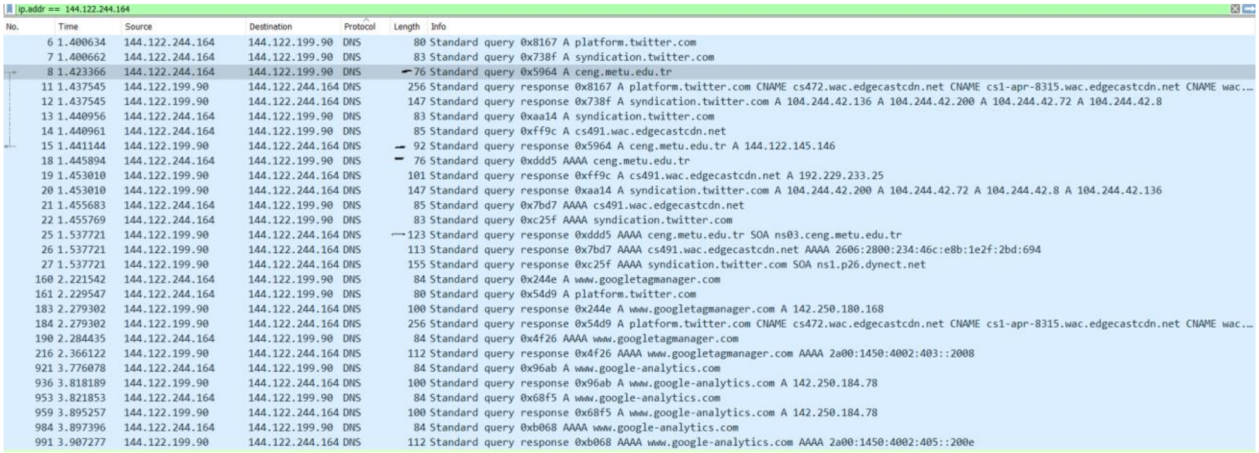
435 Data Communications and Networking

Homework 1

Burak Bahar

2380137

2.1) 2 queries where sent to ceng from my ip. There are black lines to the side.

