Zeynepnur ŞAHİNEL
2305399 30.05.2022

EE444 Introduction to Computer Networks

HW2 - Wireshark

Part 1 - Getting Familiar with Wireshark

Q.1.1)

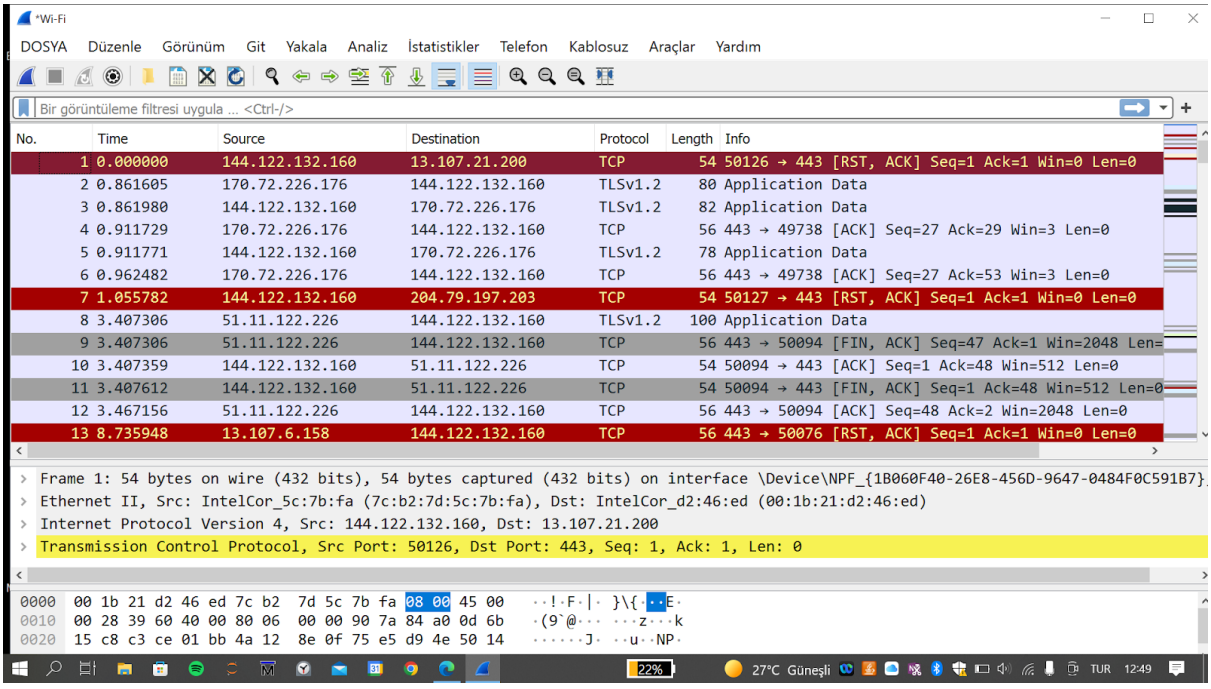


Figure 1. A screen view of Wireshark

TCP: Transmission Control Protocol

TLSv1.2: Transport Layer Security version 1.2 Protocol

ARP: Address Resolution Protocol

DNS: Domain Name System

DHCPv6: Dynamic Host Configuration Protocol version 6

UDP: User Datagram Protocol

HTTP: Hyper Text Transfer Protocol

Zeynepnur ŞAHİNEL
2305399

Part 2 - HTTP, TCP, DNS

Q.2.1)

HTTP is a web application layer protocol. Here, my computer is a client and it tries to establish a contact with the Metu server to view the image object. In this process, HTTP (HyperText Transfer Protocol) is used to communicate. From Fig 2, it can be seen that my computer (144.122.132.160) makes a request with the GET command and the server (144.122.145.144) responds with a status code.

Q.2.2)

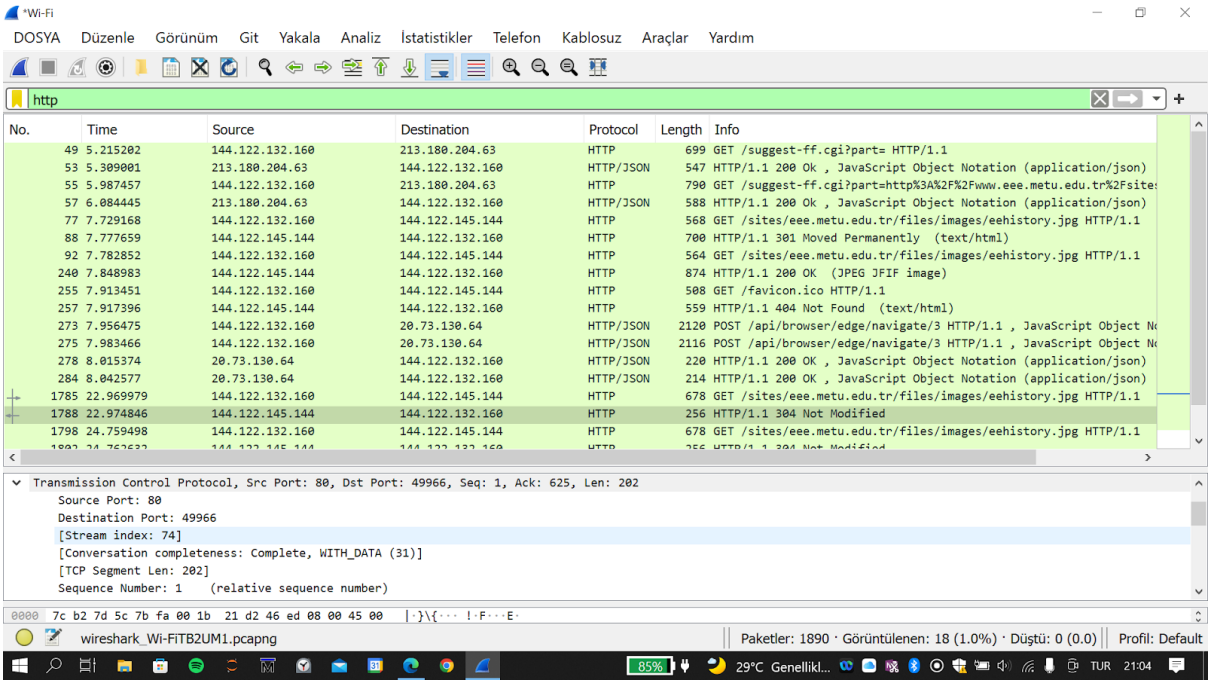


Figure 2. HTTP traffic view

From Fig 2, it can be seen that

The IP address of the actual source of the image file: 144.122.145.144

The port number of the actual source of the image file: 80

My IP address: 144.122.132.160

TCP Stream Index: 74

Zeynepnur ŞAHİNEL
2305399

Q.2.3)

