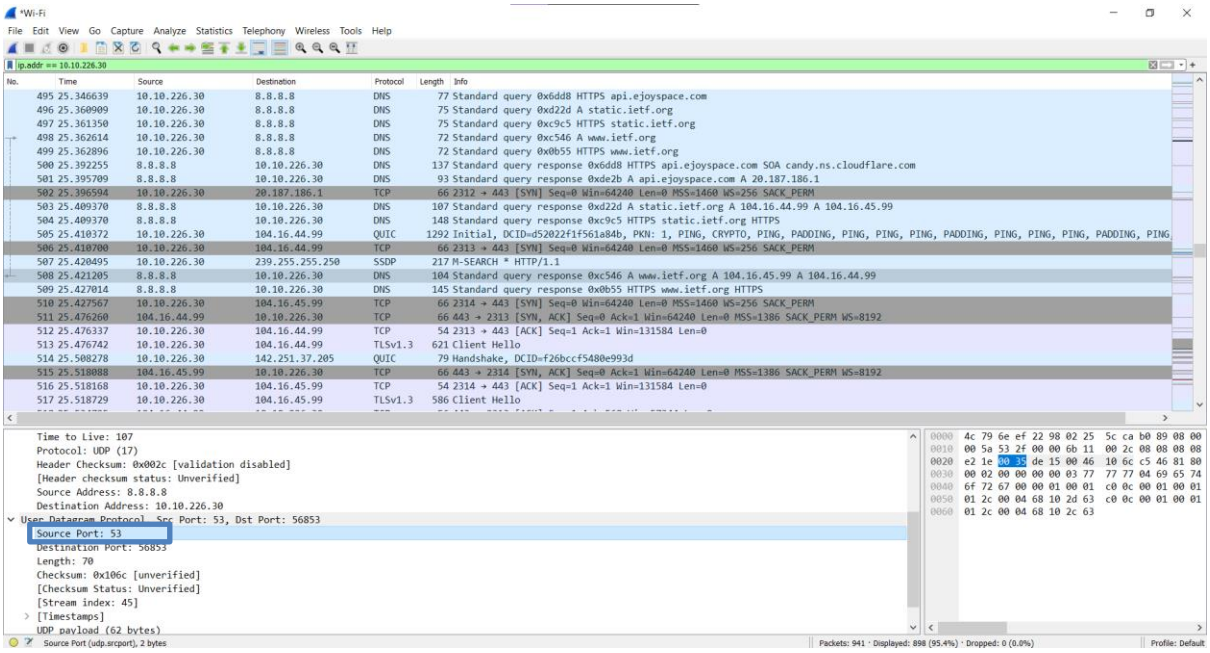
1. They’re sent over UDP



2. Destination port: 53

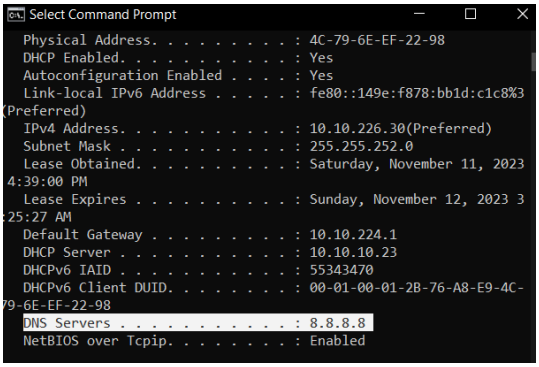


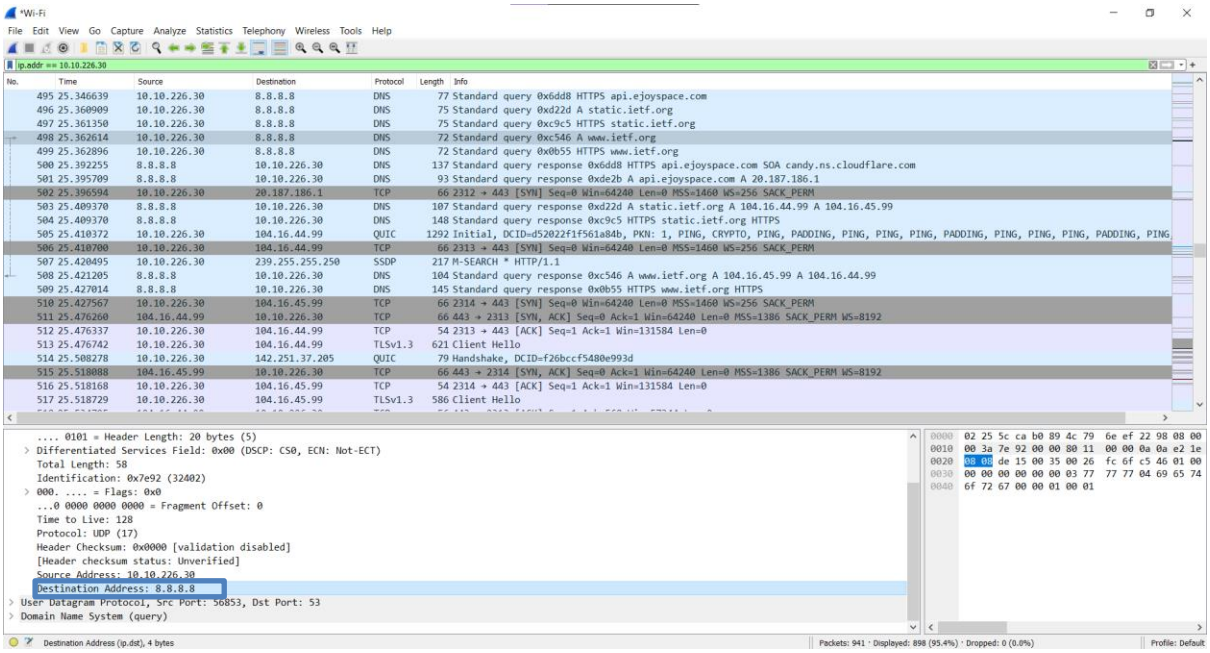
2.2 Source port : 56853



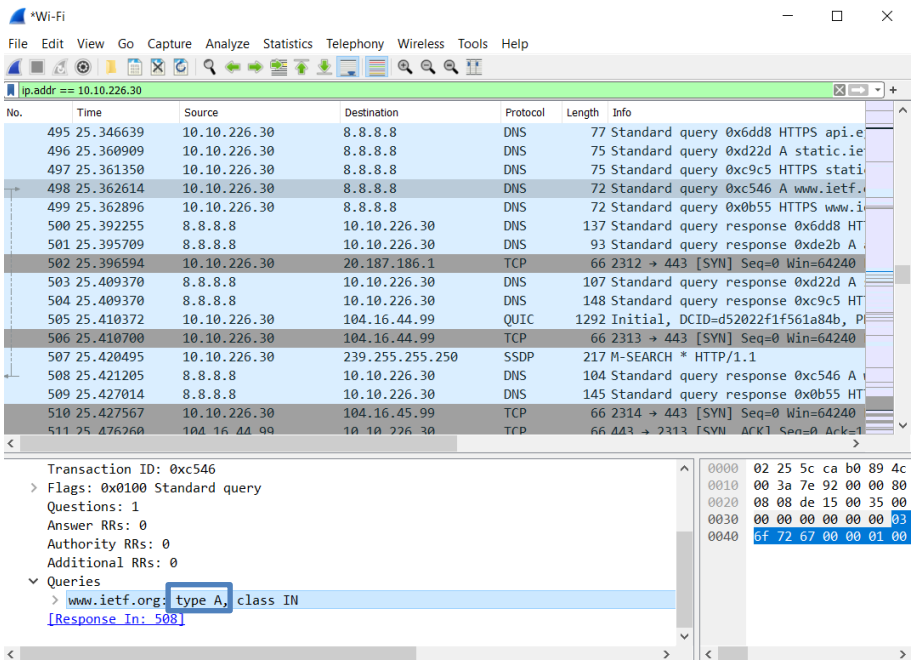
3. Yes it’s the same destination address