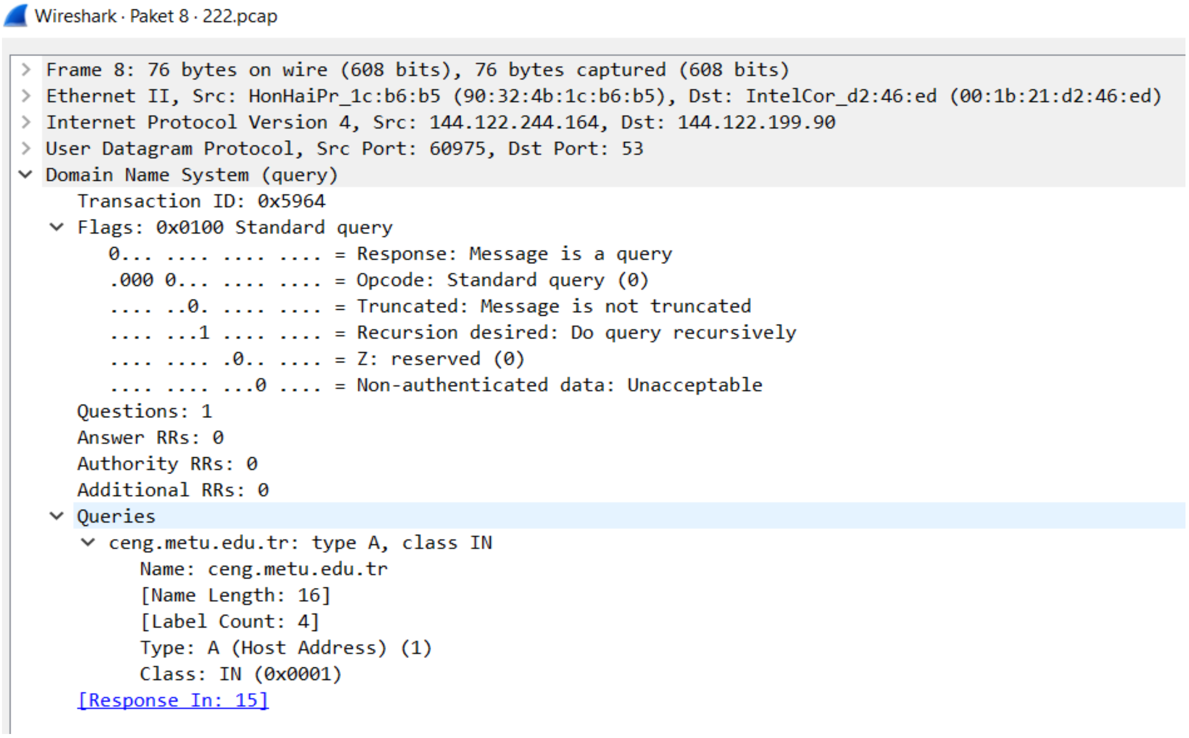


ip.addr == 144.122.244.164

No.	Time	Source	Destination	Protocol	Length	Info
6	1.400634	144.122.244.164	144.122.199.90	DNS	80	Standard query 0x8167 A platform.twitter.com
7	1.400662	144.122.244.164	144.122.199.90	DNS	83	Standard query 0x738f A syndication.twitter.com
8	1.423366	144.122.244.164	144.122.199.90	DNS	76	Standard query 0x5964 A ceng.metu.edu.tr
11	1.437545	144.122.199.90	144.122.244.164	DNS	256	Standard query response 0x8167 A platform.twitter.com CNAME cs472.wac.edgecastcdn.net CNAME cs1-apr-8315.wac.edgecastcdn.net CNAME wac.…
12	1.437545	144.122.199.90	144.122.244.164	DNS	147	Standard query response 0x738f A syndication.twitter.com A 104.244.42.136 A 104.244.42.200 A 104.244.42.72 A 104.244.42.8
13	1.440956	144.122.244.164	144.122.199.90	DNS	83	Standard query 0xaa14 A syndication.twitter.com
14	1.440961	144.122.244.164	144.122.199.90	DNS	85	Standard query 0xff9c A cs491.wac.edgecastcdn.net
15	1.441144	144.122.199.90	144.122.244.164	DNS	92	Standard query response 0x5964 A ceng.metu.edu.tr A 144.122.145.146
18	1.445894	144.122.244.164	144.122.199.90	DNS	76	Standard query 0xddd5 AAAA ceng.metu.edu.tr
19	1.453010	144.122.199.90	144.122.244.164	DNS	101	Standard query response 0xff9c A cs491.wac.edgecastcdn.net A 192.229.233.25
20	1.453010	144.122.199.90	144.122.244.164	DNS	147	Standard query response 0xaa14 A syndication.twitter.com A 104.244.42.200 A 104.244.42.72 A 104.244.42.8 A 104.244.42.136
21	1.455683	144.122.244.164	144.122.199.90	DNS	85	Standard query 0x7bd7 AAAA cs491.wac.edgecastcdn.net
22	1.455769	144.122.244.164	144.122.199.90	DNS	83	Standard query 0xc25f AAAA syndication.twitter.com
25	1.537721	144.122.199.90	144.122.244.164	DNS	123	Standard query response 0xddd5 AAAA ceng.metu.edu.tr SOA ns03.ceng.metu.edu.tr
26	1.537721	144.122.199.90	144.122.244.164	DNS	113	Standard query response 0x7bd7 AAAA cs491.wac.edgecastcdn.net AAAA 2606:2800:234:46c:e8b:1e2f:2bd:694
27	1.537721	144.122.199.90	144.122.244.164	DNS	155	Standard query response 0xc25f AAAA syndication.twitter.com SOA ns1.p26.dynect.net
160	2.221542	144.122.244.164	144.122.199.90	DNS	84	Standard query 0x244e A www.googletagmanager.com
161	2.229547	144.122.244.164	144.122.199.90	DNS	80	Standard query 0x54d9 A platform.twitter.com
183	2.279302	144.122.199.90	144.122.244.164	DNS	100	Standard query response 0x244e A www.googletagmanager.com A 142.250.180.168
184	2.279302	144.122.199.90	144.122.244.164	DNS	256	Standard query response 0x54d9 A platform.twitter.com CNAME cs472.wac.edgecastcdn.net CNAME cs1-apr-8315.wac.edgecastcdn.net CNAME wac.…
190	2.284435	144.122.244.164	144.122.199.90	DNS	84	Standard query 0x4f26 AAAA www.googletagmanager.com
216	2.366122	144.122.199.90	144.122.244.164	DNS	112	Standard query response 0x4f26 AAAA www.googletagmanager.com AAAA 2a00:1450:4002:403::2008
921	3.776078	144.122.244.164	144.122.199.90	DNS	84	Standard query 0x96ab A www.google-analytics.com
936	3.818189	144.122.199.90	144.122.244.164	DNS	100	Standard query response 0x96ab A www.google-analytics.com A 142.250.184.78
953	3.821853	144.122.244.164	144.122.199.90	DNS	84	Standard query 0x68f5 A www.google-analytics.com
959	3.895257	144.122.199.90	144.122.244.164	DNS	100	Standard query response 0x68f5 A www.google-analytics.com A 142.250.184.78
984	3.897396	144.122.244.164	144.122.199.90	DNS	84	Standard query 0xb068 AAAA www.google-analytics.com
991	3.907277	144.122.199.90	144.122.244.164	DNS	112	Standard query response 0xb068 AAAA www.google-analytics.com AAAA 2a00:1450:4002:405::200e