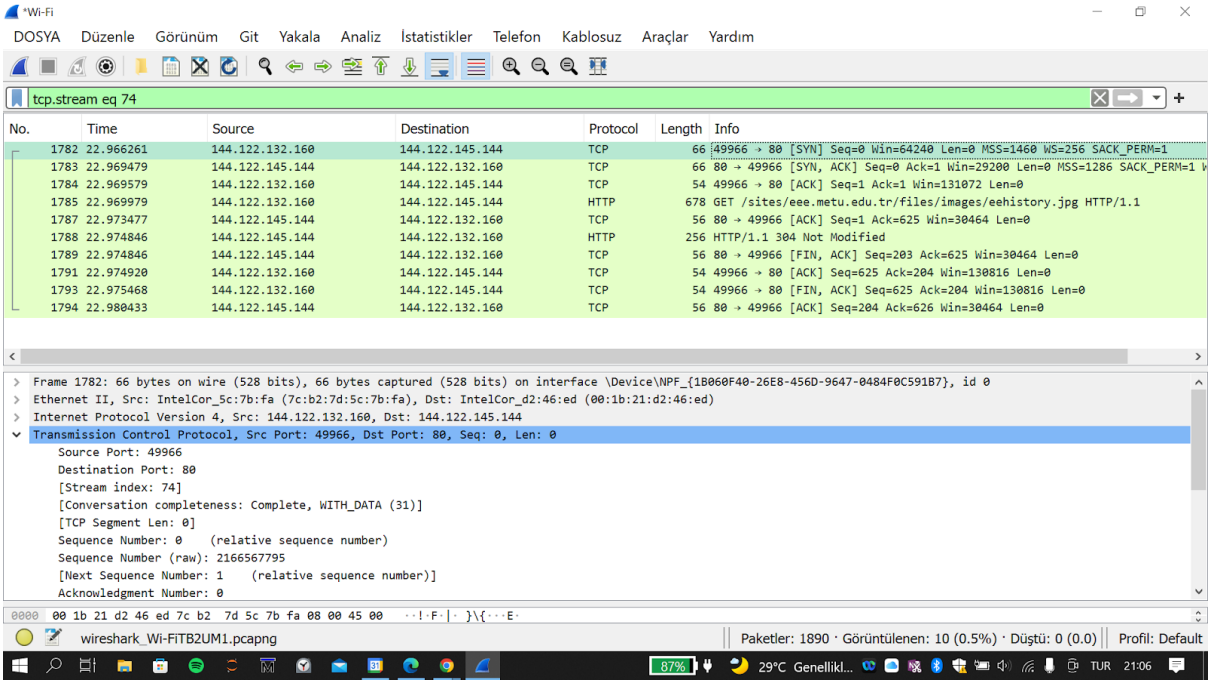


Figure 3. TCP Stream 74 view

The three-way handshaking process includes 3 steps. Figure 4 illustrates this process. Initially, the client (me) sends the SYN to the server. Here, SYN is a flag standing for synchronization. If a client wants to establish a connection, it sets this flag to 1. (From Fig. 5. a). In the second step, the server receives this message and sends a corresponding response by setting both SYN and ACK flags. (Fig. 5. b) In the last part, the client takes the message and sends an ACK to let the server know that the message has reached it. (Fig. 5. c) [1]

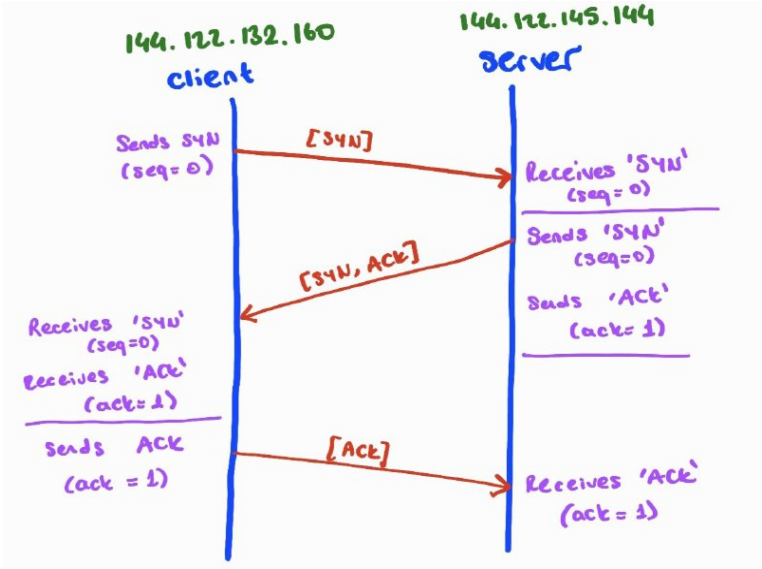
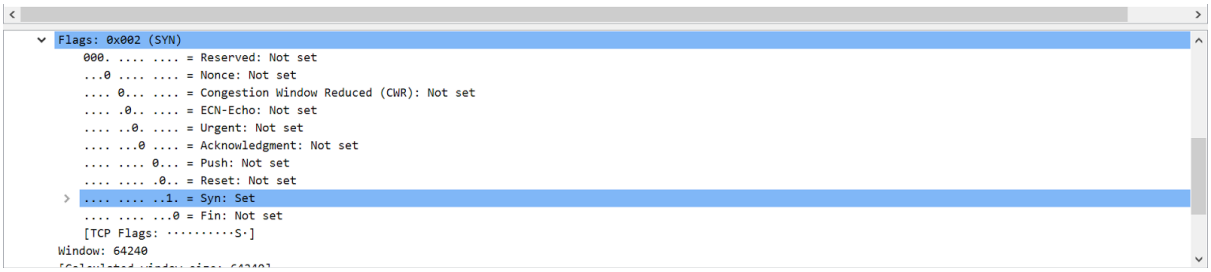
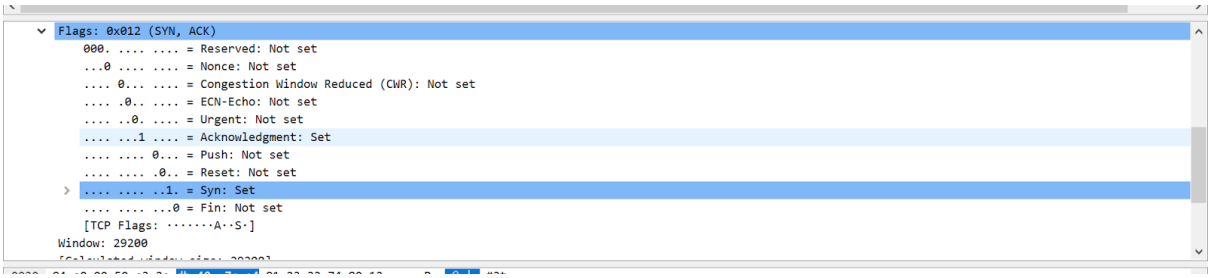


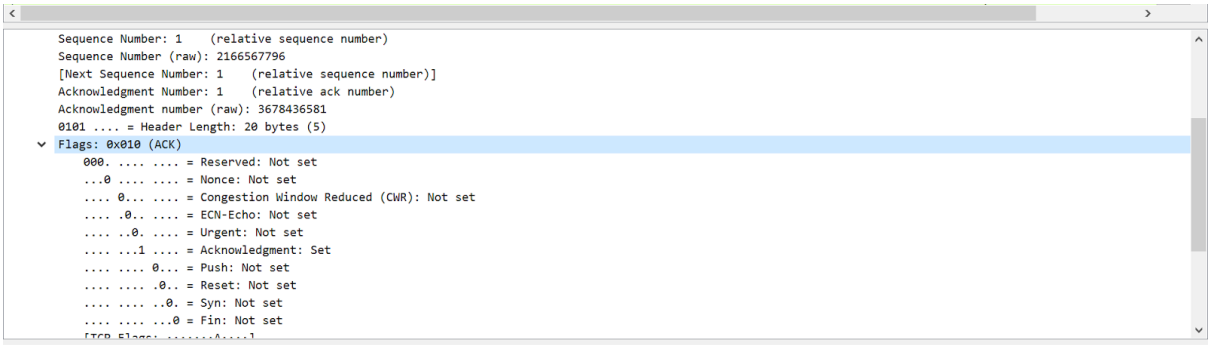
Figure 4. Illustration of the TCP 3-way handshaking



(a)



(b)



(c)

Figure 5. (a) Flags of the row 1782 (client to server initial communication) (b) Flags of the row 1783 (response of the server). (c) Flags of the row 1784 (TCP 3-way handshaking final part)

Q.2.4)

The longest frame for the stream 74 is 678 bytes (row 1785)

Encapsulation of the longest frame:

1) Looking at the TCP requests:

   From Fig. 3 row 1787, it can be seen that the ACK flag is 625, (one more of the actual data size -payload-) Thus, the payload is 624 bytes, yielding 54 bytes of encapsulation. (Fig. 6 and 7) [2]

2) Counting the headers in a single frame:

   From Fig. 8, it can be seen that the TCP payload is 624 bytes.