   The Destination Address: 8.8.8.8

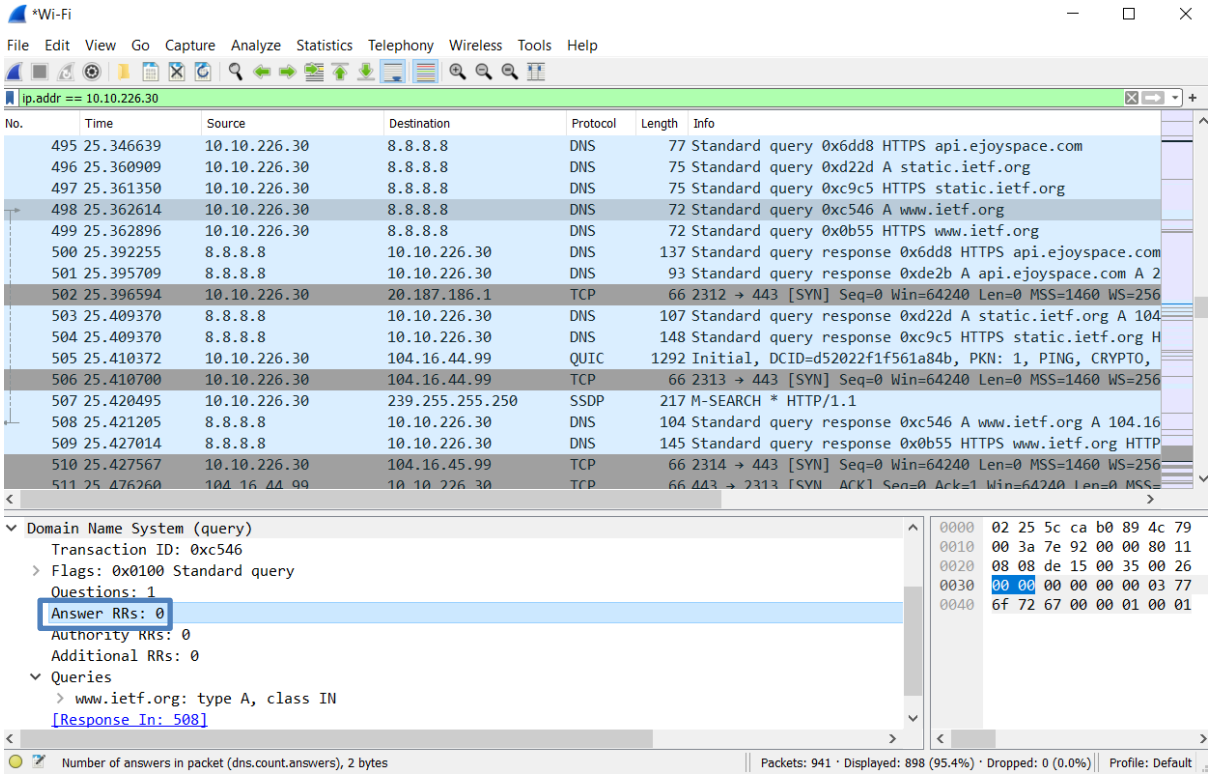

Select Command Prompt
Physical Address. . . . . : 4C-79-6E-EF-22-98
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::149e:f878:bb1d:c1c8%3
(Preferred)
IPv4 Address. . . . . : 10.10.226.30(Preferred)
Subnet Mask . . . . . : 255.255.252.0
Lease Obtained. . . . . : Saturday, November 11, 2023
4:39:00 PM
Lease Expires . . . . . : Sunday, November 12, 2023 3
:25:27 AM
Default Gateway . . . . . : 10.10.224.1
DHCP Server . . . . . : 10.10.10.23
DHCPv6 IAID . . . . . : 55343470
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-76-A8-E9-4C-
79-6E-EF-22-98
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.10.226.30
No. Time Source Destination Protocol Length Info
495 25.346639 10.10.226.30 8.8.8.8 DNS 77 Standard query 0x6dd8 HTTPS api.ejoyspace.com
496 25.360909 10.10.226.30 8.8.8.8 DNS 75 Standard query 0xd22d A static.ietf.org
497 25.361350 10.10.226.30 8.8.8.8 DNS 75 Standard query 0xc9c5 HTTPS static.ietf.org
498 25.362614 10.10.226.30 8.8.8.8 DNS 72 Standard query 0xc546 A www.ietf.org
499 25.362896 10.10.226.30 8.8.8.8 DNS 72 Standard query 0x0b55 HTTPS www.ietf.org
500 25.392255 8.8.8.8 10.10.226.30 DNS 137 Standard query response 0x6dd8 HTTPS api.ejoyspace.com SOA candy.ns.cloudflare.com
501 25.395709 8.8.8.8 10.10.226.30 DNS 93 Standard query response 0xde2b A api.ejoyspace.com A 20.187.186.1
502 25.396594 10.10.226.30 20.187.186.1 TCP 66 2312 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
503 25.409370 8.8.8.8 10.10.226.30 DNS 107 Standard query response 0xd22d A static.ietf.org A 104.16.44.99 A 104.16.45.99
504 25.409370 8.8.8.8 10.10.226.30 DNS 148 Standard query response 0xc9c5 HTTPS static.ietf.org HTTPS
505 25.410372 10.10.226.30 104.16.44.99 QUIC 1292 Initial, DCID=d52022f1f561a84b, PKN: 1, PING, CRYPTO, PING, PADDING, PING, PING, PING, PADDING, PING, PING, PING, PADDING, PING
506 25.410700 10.10.226.30 104.16.44.99 TCP 66 2313 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
507 25.420495 10.10.226.30 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
508 25.421205 8.8.8.8 10.10.226.30 DNS 104 Standard query response 0xc546 A www.ietf.org A 104.16.45.99 A 104.16.44.99
509 25.427014 8.8.8.8 10.10.226.30 DNS 145 Standard query response 0x0b55 HTTPS www.ietf.org HTTPS
510 25.427567 10.10.226.30 104.16.45.99 TCP 66 2314 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
511 25.476260 104.16.44.99 10.10.226.30 TCP 66 443 → 2313 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1386 SACK_PERM WS=8192
512 25.476337 10.10.226.30 104.16.44.99 TCP 54 2313 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
513 25.476742 10.10.226.30 104.16.44.99 TLSv1.3 621 Client Hello
514 25.508278 10.10.226.30 142.251.37.205 QUIC 79 Handshake, DCID=f26bccf5480e993d
515 25.518888 104.16.45.99 10.10.226.30 TCP 66 443 → 2314 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1386 SACK_PERM WS=8192
516 25.518168 10.10.226.30 104.16.45.99 TCP 54 2314 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
517 25.518729 10.10.226.30 104.16.45.99 TLSv1.3 586 Client Hello
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 58
Identification: 0x7e92 (32402)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: UDP (17)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.10.226.30
Destination Address: 8.8.8.8
User Datagram Protocol, Src Port: 56853, Dst Port: 53
Domain Name System (query)
0000 02 25 5c ca b0 89 4c 79 6e ef 22 98 08 00
0010 00 3a 7e 92 00 00 80 11 00 00 0a 0a e2 1e
0020 08 08 de 15 00 35 00 26 fc 6f c5 46 01 00
0030 00 00 00 00 00 00 03 77 77 77 04 69 65 74
0040 6f 72 67 00 00 01 00 01
Destination Address (ip.dst), 4 bytes
Packets: 941 · Displayed: 898 (95.4%) · Dropped: 0 (0.0%)
Profile: Default

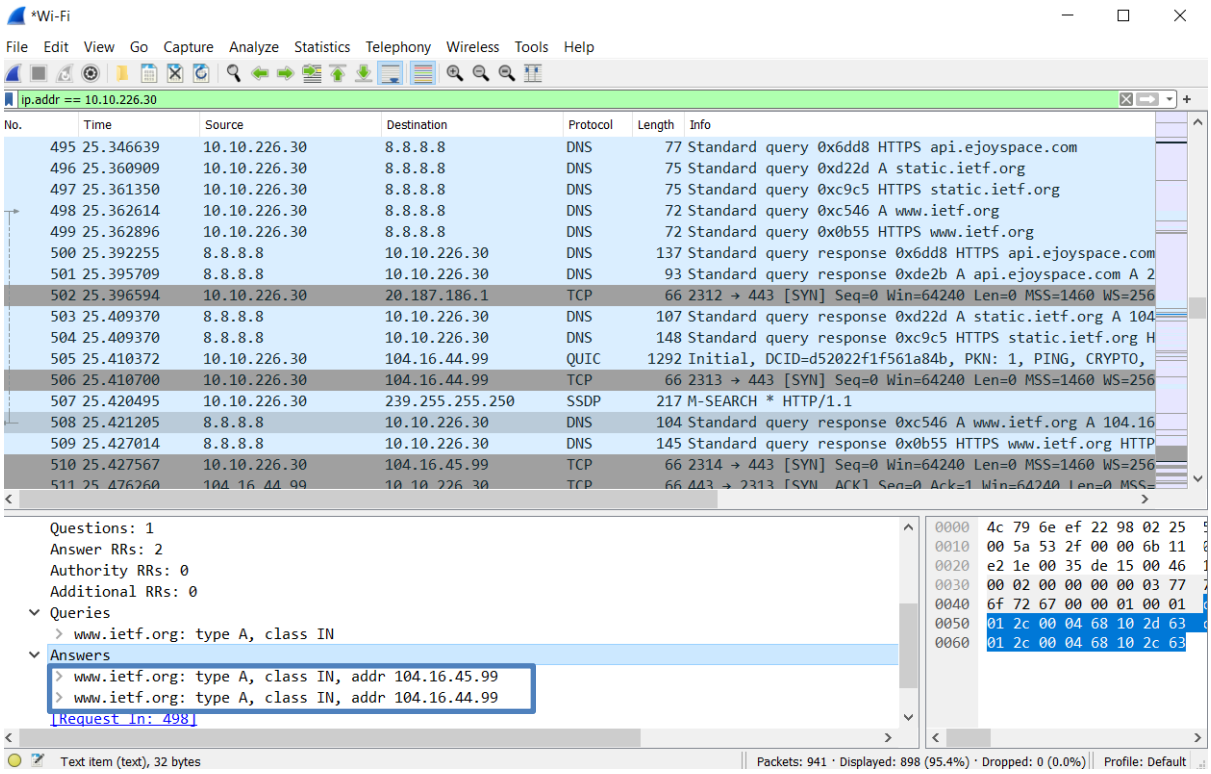
4. Type A


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 10.10.226.30
No. Time Source Destination Protocol Length Info
495 25.346639 10.10.226.30 8.8.8.8 DNS 77 Standard query 0x6dd8 HTTPS api.e
496 25.360909 10.10.226.30 8.8.8.8 DNS 75 Standard query 0xd22d A static.ie
497 25.361350 10.10.226.30 8.8.8.8 DNS 75 Standard query 0xc9c5 HTTPS stati
498 25.362614 10.10.226.30 8.8.8.8 DNS 72 Standard query 0xc546 A www.ietf.
499 25.362896 10.10.226.30 8.8.8.8 DNS 72 Standard query 0x0b55 HTTPS www.i
500 25.392255 8.8.8.8 10.10.226.30 DNS 137 Standard query response 0x6dd8 HT
501 25.395709 8.8.8.8 10.10.226.30 DNS 93 Standard query response 0xde2b A
502 25.396594 10.10.226.30 20.187.186.1 TCP 66 2312 → 443 [SYN] Seq=0 Win=64240
503 25.409370 8.8.8.8 10.10.226.30 DNS 107 Standard query response 0xd22d A
504 25.409370 8.8.8.8 10.10.226.30 DNS 148 Standard query response 0xc9c5 HT
505 25.410372 10.10.226.30 104.16.44.99 QUIC 1292 Initial, DCID=d52022f1f561a84b, P
506 25.410700 10.10.226.30 104.16.44.99 TCP 66 2313 → 443 [SYN] Seq=0 Win=64240
507 25.420495 10.10.226.30 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
508 25.421205 8.8.8.8 10.10.226.30 DNS 104 Standard query response 0xc546 A
509 25.427014 8.8.8.8 10.10.226.30 DNS 145 Standard query response 0x0b55 HT
510 25.427567 10.10.226.30 104.16.45.99 TCP 66 2314 → 443 [SYN] Seq=0 Win=64240
Transaction ID: 0xc546
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.ietf.org: type A, class IN
[Response In: 508]
0000 02 25 5c ca b0 89 4c
0010 00 3a 7e 92 00 00 80
0020 08 08 de 15 00 35 00
0030 00 00 00 00 00 00 03
0040 6f 72 67 00 00 01 00