Picture 1

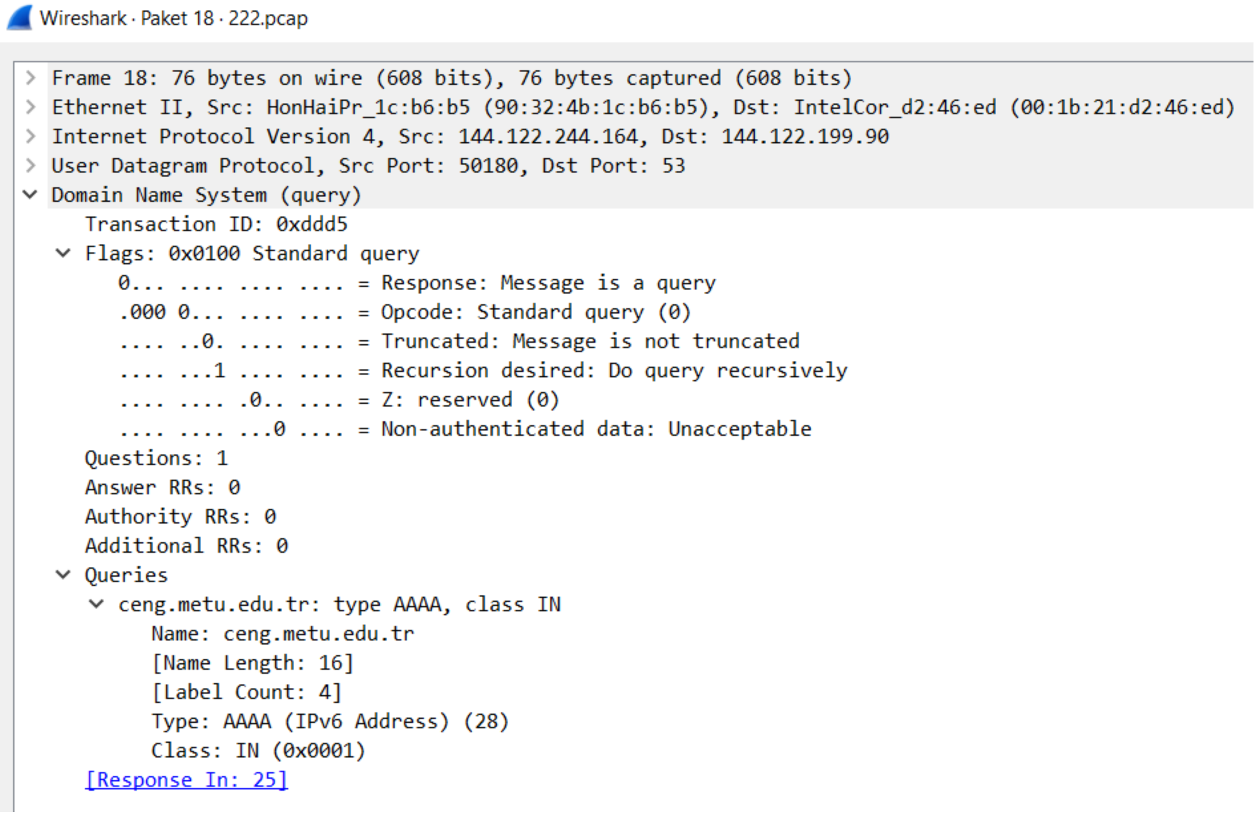
2.2) In the DNS (query)part, there was only one query as we can see underneath.