   Thus, subtracting the TCP payload gives a header length which is 54 (678-624)

Zeynepnur ŞAHİNEL
2305399

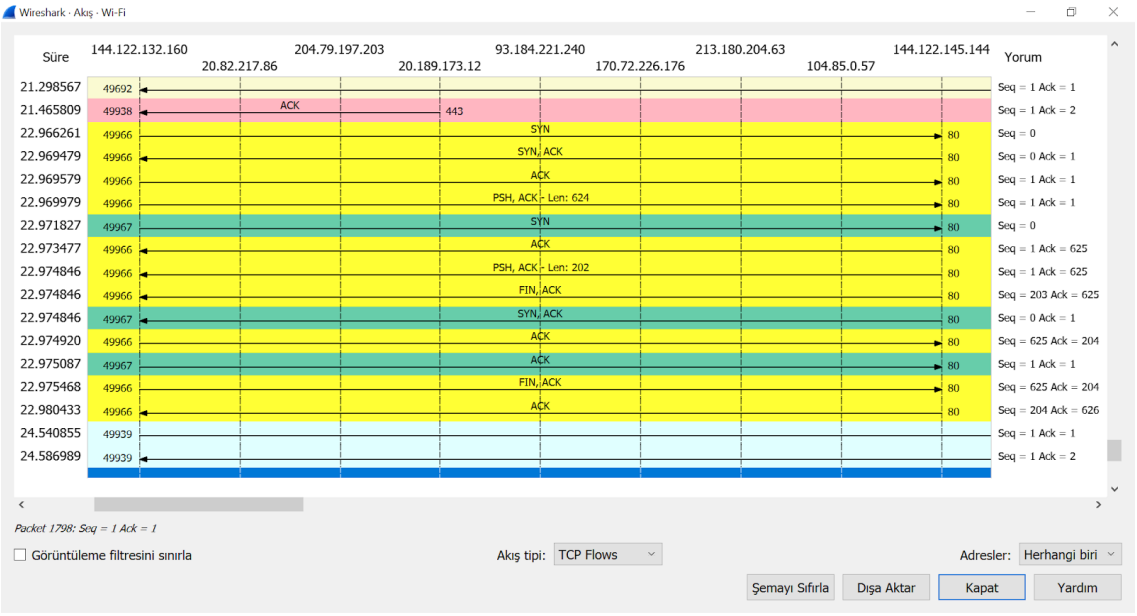


Figure 6. TCP Flow Graph

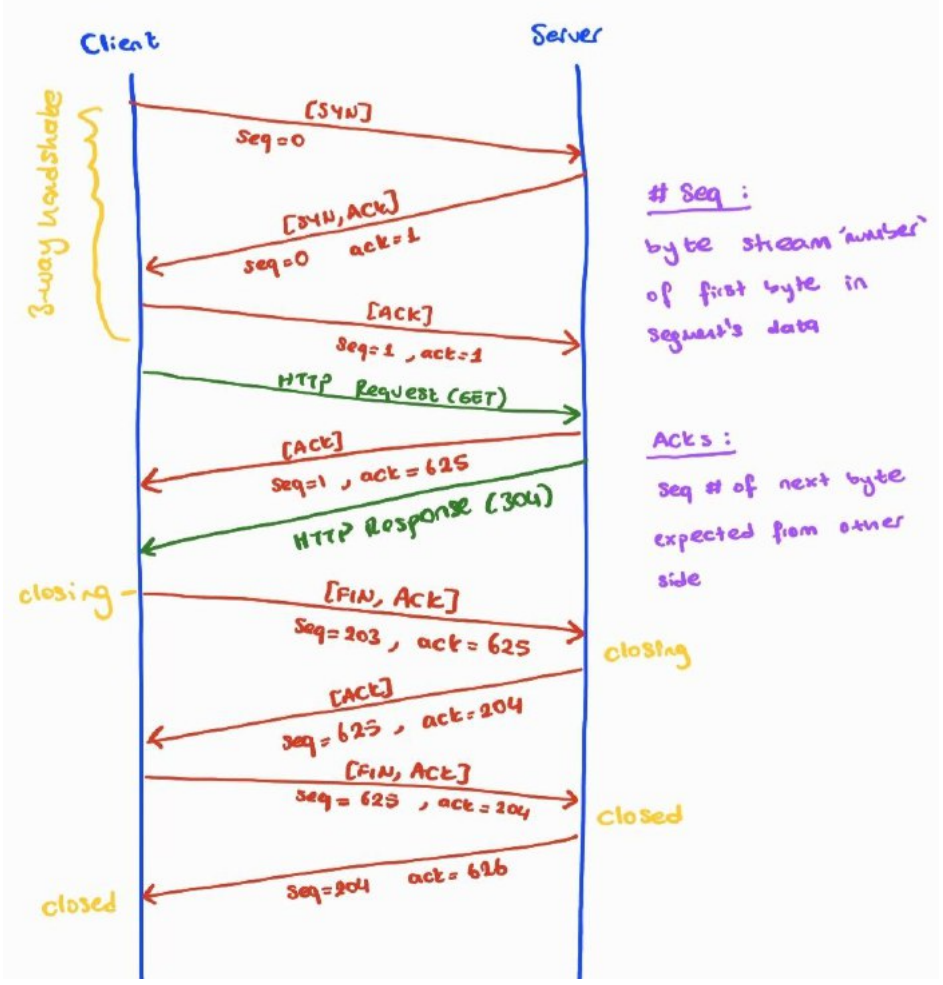


Figure 7. TCP connection timeline

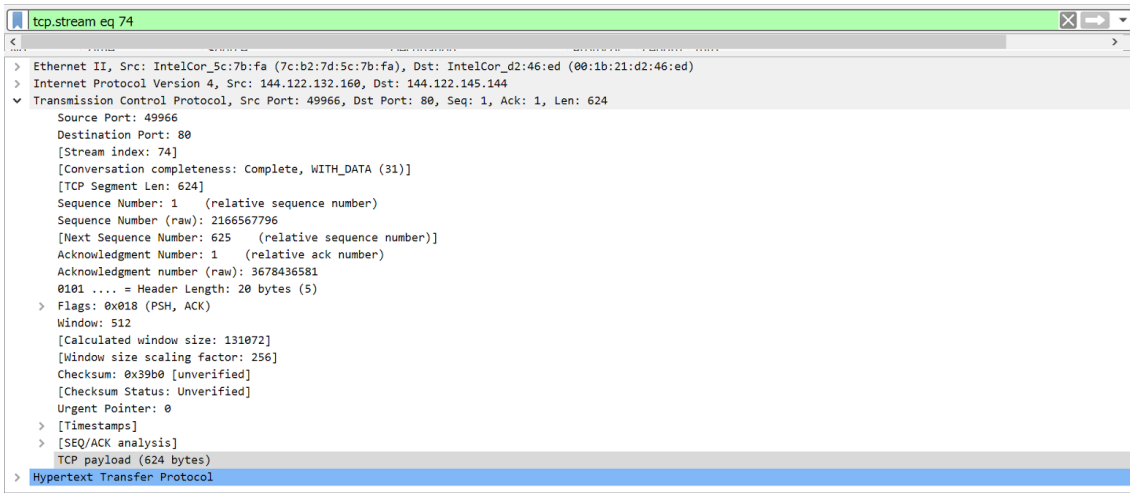
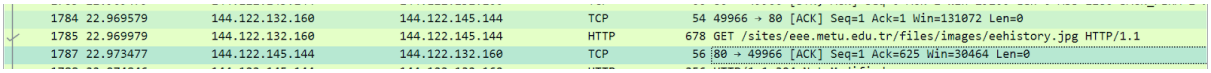


Figure 7. TCP Segment Informations

Q.2.5)

From Reference [3], throughput can be calculated as below:



Bytes transferred: 624

Time Interval: 22.973477-22.969579=0.003898

Throughput=Bytes transferred/Time Interval=160082 bytes/sec = 1280656 bps

Q.2.6)

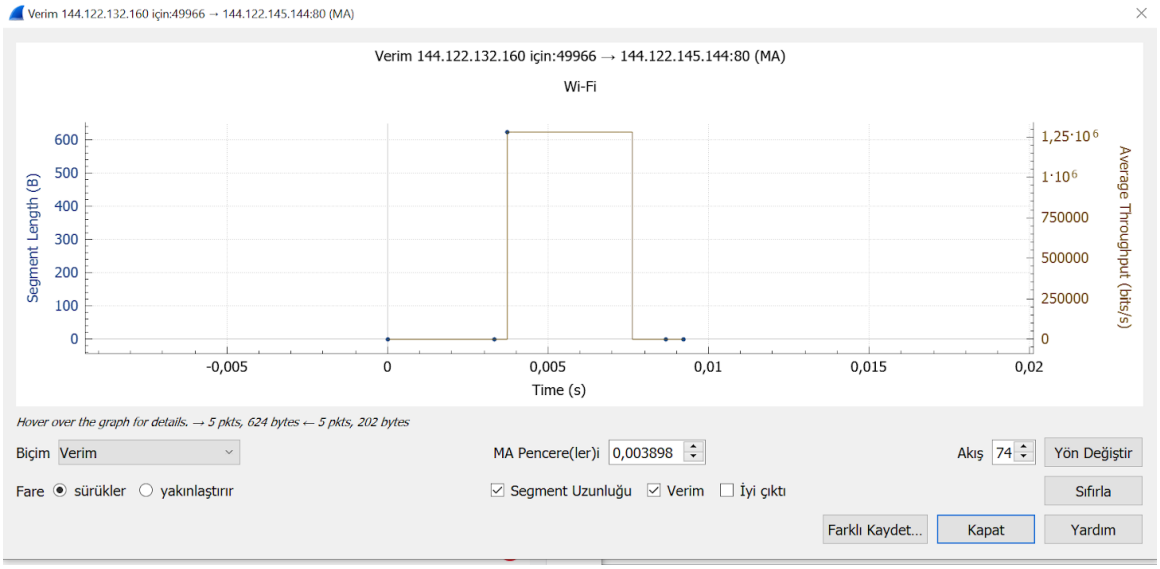
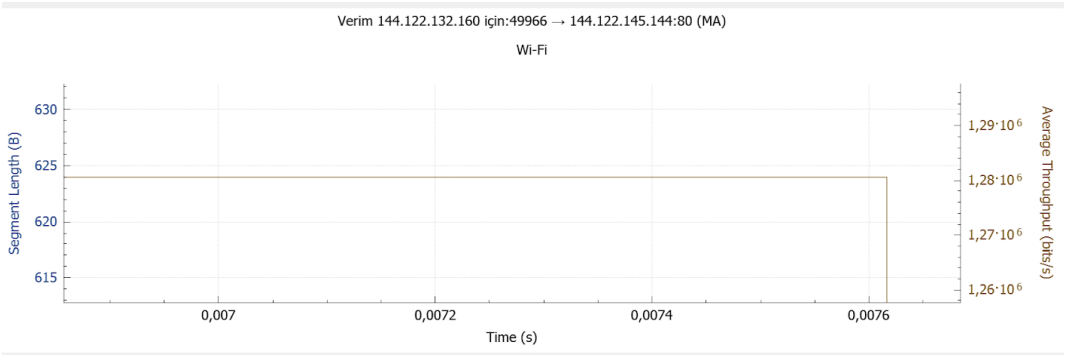