Zero answers



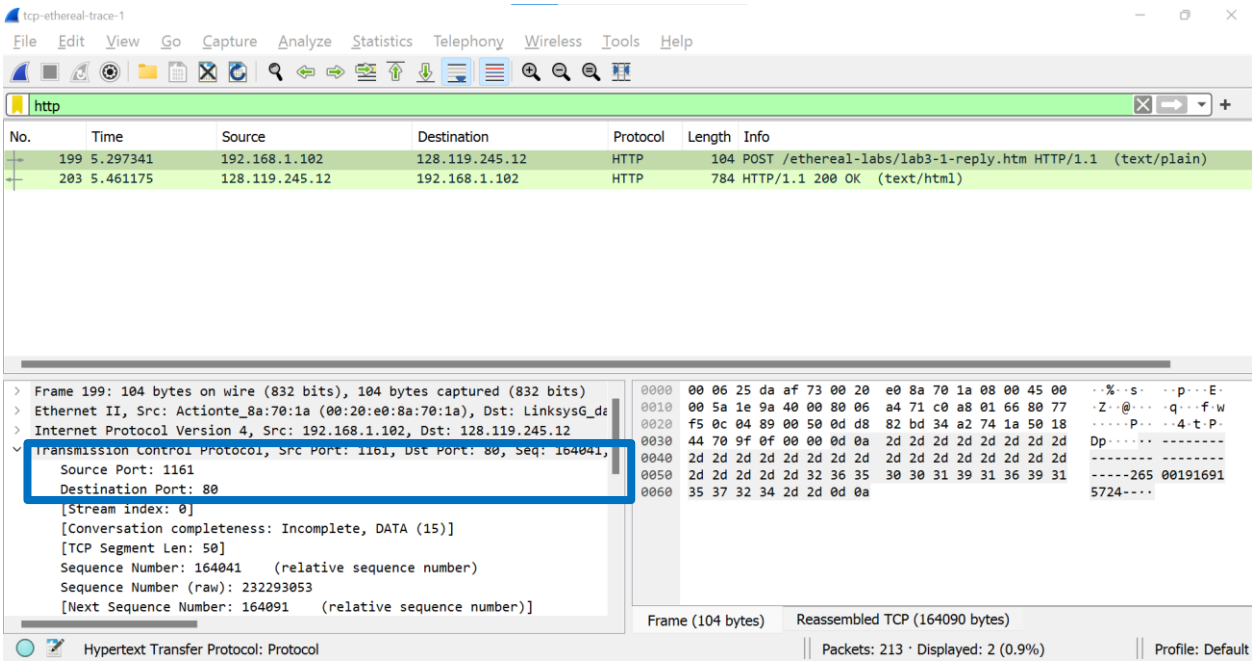
5. 2 answers



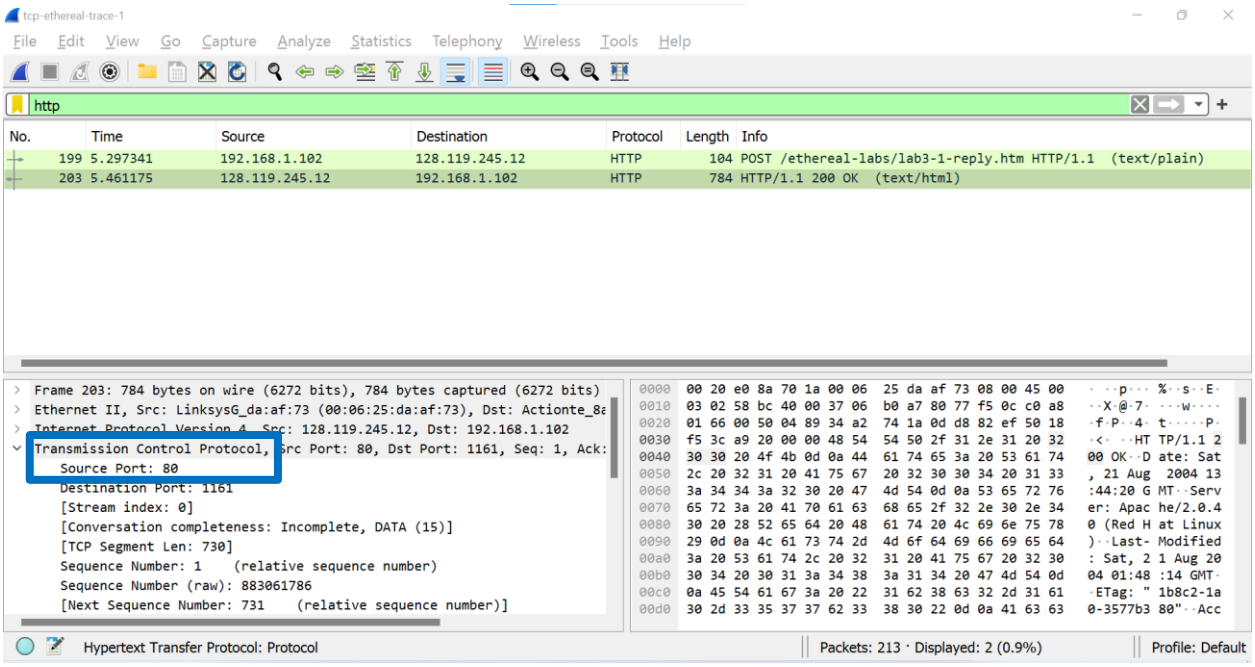
---

3. TCP protocol:

1-

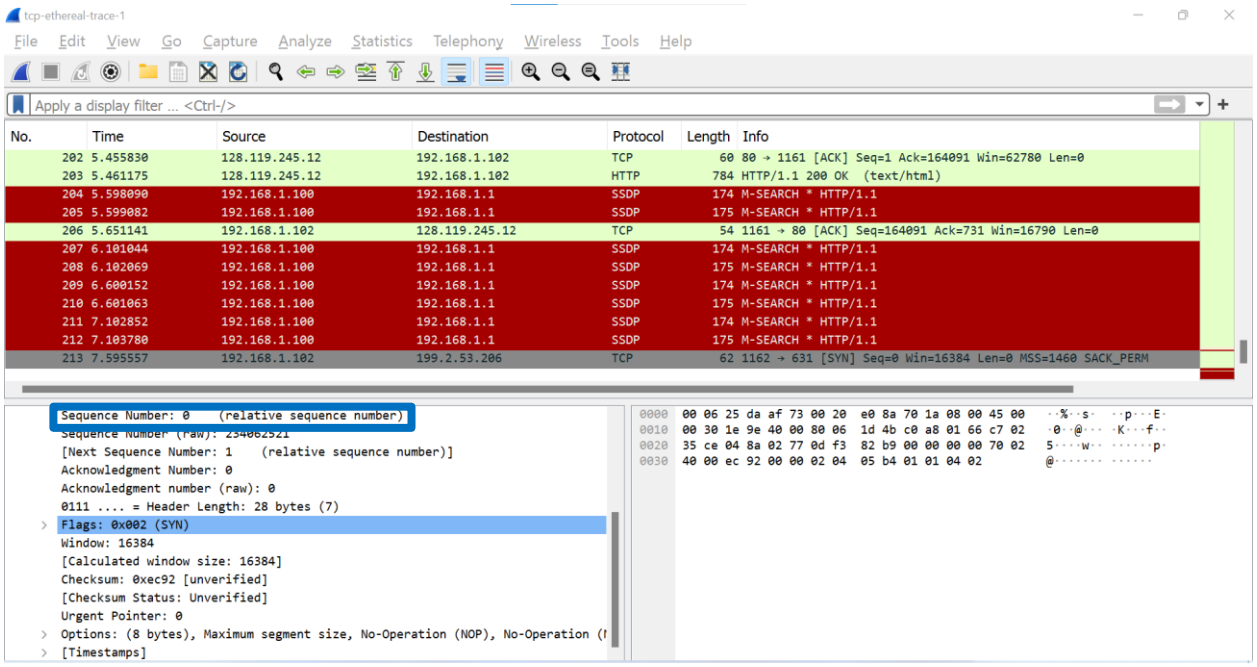


2-

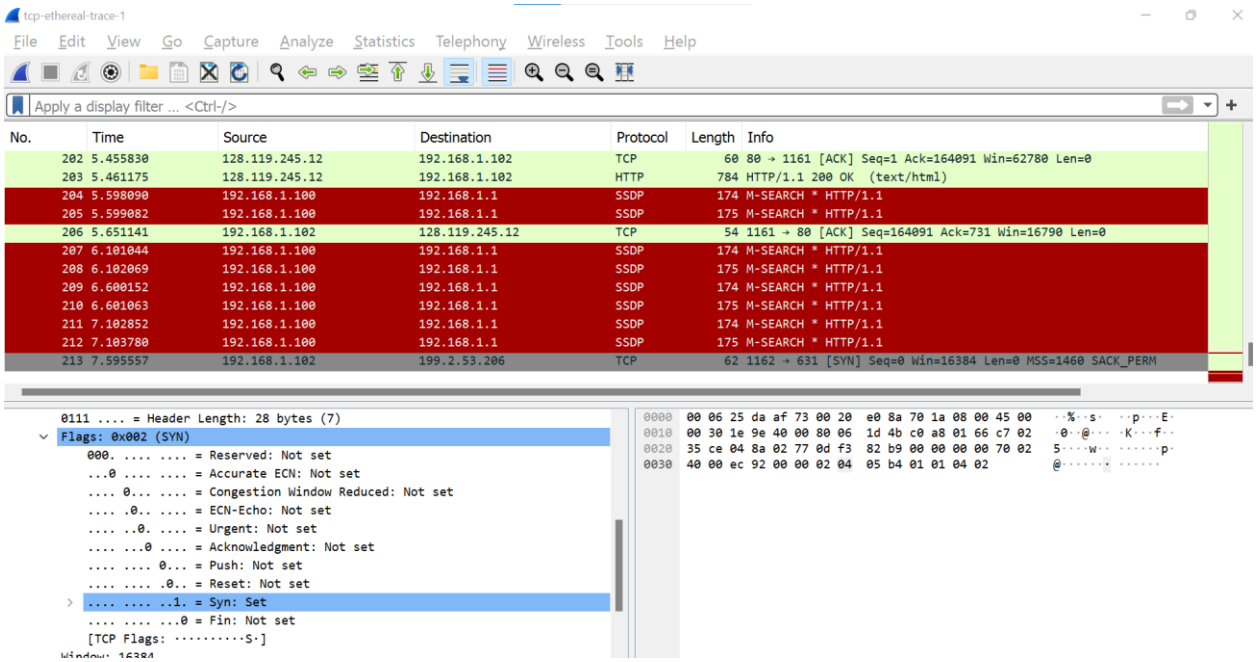


3-

- **Sequence number**

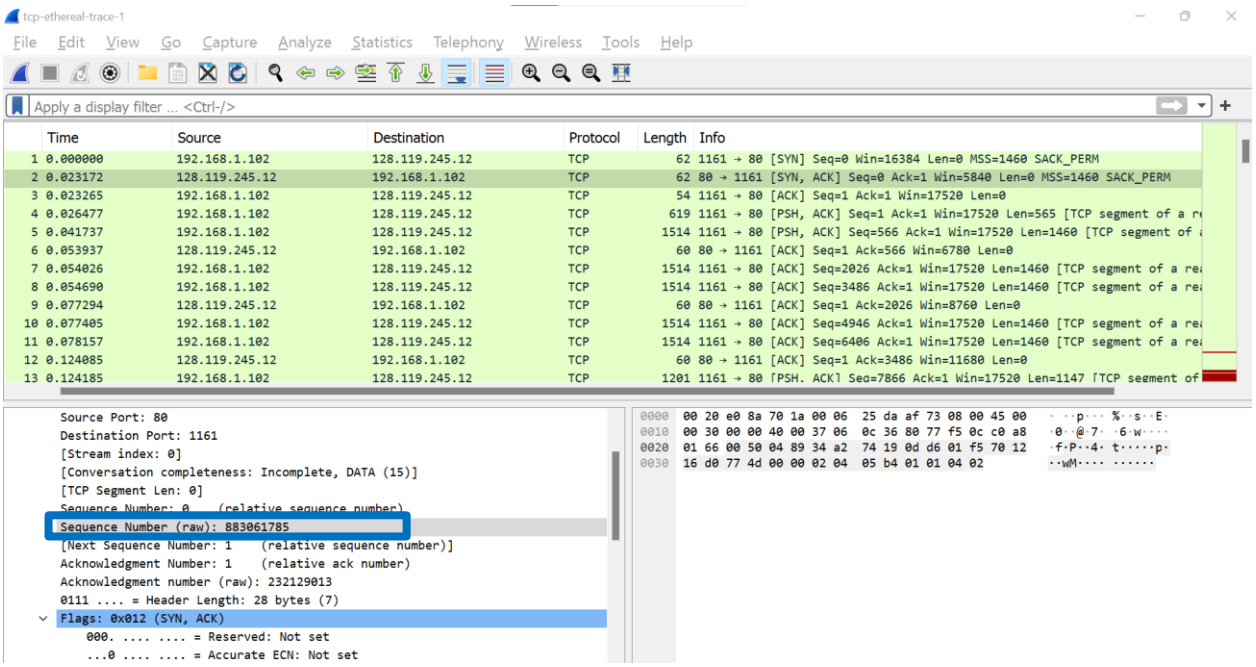


SYN flag is set, then it is SYN