Wireshark · Paket 8 · 222.pcap

```
> Frame 8: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: HonHaiPr_1c:b6:b5 (90:32:4b:1c:b6:b5), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.244.164, Dst: 144.122.199.90
> User Datagram Protocol, Src Port: 60975, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x5964
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v ceng.metu.edu.tr: type A, class IN
        Name: ceng.metu.edu.tr
        [Name Length: 16]
        [Label Count: 4]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
    [Response In: 15]
```

No. 8 From Picture 1

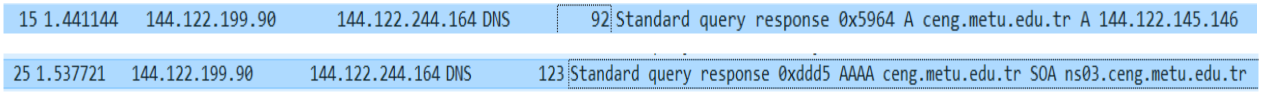


```
Wireshark · Paket 18 · 222.pcap

> Frame 18: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: HonHaiPr_1c:b6:b5 (90:32:4b:1c:b6:b5), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.244.164, Dst: 144.122.199.90
> User Datagram Protocol, Src Port: 50180, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0xddd5
  v Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v ceng.metu.edu.tr: type AAAA, class IN
        Name: ceng.metu.edu.tr
        [Name Length: 16]
        [Label Count: 4]
        Type: AAAA (IPv6 Address) (28)
        Class: IN (0x0001)
    [Response In: 25]
```