Figure 8. TCP Stream Graph



Zoomed version of Fig. 8

Q.2.7)

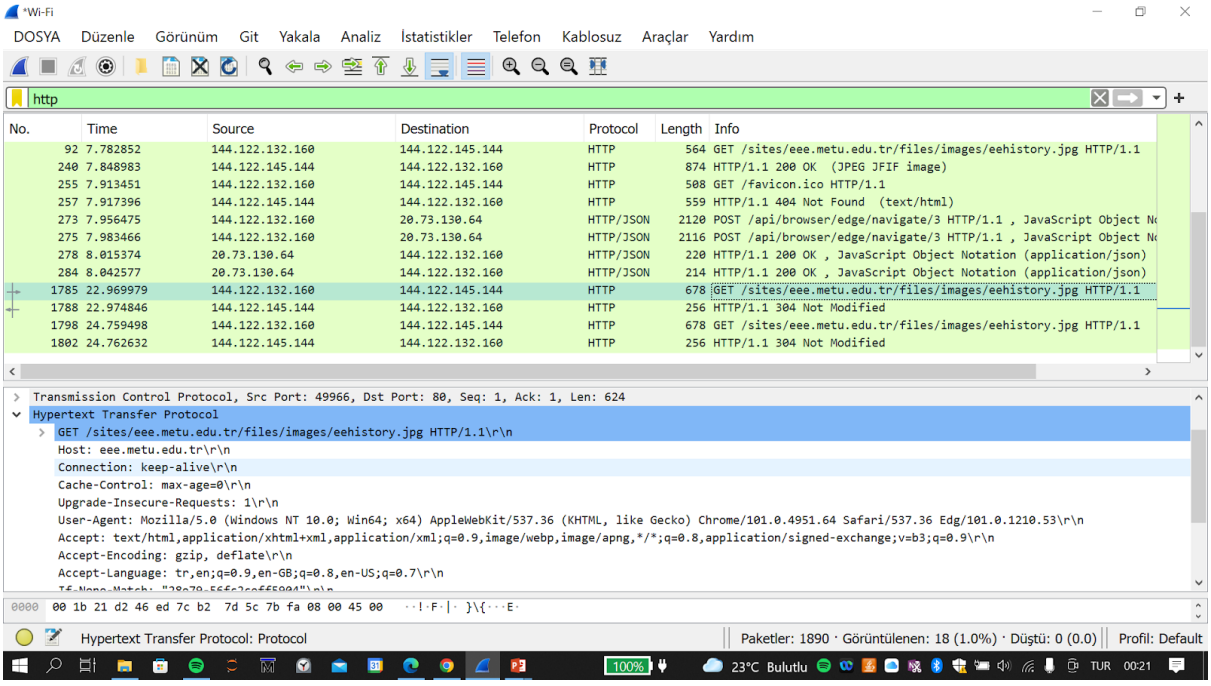


Figure 9. HTTP frame view

From the middlebox in Figure 9, inside the Hypertext Transfer Protocol part, connection is keep-alive. This means HTTP is persistent. Through persistent HTTP multiple objects can be sent over a single TCP connection between client, and server.

Q.2.8)

http://eee.metu.edu.tr/sites/eee.metu.edu.tr/files/images/eehistory.jpeg

144.122.132.160	144.122.145.144	HTTP	593 GET /sites/eee.metu.edu.tr/files/images/eehistory.jpeg HTTP/1.1
144.122.145.144	144.122.132.160	HTTP	834 HTTP/1.1 404 Not Found (text/html)

https://horde.metu.edu.tr/imp/dynamic.php?page=mailbox

144.122.132.160	144.122.199.210	HTTP	1135 GET /imp/dynamic.php?page=mailbox HTTP/1.1
144.122.199.210	144.122.132.160	HTTP	132 HTTP/1.1 200 OK (text/html)

Zeynepnur ŞAHİNEL
2305399

http://odtuclass2021s.metu.edu.tr/my/

```
144.122.132.160    144.122.145.167    HTTP    532 GET /my/ HTTP/1.1
144.122.145.167    144.122.132.160    HTTP    189 HTTP/1.1 302 Found
```

https://www.dr.com.tr/Themes/DR/Content/NewTheme/assets/dist/js/datalayer/homep
https://vsh.visilabs.net/Visilabs.min.js?sid=2B64733449375753437573 3D&oid=65673

```
18450 133.286338   144.122.132.160   46.17.134.217     HTTP   3691 GET /Themes/DR/Content/NewTheme/assets/dist/js/homepage.js?ver=9
18451 133.286894   144.122.132.160   46.17.134.217     HTTP   3707 GET /Themes/DR/Content/NewTheme/assets/dist/js/datalayer/homepag
18484 133.300688   46.17.134.217     144.122.132.160   HTTP    119 HTTP/1.1 200 OK  (application/javascript)
18509 133.314942   46.17.134.217     144.122.132.160   HTTP    567 HTTP/1.1 200 OK  (application/javascript)
18513 133.337078   144.122.132.160   185.29.195.172    HTTP    777 GET /Visilabs.min.js?sid=2B64733449375753437573 3D&oid=6567387344
18522 133.358727   185.29.195.172    144.122.132.160   HTTP    552 HTTP/1.1 301 Moved Permanently  (text/html)
```

```
Purpose: prefetch\r\n
Sec-Fetch-Site: cross-site\r\n
Sec-Fetch-Mode: no-cors\r\n
Sec-Fetch-Dest: script\r\n
Referer: https://www.dr.com.tr/\r\n
Accept-Encoding: gzip, deflate, br\r\n
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7,de;q=0.6\r\n
\r\n
[Full request URI: https://vsh.visilabs.net/Visilabs.min.js?sid=2B64733449375753437573 3D&oid=6567387344534557696E673D&site=DR]
[HTTP request 1/1]
[Response in frame: 18522]
```

Table 1. Status Codes and Their Meanings [4]

Status Code	Meaning
200 OK	**Successful Responses.** The request succeeded. The success depends on the HTTP Method. Here for the GET command: “The source has been fetched and transmitted in the message body.”
404 Not Found	**Client Error Responses**. The server can not find the requested resource, meaning that the URL is not recognized.
302 Found	**Redirection Messages.** The URI of the requested resource has been changed temporarily.
301 Moved Permanently	**Redirection Messages.** The URL of the resource has been changed permanently.