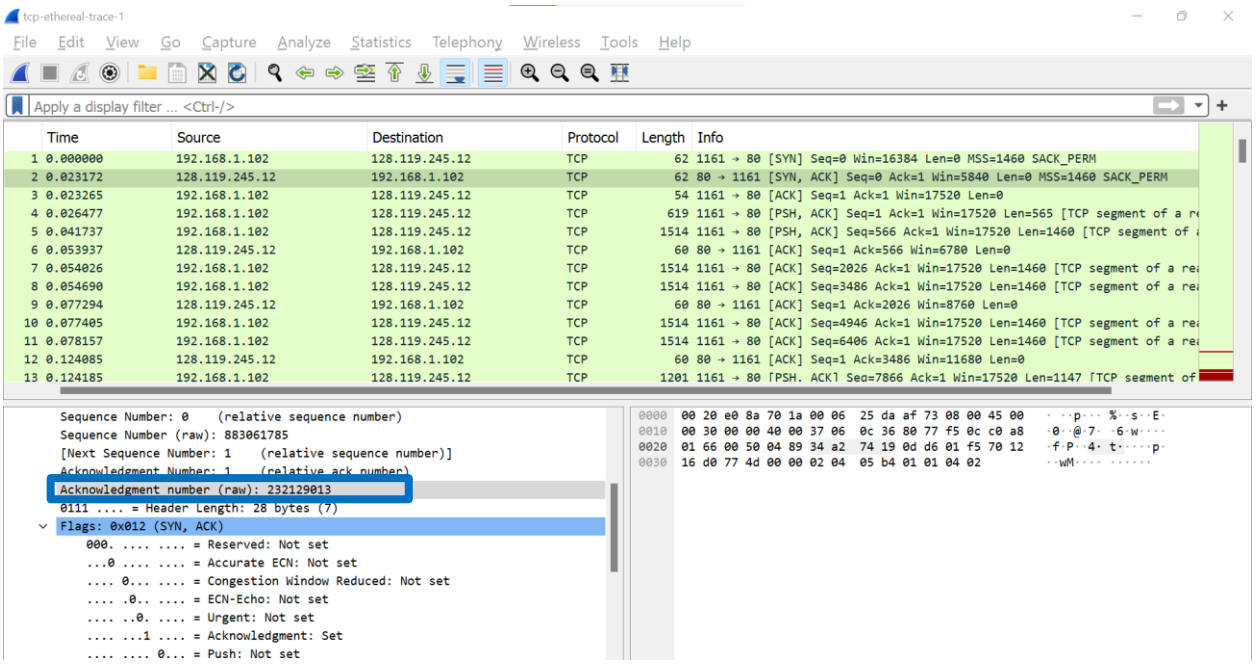


4-

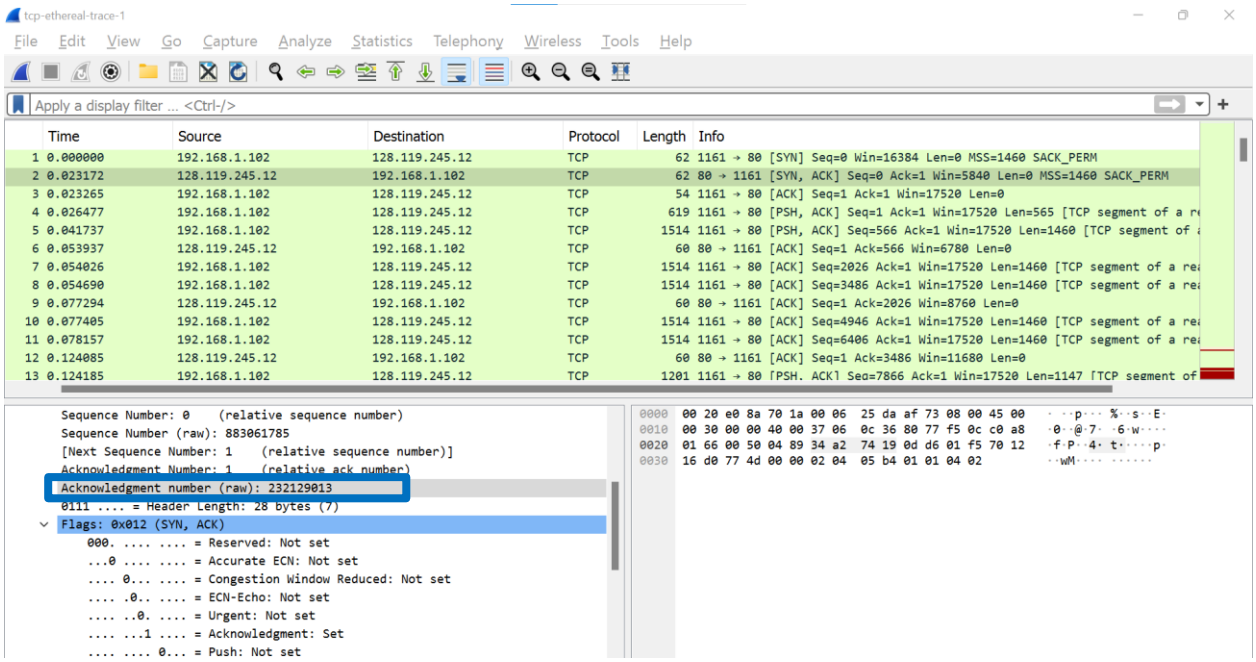
Sequence number



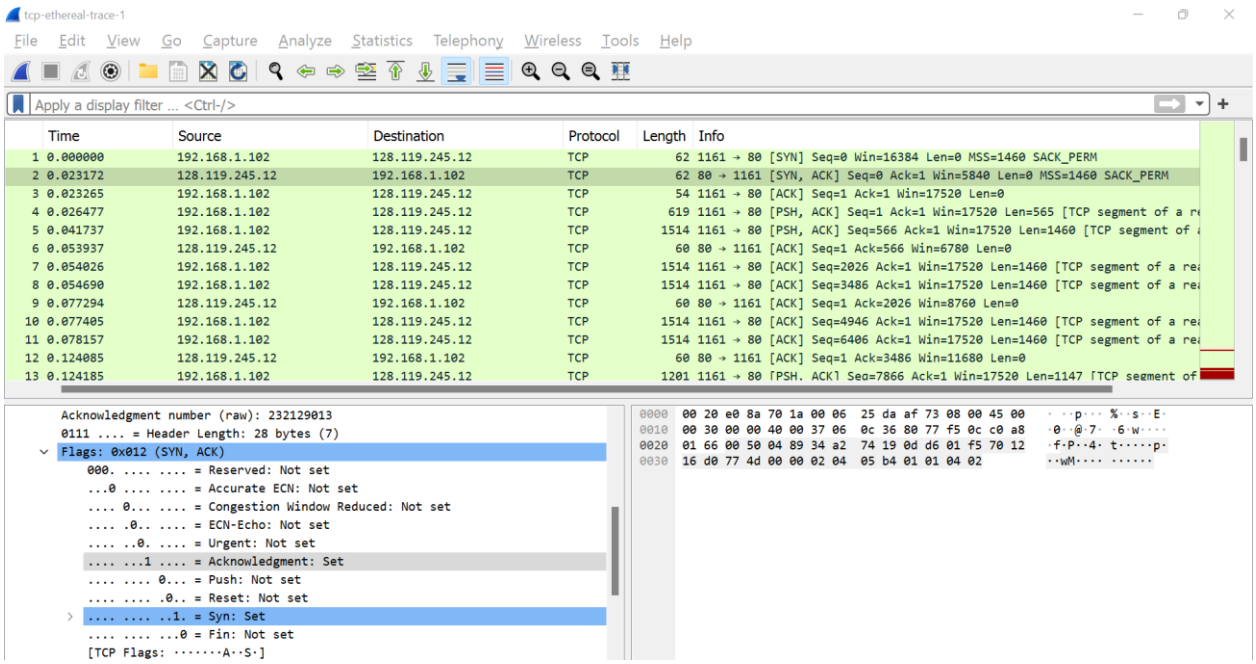
ACK Value



ACK Value for SYN + ACK = Sequence number of the next ACK segment

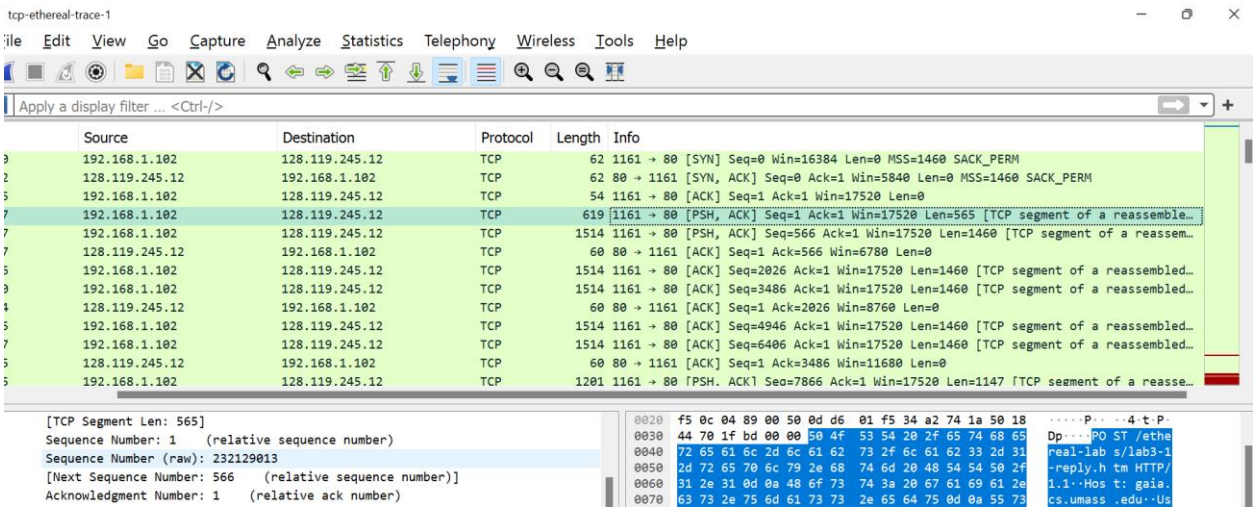


SYN and ACK both flags are set.