Zeynepnur ŞAHİNEL
2305399

Q.2.9)

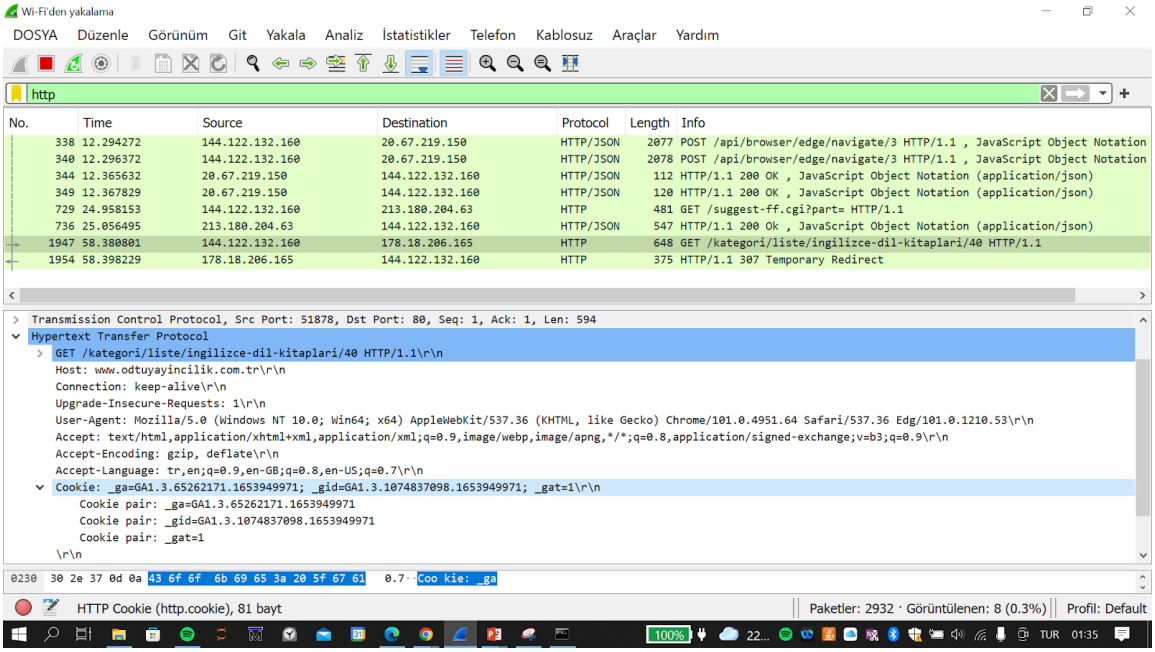
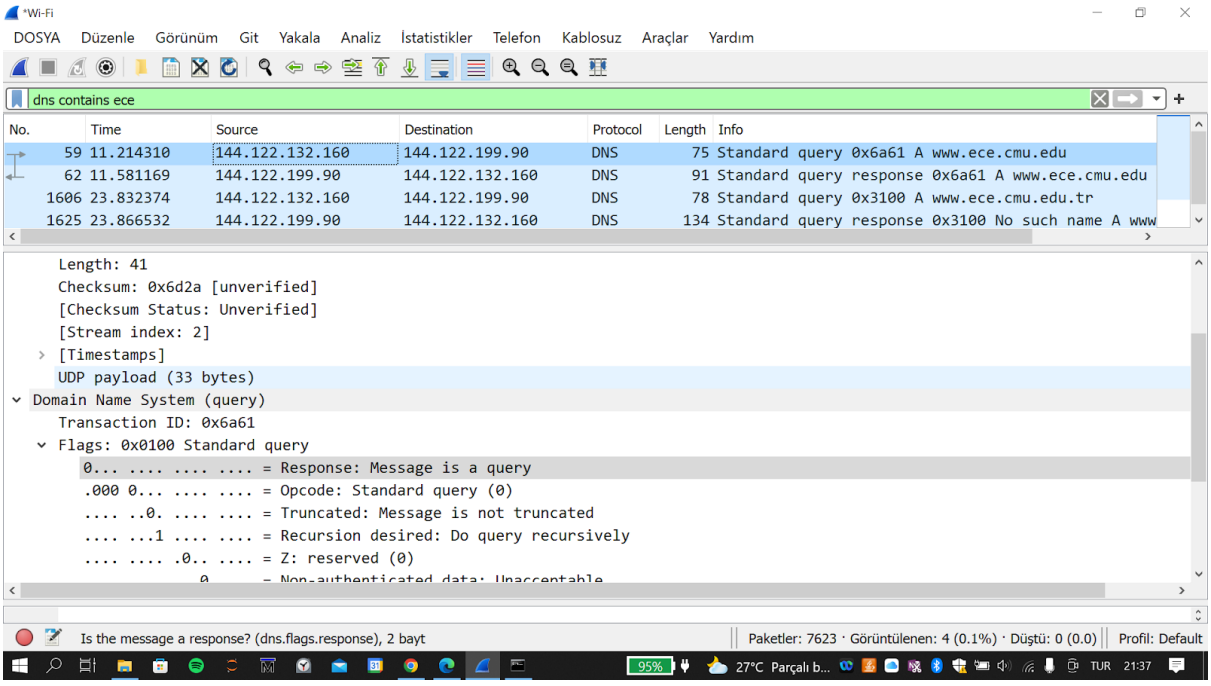
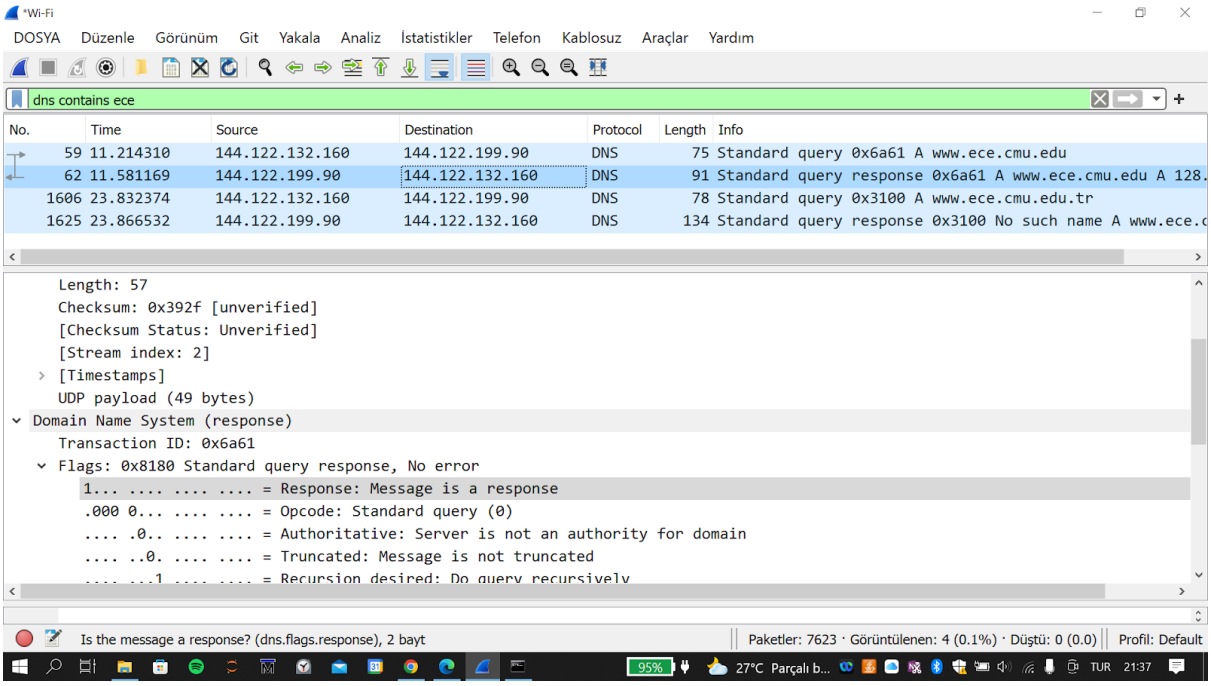


Figure 10. Cookies from http://www.odtuyayincilik.com.tr

Q.2.10)

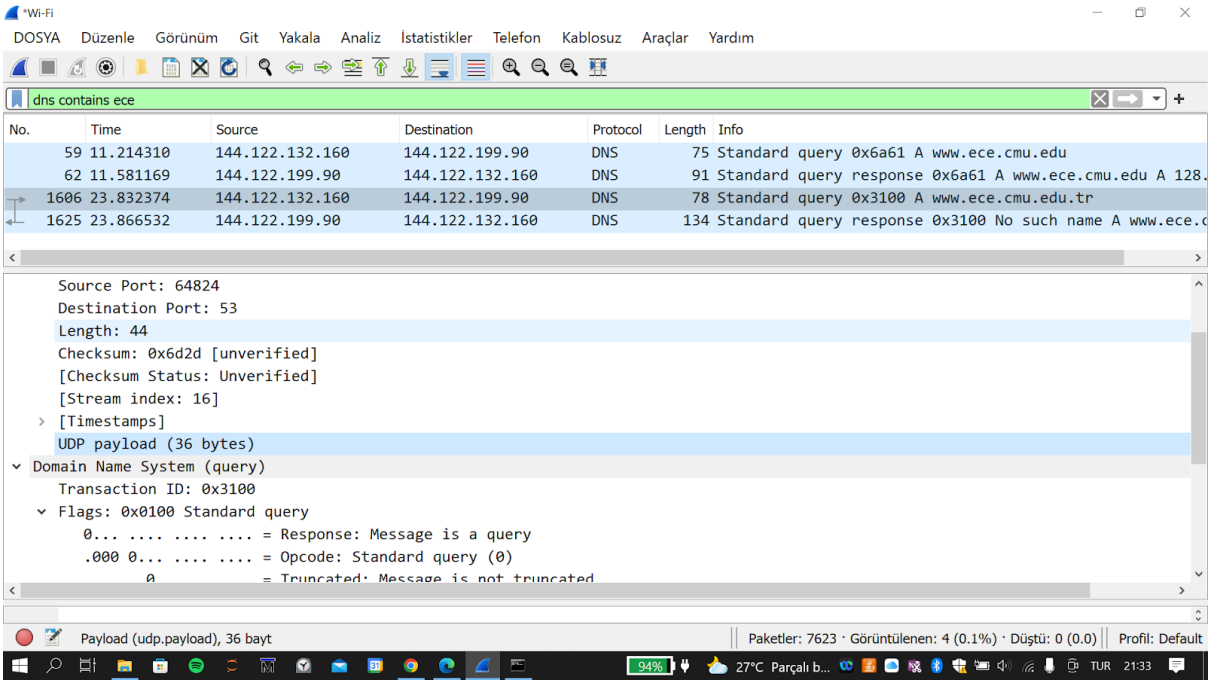


(a)

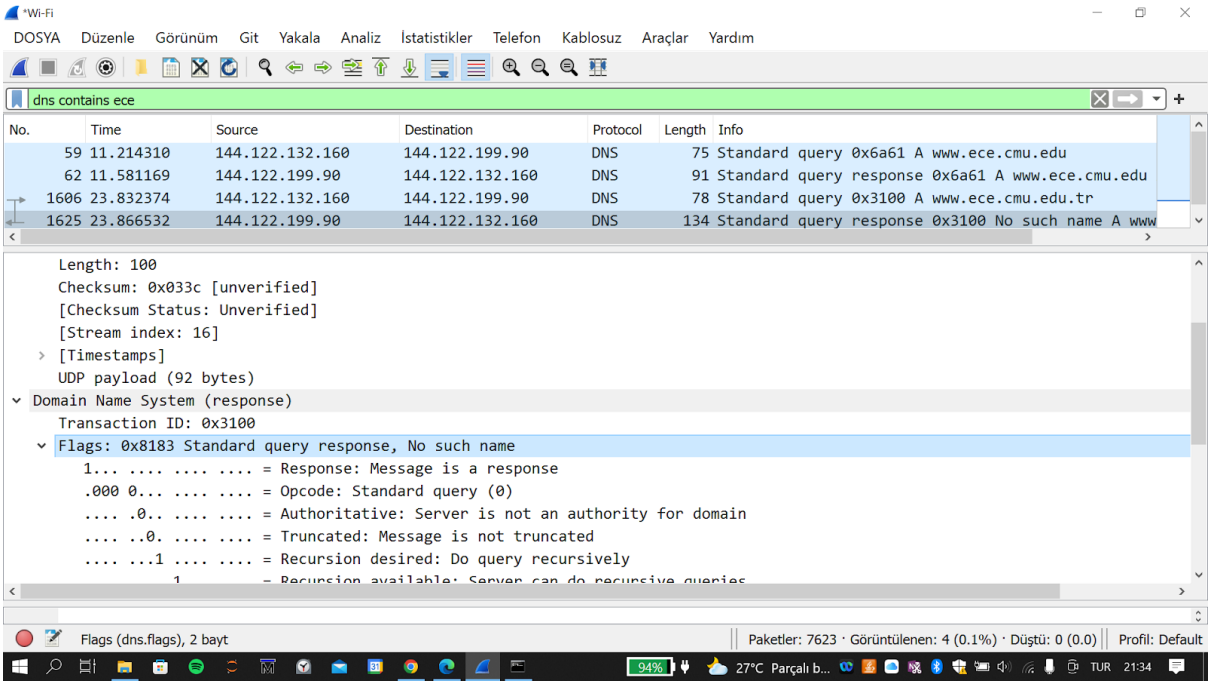


(b)

Not found page



(c)



(d)

Figure 11. (a)Standart query for www.ece.cmu.edu (b) Standart query-response for www.ece.cmu.edu (c) Standart query for www.ece.cmu.edu.tr (d) Standart query-response for www.ece.cmu.edu.tr

DNS header length= 8 bytes (can be seen from Fig. 11 a,b,c,d) Length-UDP Payload =8 bytes
Transaction ID length = 16 bits
The most significant bit determines the whether it is a query or response. If the flag bit is 1, then it is a response, otherwise, it is a query.

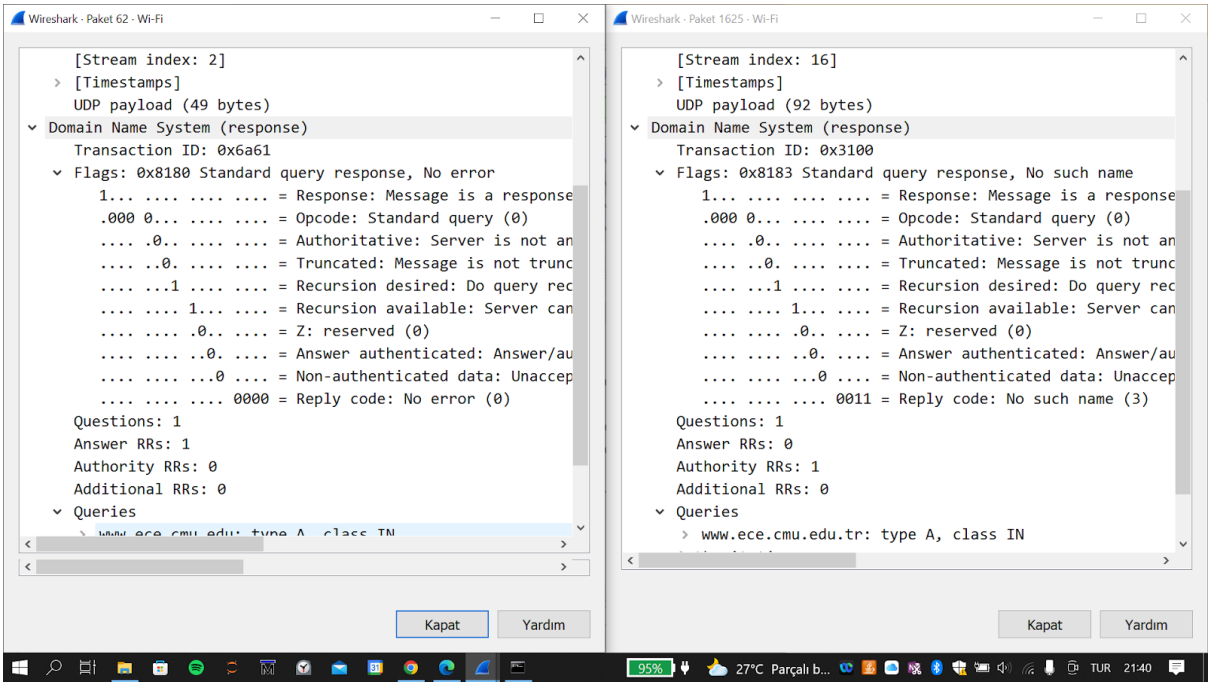
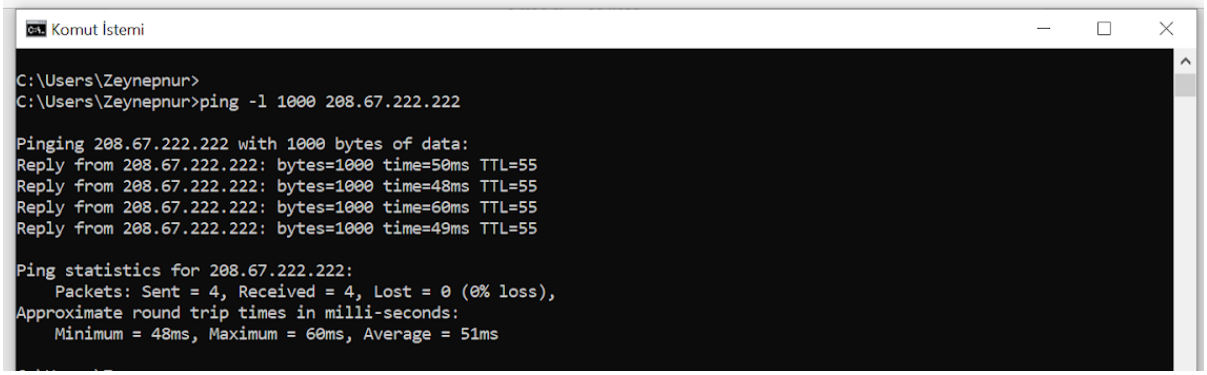