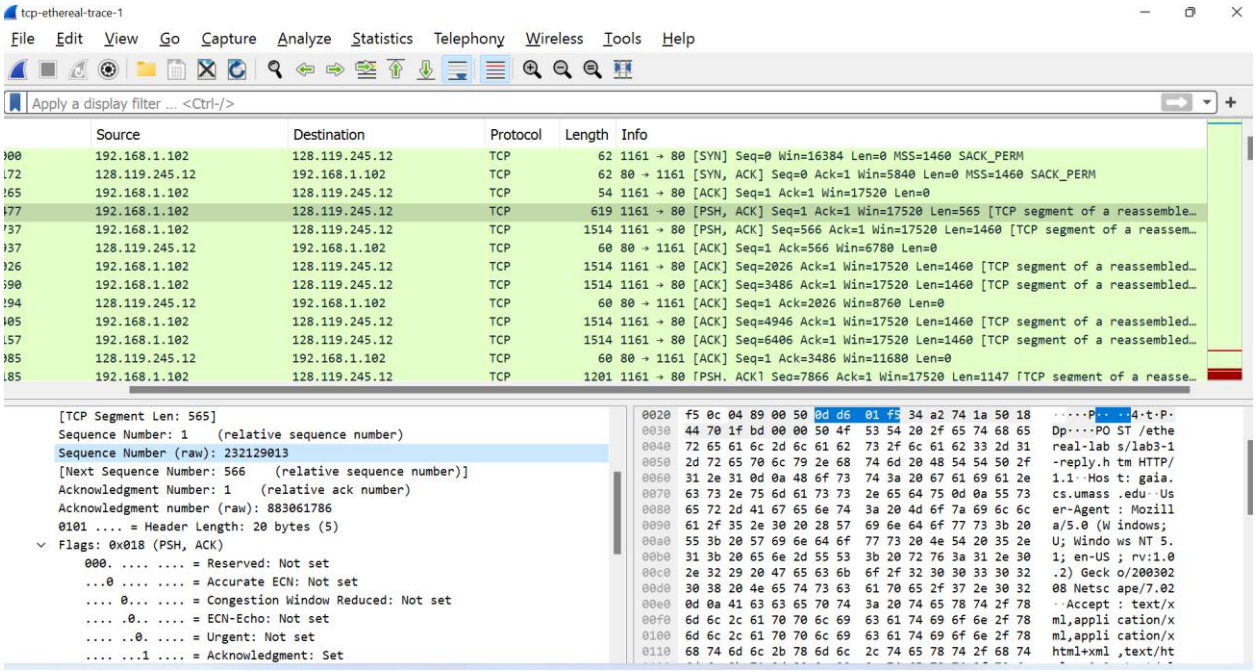


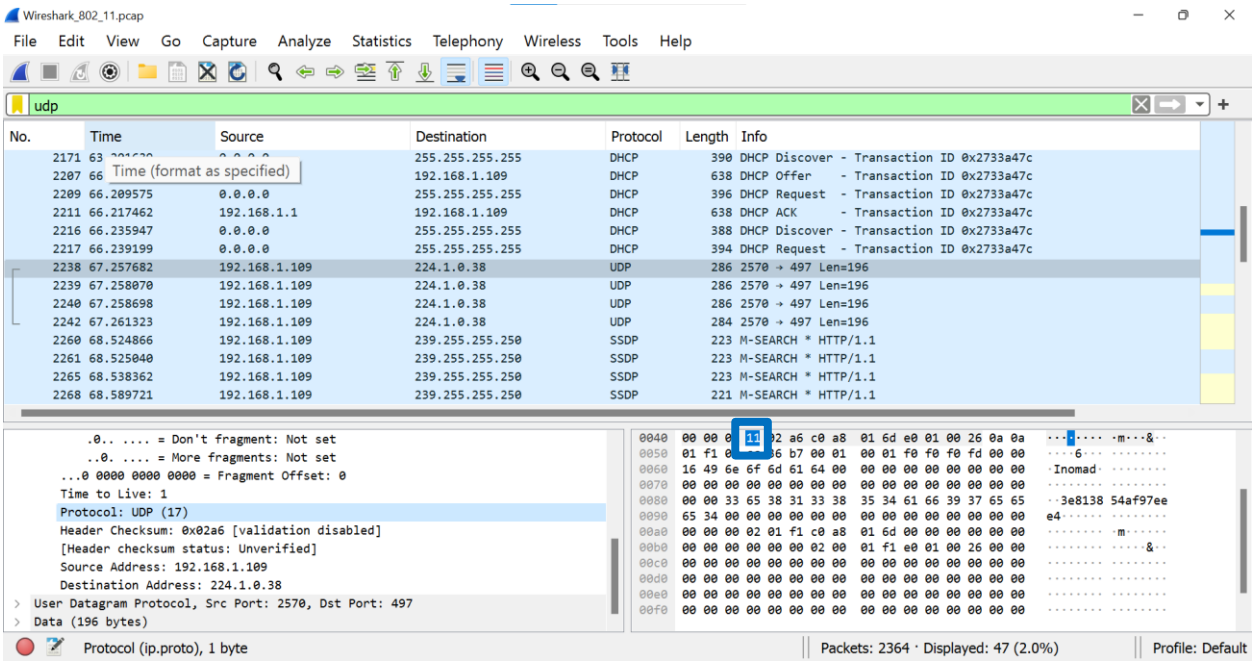
5-

POST



Sequence number





6. **Segment length: 667, 1448, 1448, 1448, 1448, 1448**
7. **TCP segment is 1 byte**

The last segment is 164091 bytes

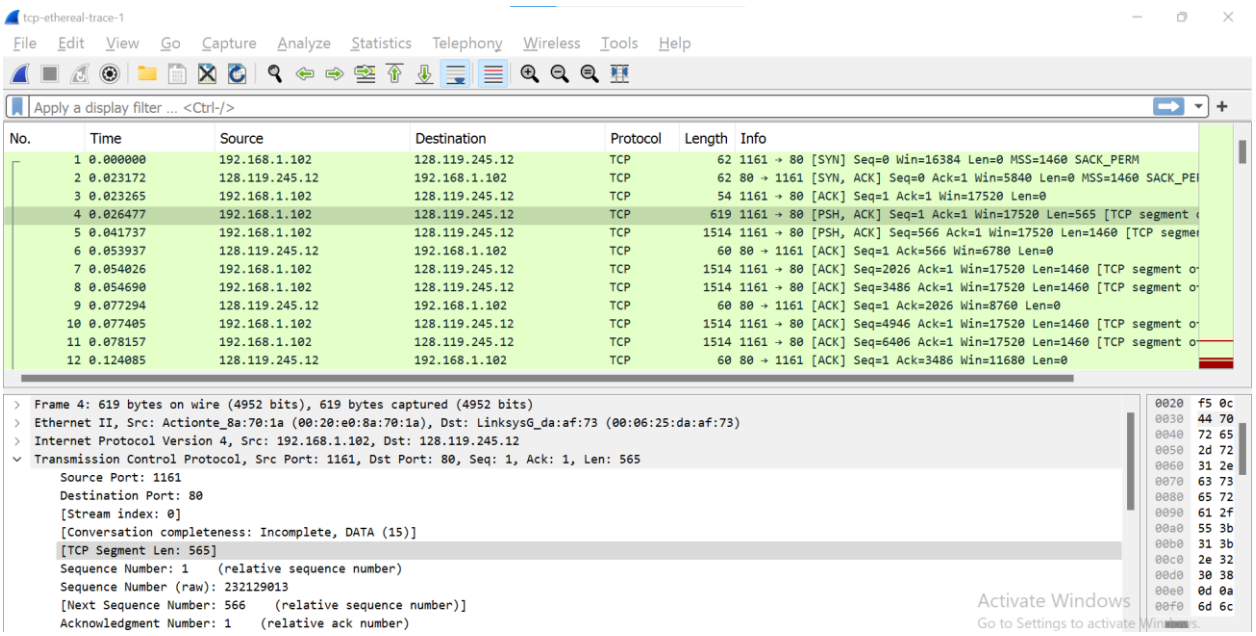
Total data =164091 - 1 = 164090 bytes

Transmission time for first segment = 0.026477 seconds

Transmission time for last segment = 5.455830 seconds

difference = 5.455830 - 0.026477 = 5.4294

The throughput = 164090 / 5.4294 = 30,222.49235642981

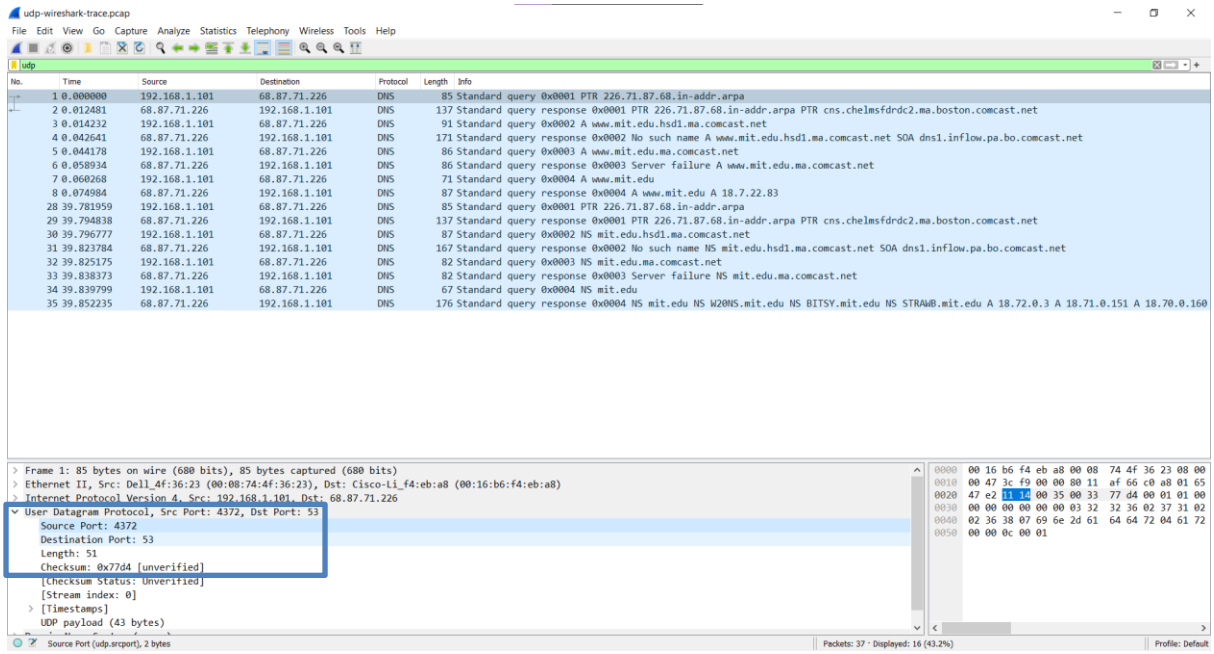


---

4. UDP protocol:

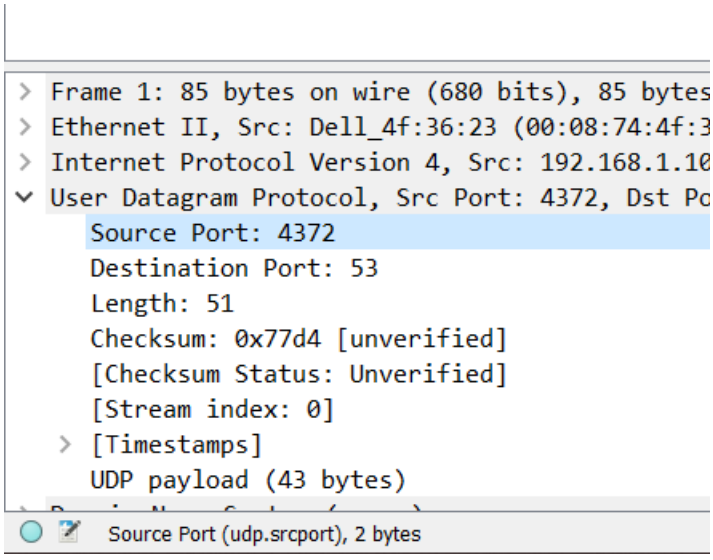
1. 4 header fields

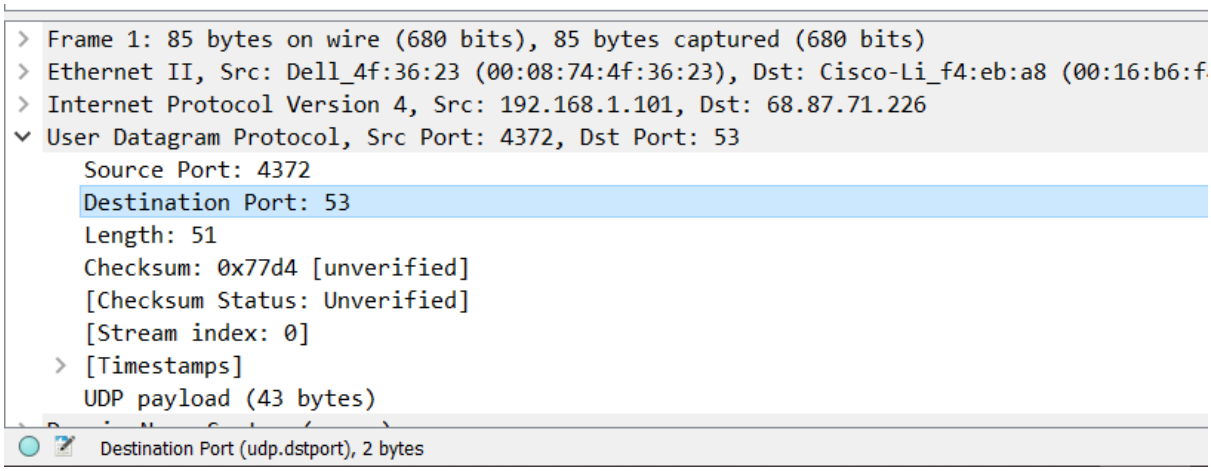
   Source port & Destination port & Length and Checksum.