Figure 12. Domain Name System information of two responses

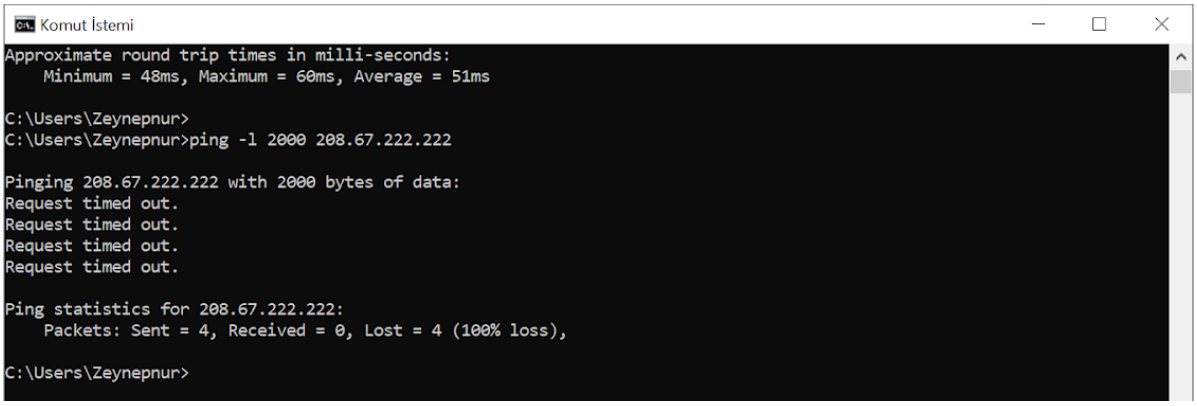
From Figure 12, it can be said that only the last 4 bits are different from each other. When the least significant bits are “0000” it means that “No error”. If these bits are “0011”, it represents the “No such name” response code.

Part 3- ICMP

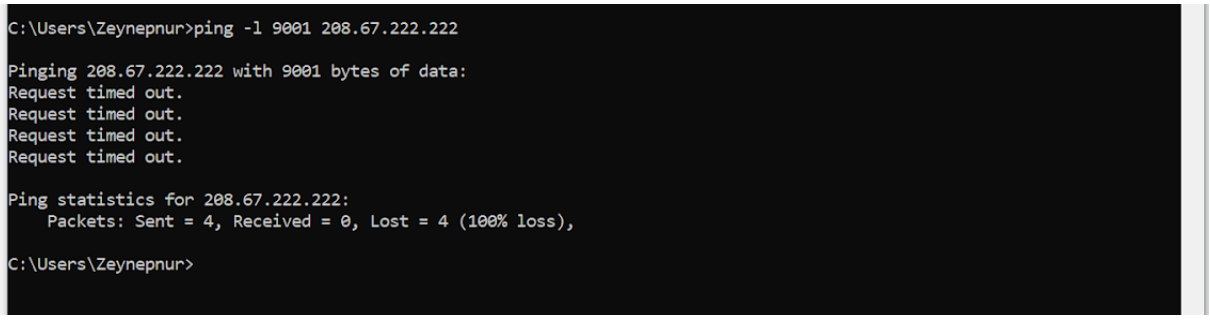
Q.3.1)



ping -l [size] command means send this amount of buffer. Connection is successful. All packets are received and sent back to the host. Also average RTT is calculated.



Sends 2000 bytes buffer to the previous host, however, packets were not received. Since standard maximum transmission unit is 1500 bytes. (jumboframe)



Sends 9001 bytes buffer to the previous host, however, packets were not received. Since standard maximum transmission unit is 1500 bytes. (jumboframe)

```
C:\Users\Zeynepnur> ping 0.0.0.0

Pinging 0.0.0.0 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 0.0.0.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

This address is an invalid destination address. It can only be used for a source address when host has no assigned address.

```
C:\Users\Zeynepnur>
C:\Users\Zeynepnur> ping 127.0.0.0

Pinging 127.0.0.0 with 32 bytes of data:
General failure.
General failure.
General failure.
General failure.

Ping statistics for 127.0.0.0:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Zeynepnur>
```

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as the localhost address. This loopback IP address is managed entirely by and within the operating system. Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. [5]

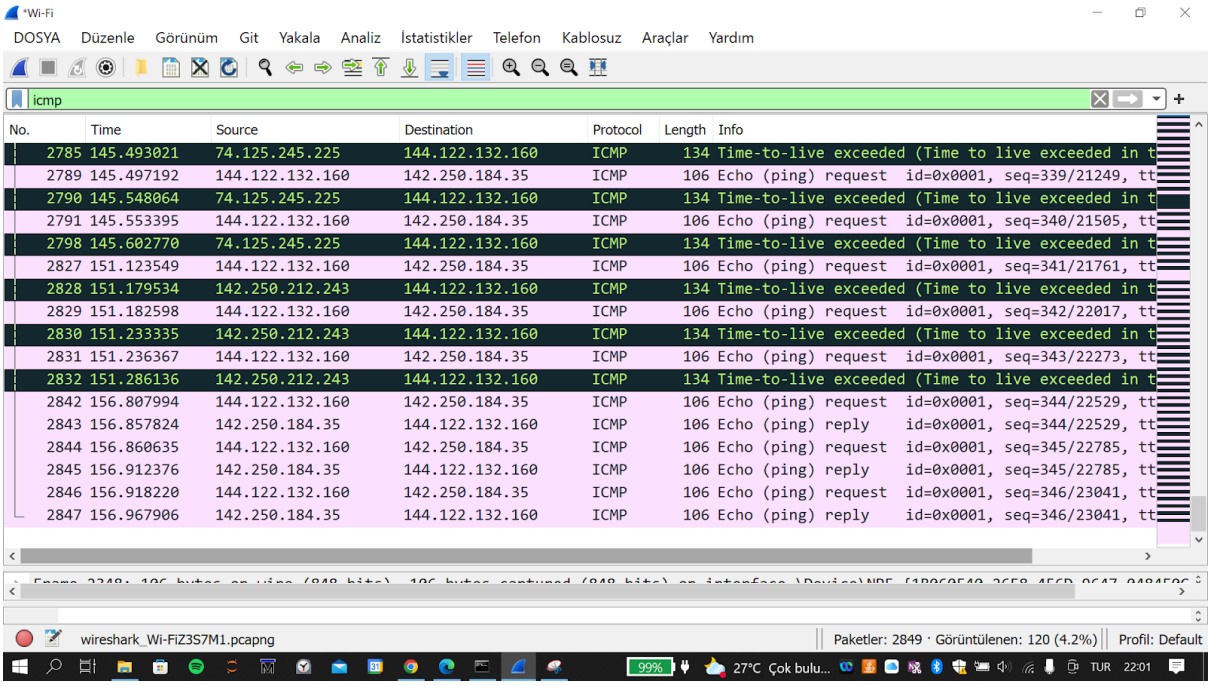
```
C:\Users\Zeynepnur> ping 255.255.255.255
Ping request could not find host 255.255.255.255. Please check the name and try again.

C:\Users\Zeynepnur>
```

255.255.255.255 is a broadcast address. In this command, we are trying to ping to a every device on my local network simultaneously. Thus it gives an error.