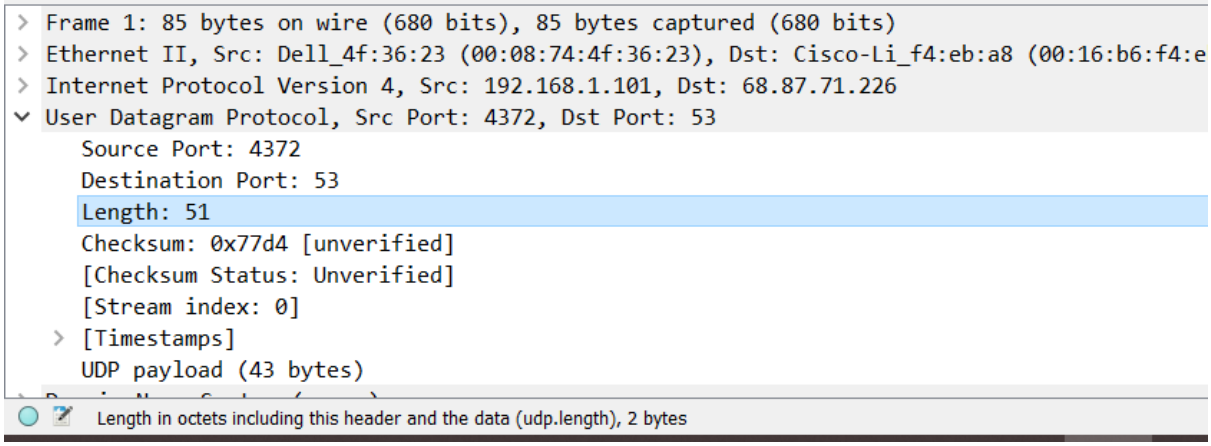


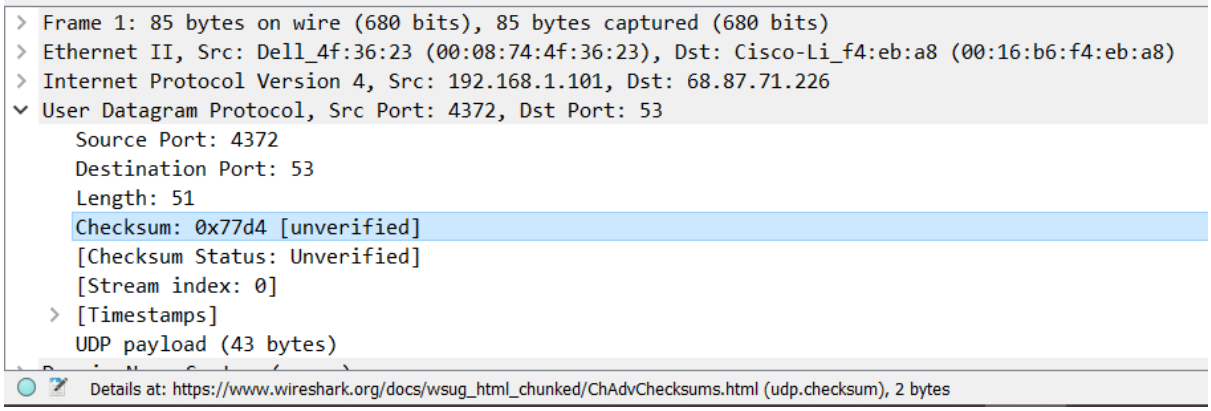
2. Length of header fields in bytes:

   They’re all 2 bytes.





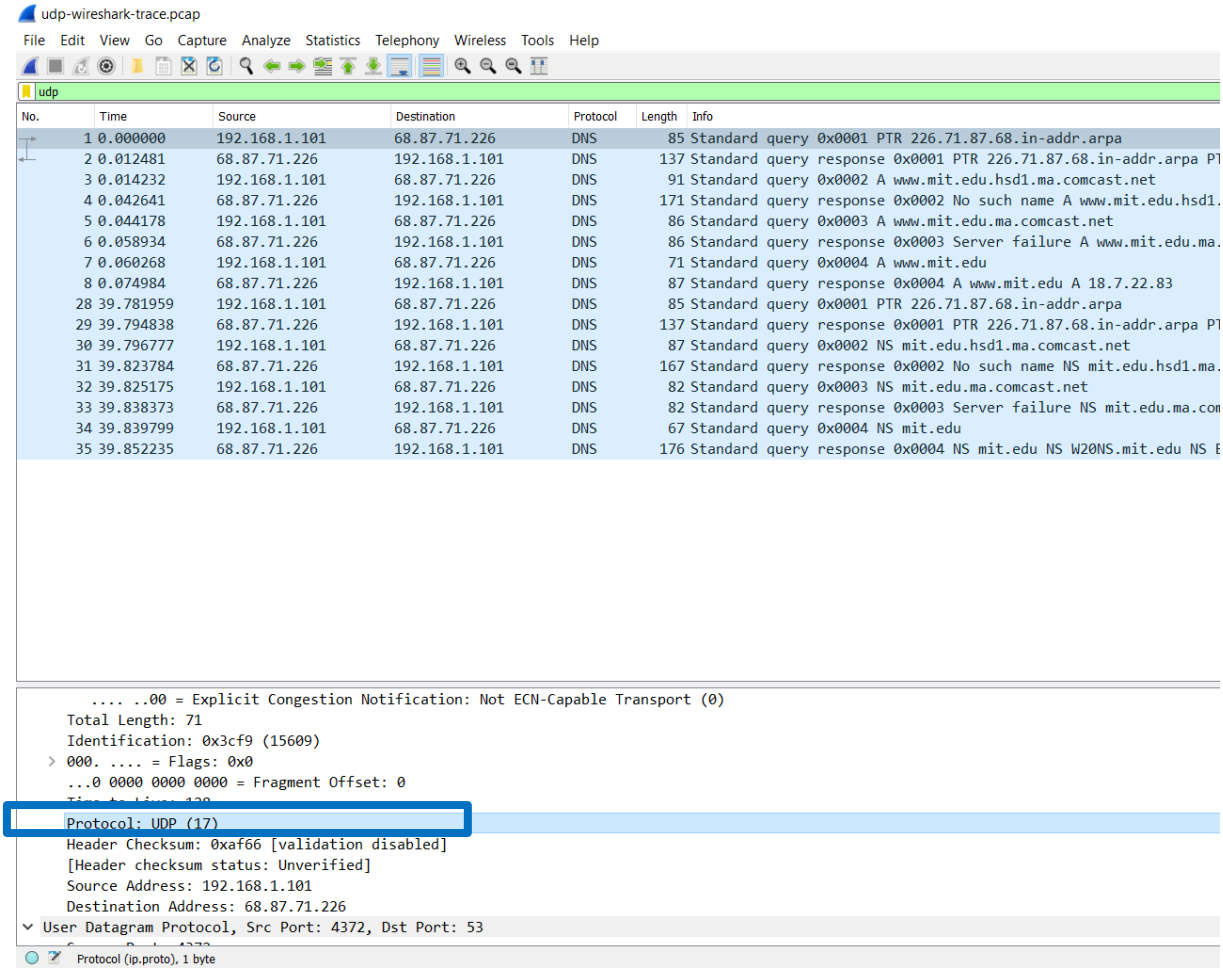




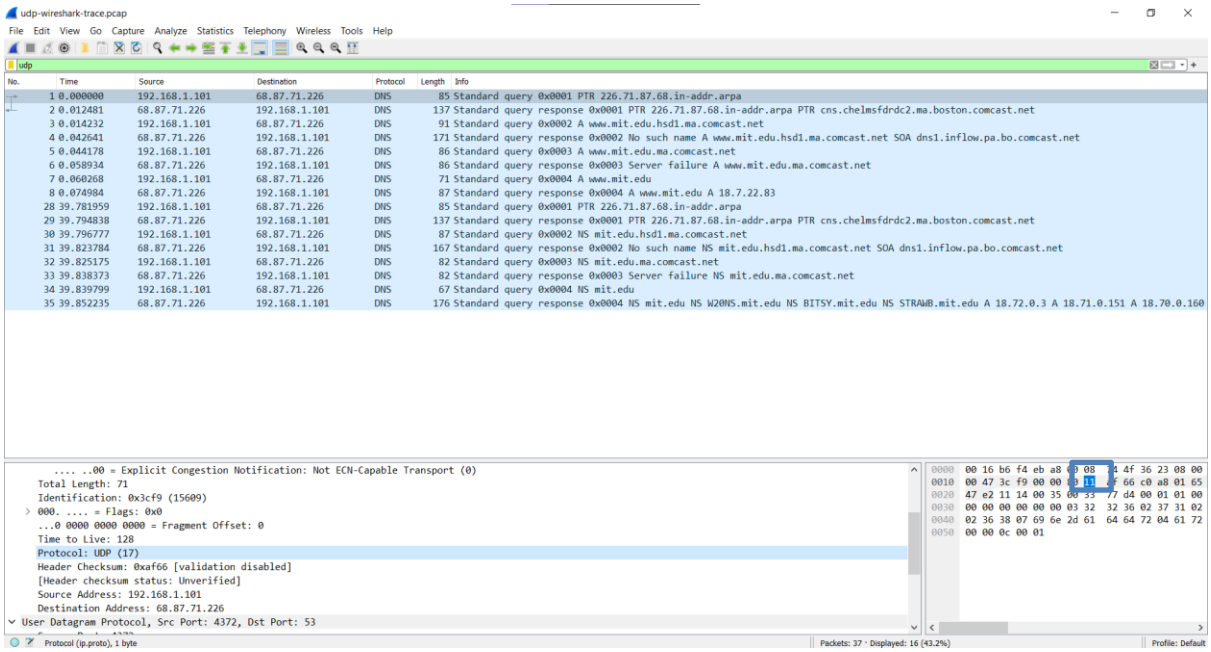
The value in the length field is: the sum of the 8 header bytes: 4*2=8 header bytes.

3. In this case, (2^ 16 -1) = 65535 is the largest source port number that can exist.
   There are 8 bytes in the header. Thus, 65535 – 8 = 65527 bytes is the maximum number of bytes that can be included in a UDP payload.
4. The largest possible source port number is (2 ^ 16 -1) = 65535

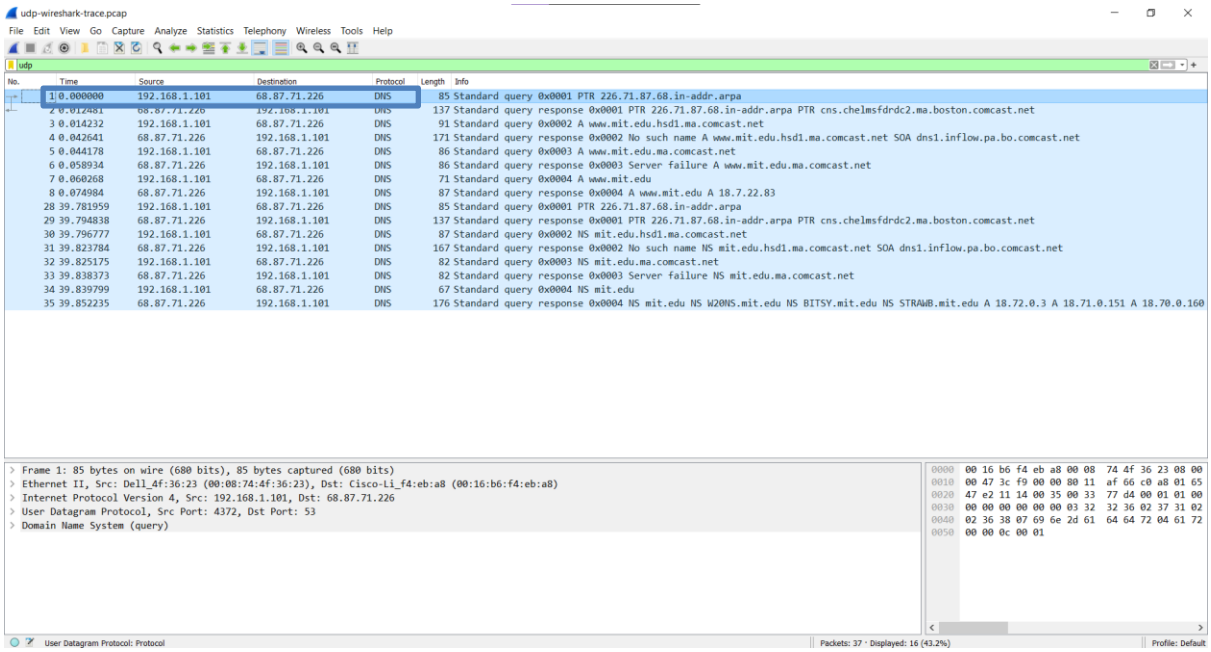
5. **Decimal 17**



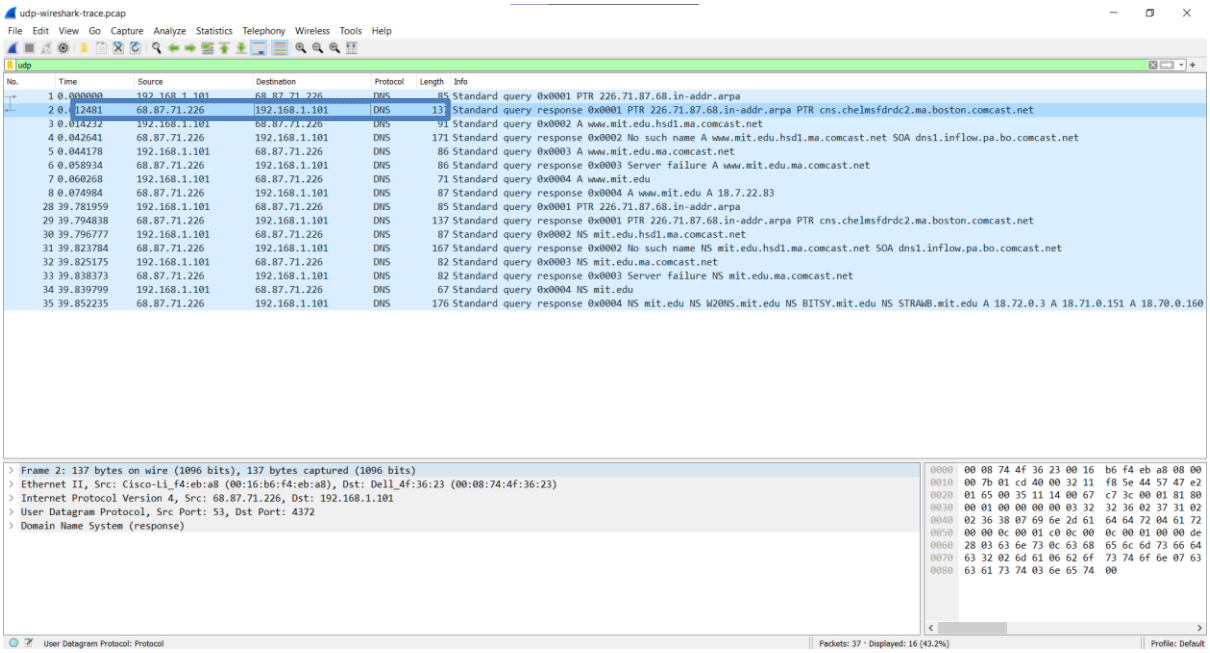
Hexadecimal 11



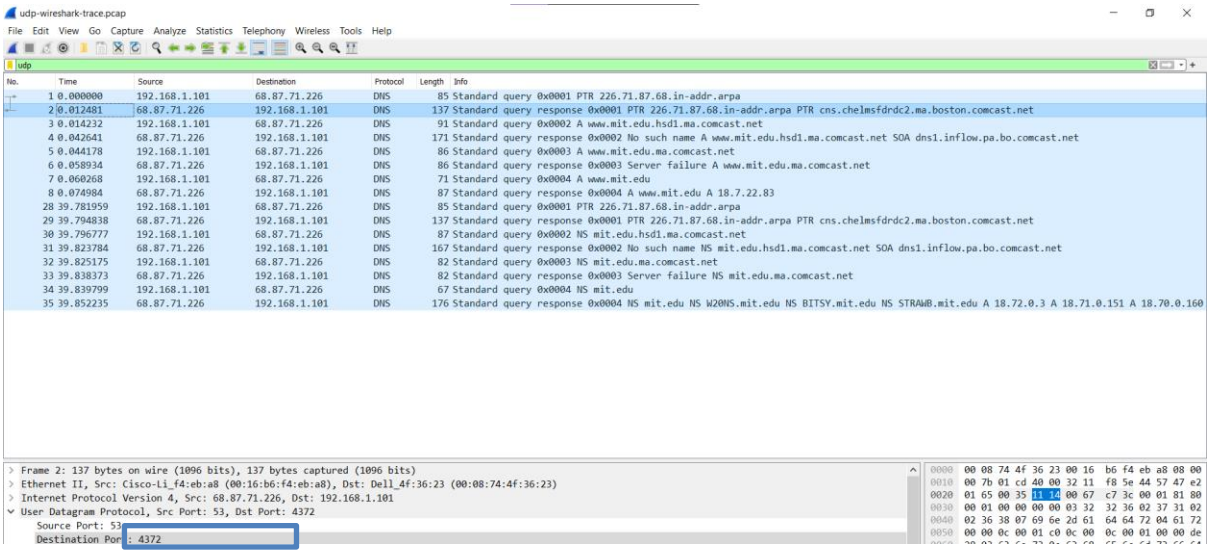
6. Send packet



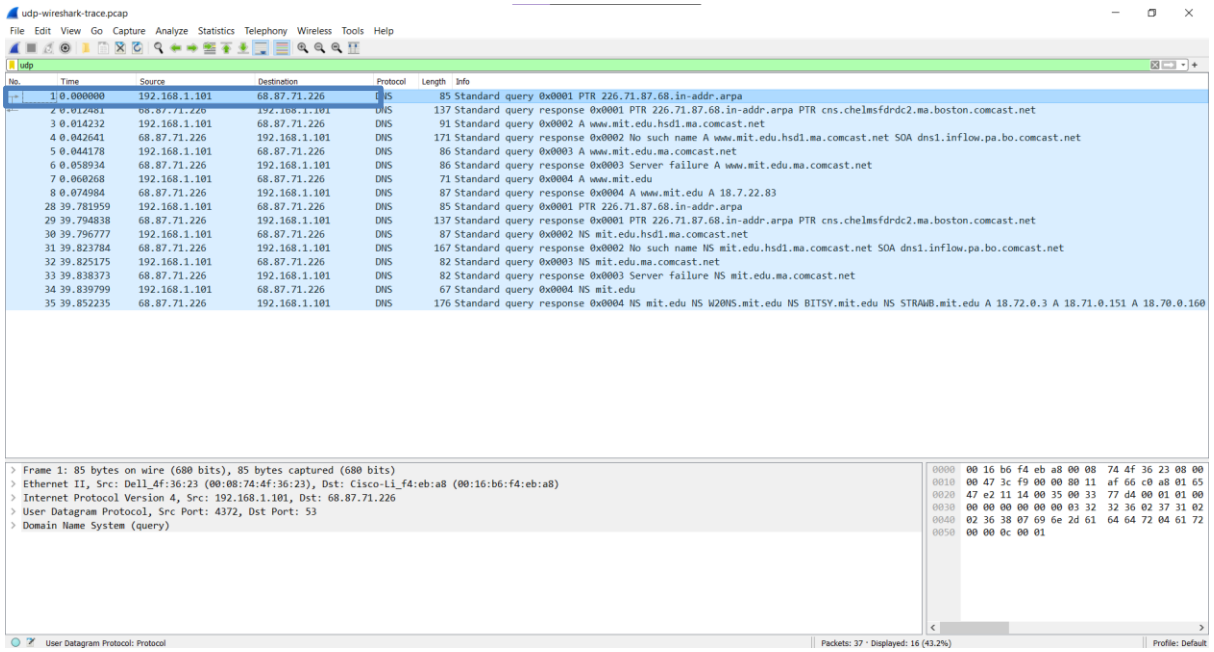
Reply packet



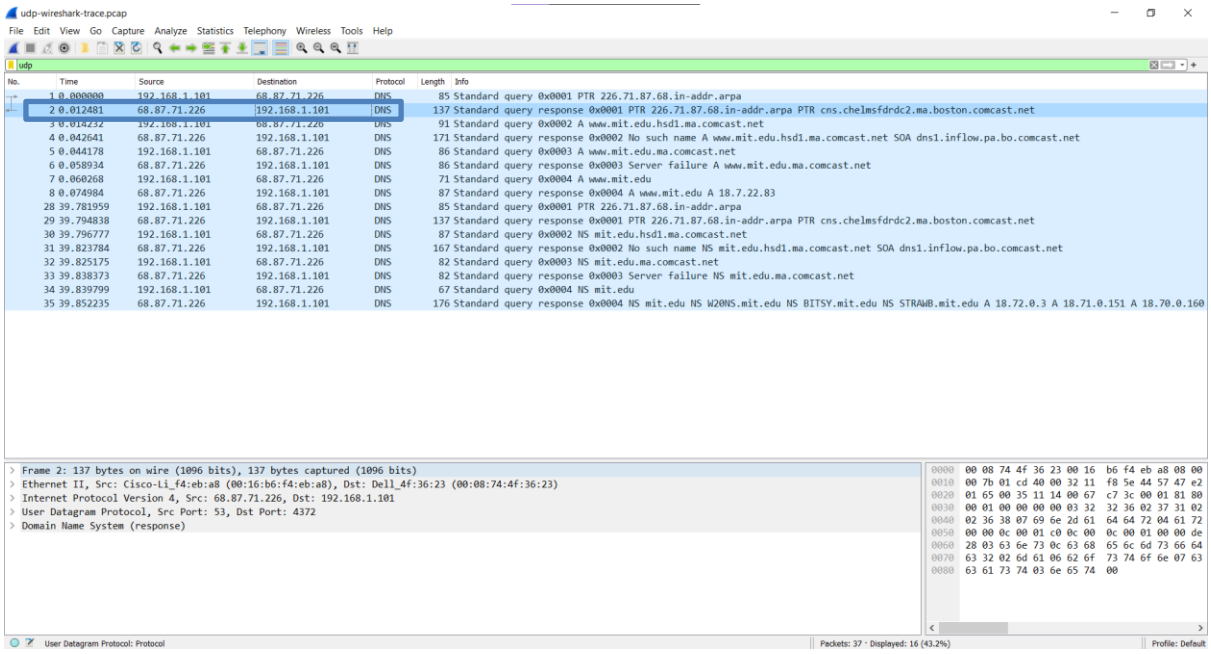
Reply destination port the same as sending source port