```
C:\Users\Zeynepnur>tracert twitter.com

Tracing route to twitter.com [104.244.42.65]
over a maximum of 30 hops:

  1     2 ms     1 ms     3 ms  907a8401.drm.metu.edu.tr [144.122.132.1]
  2     5 ms     3 ms     5 ms  rt1.metu.edu.tr [144.122.2.1]
  3    23 ms    19 ms    17 ms  144.122.1.21
  4     3 ms     3 ms     3 ms  193.140.85.137
  5     5 ms     2 ms     5 ms  69.96.154.212.static.turk.net [212.154.96.69]
  6     *        *        *     Request timed out.
  7     3 ms     4 ms     3 ms  06-ulus-xrs-t2-2---06-ulus-sr12e-t3-1.statik.turktelekom.com.tr [81.212.222.209]
  8     3 ms     3 ms     2 ms  06-ebgp-ulus-sr12e-k---06-ulus-xrs-t2-2.statik.turktelekom.com.tr [81.212.217.121]
  9     9 ms     3 ms     4 ms  81.212.209.18.static.turktelekom.com.tr [81.212.209.18]
 10    48 ms    49 ms    49 ms  302-ams-col-2---06-ebgp-ulus-sr12e-k.statik.turktelekom.com.tr [212.156.102.184]
 11    56 ms    55 ms    59 ms  ae56.edge7.Amsterdam1.Level3.net [213.19.198.193]
 12    57 ms    58 ms    56 ms  ae1.3106.edge5.Amsterdam1.level3.net [4.69.162.194]
 13    56 ms    54 ms    51 ms  213.19.194.18
 14     *        *        *     Request timed out.
 15    51 ms    51 ms    53 ms  104.244.42.65

Trace complete.
```

Tracing route to the Twitter which was completed in 15 hops.

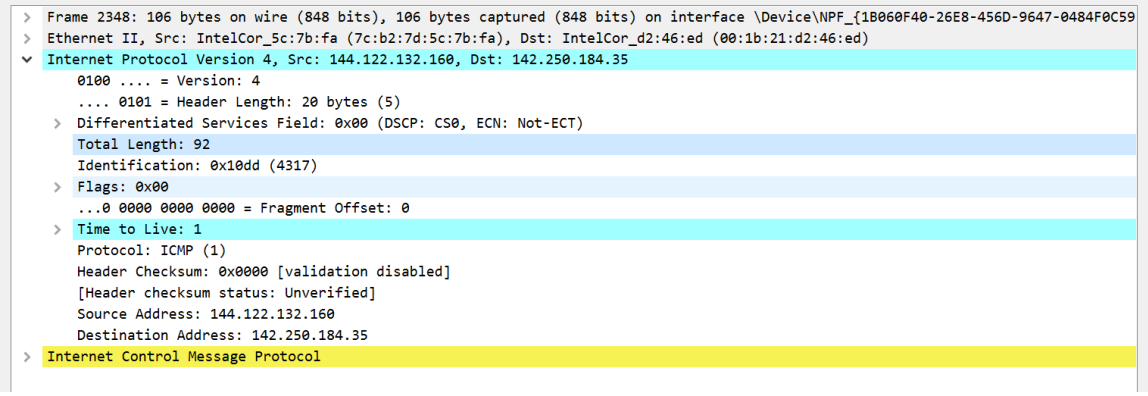
Zeynepnur ŞAHİNEL
2305399



Wireshark capture while trace routing to google.

```
C:\Users\Zeynepnur>tracert www.google.com.tr

Tracing route to www.google.com.tr [142.250.184.35]
over a maximum of 30 hops:

  1     7 ms     6 ms     2 ms  907a8401.drm.metu.edu.tr [144.122.132.1]
  2     2 ms     2 ms     3 ms  rt1.metu.edu.tr [144.122.2.1]
  3    28 ms    36 ms    30 ms  144.122.1.21
  4     3 ms     2 ms     4 ms  193.140.85.137
  5     4 ms     2 ms     5 ms  69.96.154.212.static.turk.net [212.154.96.69]
  6     *       43 ms     3 ms  212.156.64.45.static.turktelekom.com.tr [212.156.64.45]
  7    43 ms     2 ms     3 ms  06-ulus-xrs-t2-2---06-ulus-sr12e-t3-1.statik.turktelekom.com.tr [81.212.222.209]
  8     *        *        3 ms  06-ebgp-ulus-sr12e-k---06-ulus-xrs-t2-2.statik.turktelekom.com.tr [81.212.217.121]
  9     4 ms     8 ms     5 ms  81.212.209.18.static.turktelekom.com.tr [81.212.209.18]
 10    23 ms    23 ms    25 ms  307-sof-col-1---06-ulus-xrs-t2-2.statik.turktelekom.com.tr [212.156.104.152]
 11    53 ms    53 ms    51 ms  209.85.168.140
 12    54 ms    55 ms    54 ms  108.170.250.177
 13    50 ms    50 ms    51 ms  108.170.250.179
 14    50 ms    49 ms    51 ms  142.250.213.230
 15    51 ms    51 ms    52 ms  172.253.68.170
 16    51 ms    50 ms    50 ms  172.253.66.215
 17    50 ms    56 ms    51 ms  142.250.234.84
 18    50 ms    51 ms    49 ms  74.125.245.225
 19    56 ms    50 ms    49 ms  142.250.212.243
 20    49 ms    51 ms    49 ms  mil41s02-in-f3.1e100.net [142.250.184.35]

Trace complete.
```

Q.3.2)



The name in the upper layer protocol field is ICMP (1).

IP Header Length is 20 bytes.

Payload = Total Length -IP Header Length=92-20=72 bytes

Q.3.3)

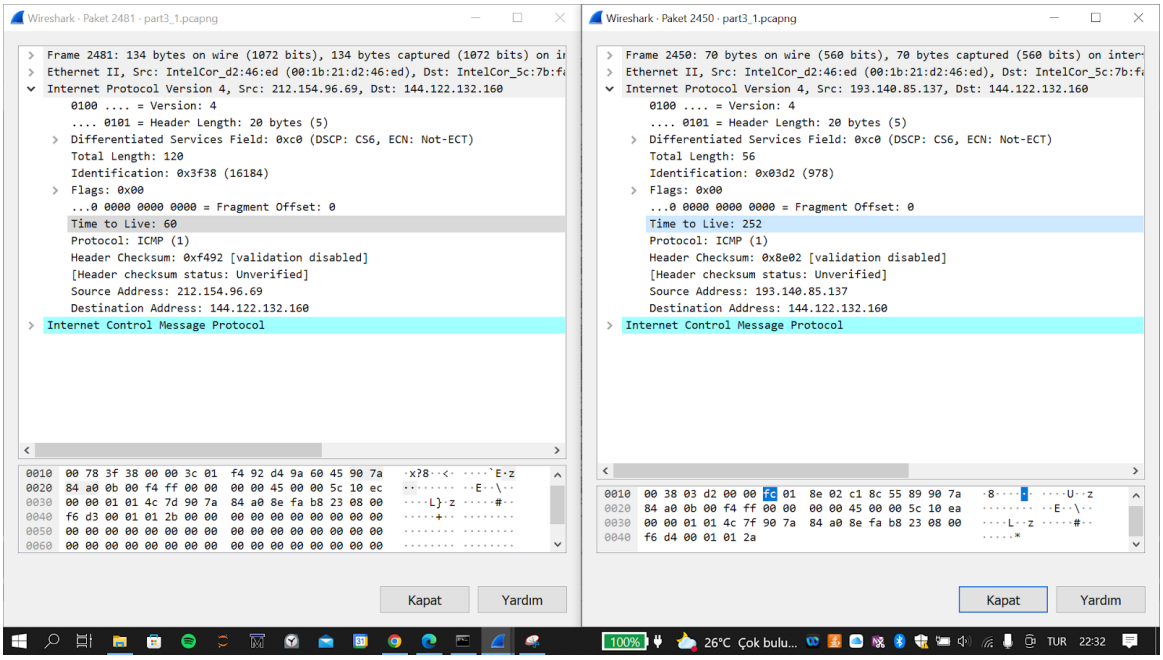
Time to Live, Header Checksum, Identification always change. Whereas, version, header length, differentiated services, upper-layer protocol (ICMP), source, and destination address must stay constant.

Q.3.4)

Three packets are sent with the same TTL. The purpose behind this is to record the source of each ICMP TTL exceeded message to provide a trace of the path the packet took to reach the destination. [6]

Zeynepnur ŞAHİNEL
2305399

Q.3.5)



The identification field changes for all the ICMP TTL-exceeded replies since the identification field is a unique value. TTL is the same for the same router whereas for different routers TTL changes. Version, header length, differentiated services, and upper-layer protocol (ICMP) are constant.

References

[1] https://afteracademy.com/blog/what-is-a-tcp-3-way-handshake-process

[2] https://packetlife.net/blog/2010/jun/7/understanding-tcp-sequence-acknowledgment-numbers/

[3] https://madpackets.com/2018/05/18/finding-throughput-with-wireshark/

[4] https://developer.mozilla.org/en-US/docs/Web/HTTP/Status

[5] https://www.tutorialspoint.com/ipv4/ipv4_reserved_addresses.htm#

[6]https://stackoverflow.com/questions/32742361/why-traceroutes-three-packets-with-same-ttl-always-go-to-same-route