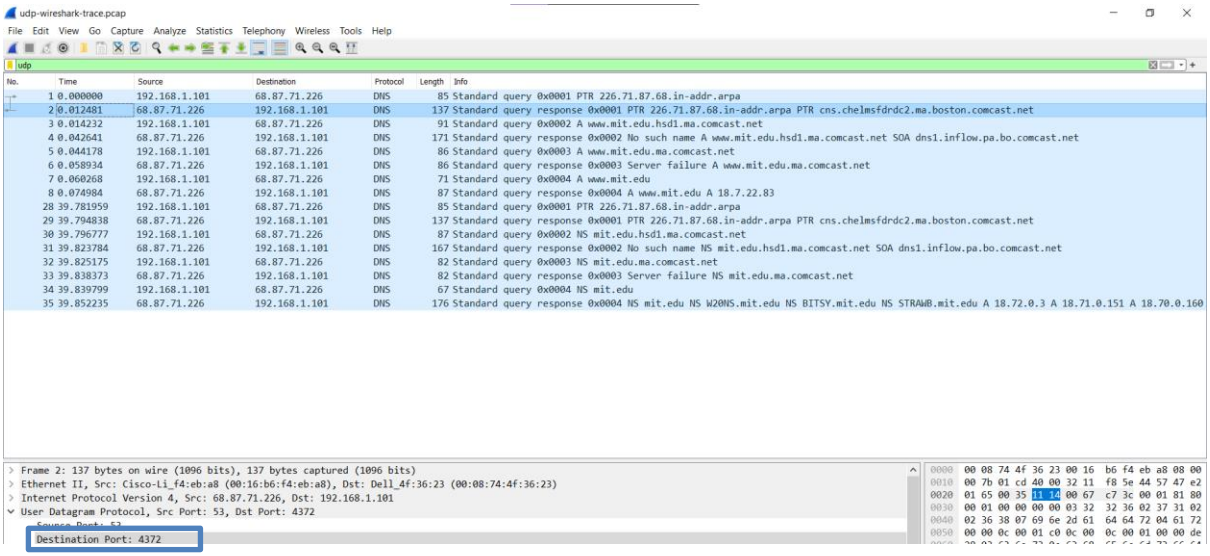


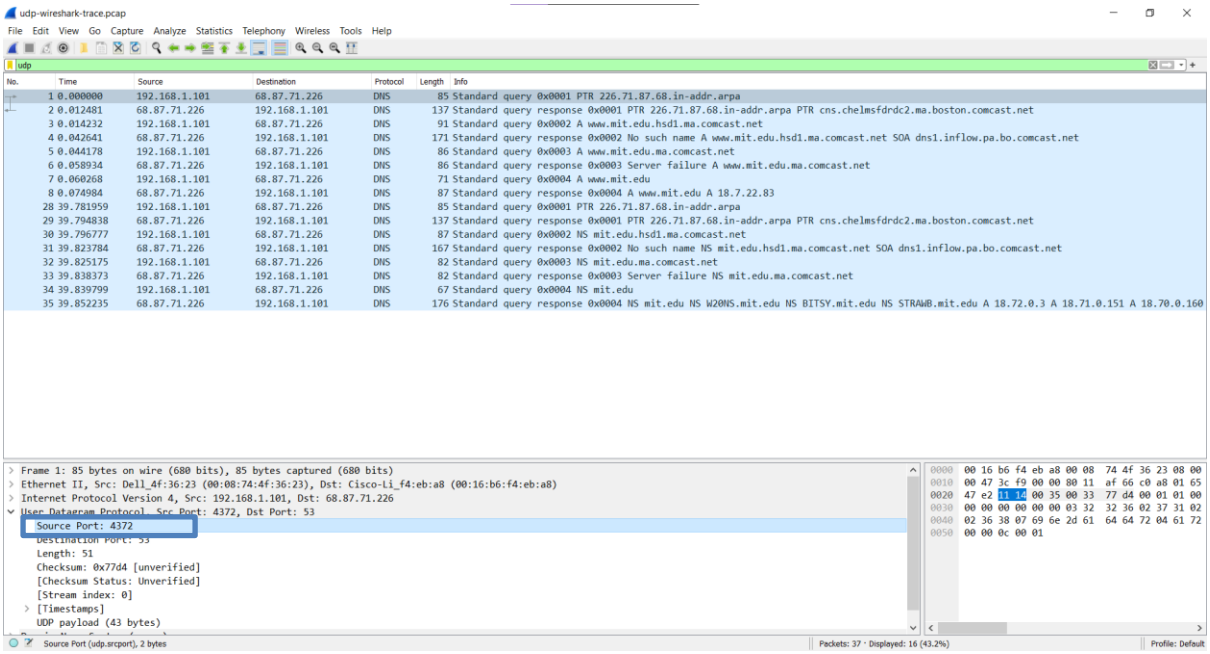
Send packet



Reply packet




udp-wireshark-trace.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.101 68.87.71.226 DNS 85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2 0.012481 68.87.71.226 192.168.1.101 DNS 137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
3 0.014232 192.168.1.101 68.87.71.226 DNS 91 Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4 0.042641 68.87.71.226 192.168.1.101 DNS 171 Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5 0.044178 192.168.1.101 68.87.71.226 DNS 86 Standard query 0x0003 A www.mit.edu.ma.comcast.net
6 0.058934 68.87.71.226 192.168.1.101 DNS 86 Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7 0.060268 192.168.1.101 68.87.71.226 DNS 71 Standard query 0x0004 A www.mit.edu
8 0.074984 68.87.71.226 192.168.1.101 DNS 87 Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28 39.781959 192.168.1.101 68.87.71.226 DNS 85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29 39.794838 68.87.71.226 192.168.1.101 DNS 137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
30 39.796777 192.168.1.101 68.87.71.226 DNS 87 Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31 39.823784 68.87.71.226 192.168.1.101 DNS 167 Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32 39.825175 192.168.1.101 68.87.71.226 DNS 82 Standard query 0x0003 NS mit.edu.ma.comcast.net
33 39.838373 68.87.71.226 192.168.1.101 DNS 82 Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34 39.839799 192.168.1.101 68.87.71.226 DNS 67 Standard query 0x0004 NS mit.edu
35 39.852235 68.87.71.226 192.168.1.101 DNS 176 Standard query response 0x0004 NS mit.edu NS W20NS.mit.edu NS BITSY.mit.edu NS STRAWB.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160
Frame 2: 137 bytes on wire (1096 bits), 137 bytes captured (1096 bits)
Ethernet II, Src: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
Internet Protocol Version 4, Src: 68.87.71.226, Dst: 192.168.1.101
User Datagram Protocol, Src Port: 53, Dst Port: 4372
Destination Port: 4372
0000 00 08 74 4f 36 23 00 16 b6 f4 eb a8 08 00
0010 00 7b 01 cd 40 00 32 11 f8 5e 44 57 47 e2
0020 01 65 00 35 11 14 00 67 c7 3c 00 01 81 80
0030 00 01 00 00 00 00 03 32 32 36 02 37 31 02
0040 02 36 38 07 69 6e 2d 61 64 64 72 04 61 72
0050 00 00 0c 00 01 c0 0c 00 0c 00 01 00 00 de


udp-wireshark-trace.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.101 68.87.71.226 DNS 85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
2 0.012481 68.87.71.226 192.168.1.101 DNS 137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
3 0.014232 192.168.1.101 68.87.71.226 DNS 91 Standard query 0x0002 A www.mit.edu.hsd1.ma.comcast.net
4 0.042641 68.87.71.226 192.168.1.101 DNS 171 Standard query response 0x0002 No such name A www.mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
5 0.044178 192.168.1.101 68.87.71.226 DNS 86 Standard query 0x0003 A www.mit.edu.ma.comcast.net
6 0.058934 68.87.71.226 192.168.1.101 DNS 86 Standard query response 0x0003 Server failure A www.mit.edu.ma.comcast.net
7 0.060268 192.168.1.101 68.87.71.226 DNS 71 Standard query 0x0004 A www.mit.edu
8 0.074984 68.87.71.226 192.168.1.101 DNS 87 Standard query response 0x0004 A www.mit.edu A 18.7.22.83
28 39.781959 192.168.1.101 68.87.71.226 DNS 85 Standard query 0x0001 PTR 226.71.87.68.in-addr.arpa
29 39.794838 68.87.71.226 192.168.1.101 DNS 137 Standard query response 0x0001 PTR 226.71.87.68.in-addr.arpa PTR cns.chelmsfdrdc2.ma.boston.comcast.net
30 39.796777 192.168.1.101 68.87.71.226 DNS 87 Standard query 0x0002 NS mit.edu.hsd1.ma.comcast.net
31 39.823784 68.87.71.226 192.168.1.101 DNS 167 Standard query response 0x0002 No such name NS mit.edu.hsd1.ma.comcast.net SOA dns1.inflow.pa.bo.comcast.net
32 39.825175 192.168.1.101 68.87.71.226 DNS 82 Standard query 0x0003 NS mit.edu.ma.comcast.net
33 39.838373 68.87.71.226 192.168.1.101 DNS 82 Standard query response 0x0003 Server failure NS mit.edu.ma.comcast.net
34 39.839799 192.168.1.101 68.87.71.226 DNS 67 Standard query 0x0004 NS mit.edu
35 39.852235 68.87.71.226 192.168.1.101 DNS 176 Standard query response 0x0004 NS mit.edu NS W20NS.mit.edu NS BITSY.mit.edu NS STRAWB.mit.edu A 18.72.0.3 A 18.71.0.151 A 18.70.0.160
Frame 1: 85 bytes on wire (680 bits), 85 bytes captured (680 bits)
Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 68.87.71.226
User Datagram Protocol, Src Port: 4372, Dst Port: 53
Source Port: 4372
Length: 51
Checksum: 0x77d4 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (43 bytes)
0000 00 16 b6 f4 eb a8 00 08 74 4f 36 23 08 00
0010 00 47 3c f9 00 00 80 11 af 66 c0 a8 01 65
0020 47 e2 11 14 00 35 00 33 77 d4 00 01 01 00
0030 00 00 00 00 00 00 03 32 32 36 02 37 31 02
0040 02 36 38 07 69 6e 2d 61 64 64 72 04 61 72
0050 00 00 0c 00 01
Source Port (udp.srcport), 2 bytes
Packets: 37 · Displayed: 16 (43.2%)
Profile: Default