No 18 From Picture 1

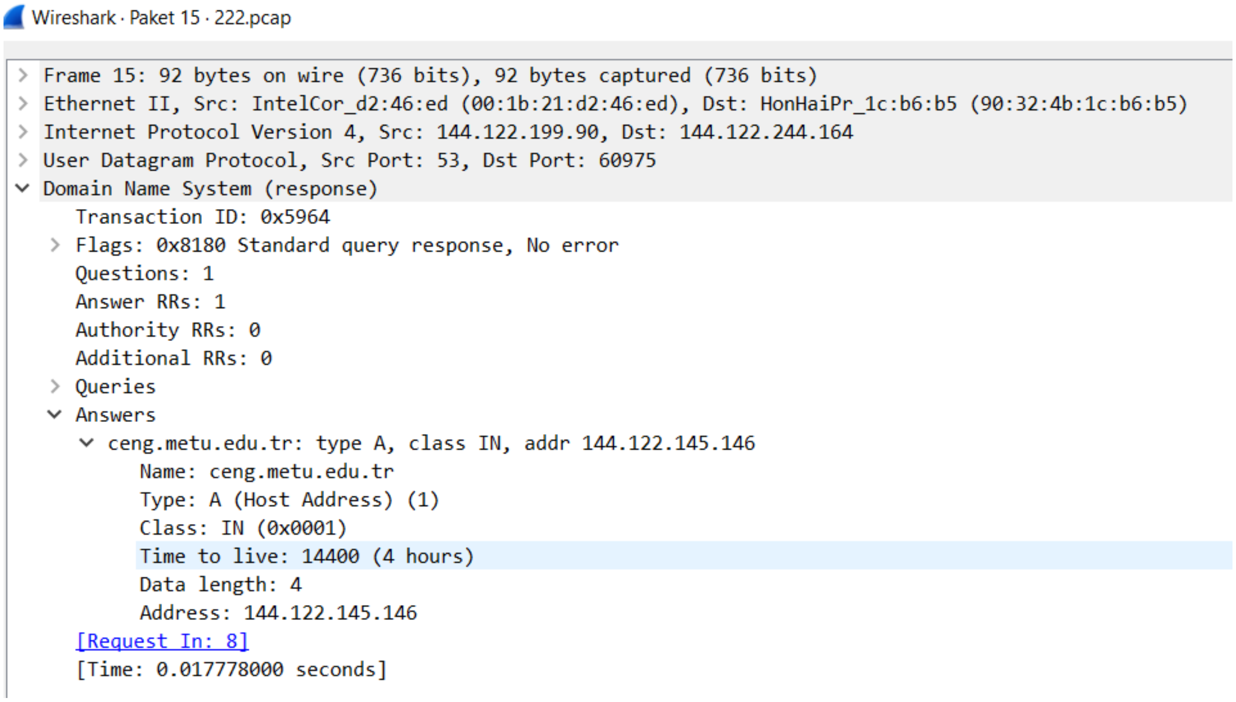
2.3)As we can see underneath and the Picture 1.The DNS query responses have the ip address of 144.122.244.164.



```
15 1.441144    144.122.199.90     144.122.244.164 DNS      92 Standard query response 0x5964 A ceng.metu.edu.tr A 144.122.145.146

25 1.537721    144.122.199.90     144.122.244.164 DNS     123 Standard query response 0xddd5 AAAA ceng.metu.edu.tr SOA ns03.ceng.metu.edu.tr
```

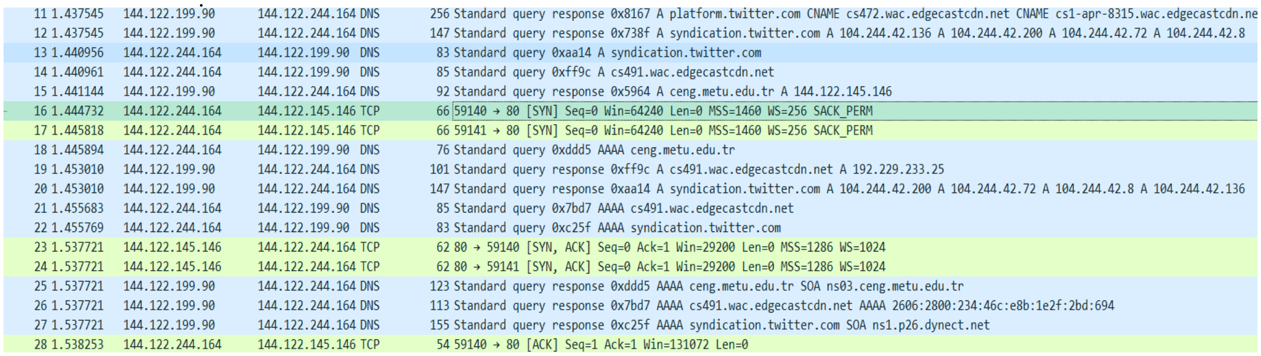
2.4)Since we are hard refreshing page there shouldn't be a cache. But we can see in the response to DNS query, there is a TTL(Time to Live) that says 14400 (4 hours) says that how long to cache a query before requesting a new one. So, I can say that there are no cache at the beginning but after the response came the cache is created.



Wireshark · Paket 15 · 222.pcap

```
> Frame 15: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: HonHaiPr_1c:b6:b5 (90:32:4b:1c:b6:b5)
> Internet Protocol Version 4, Src: 144.122.199.90, Dst: 144.122.244.164
> User Datagram Protocol, Src Port: 53, Dst Port: 60975
v Domain Name System (response)
    Transaction ID: 0x5964
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    v ceng.metu.edu.tr: type A, class IN, addr 144.122.145.146
          Name: ceng.metu.edu.tr
          Type: A (Host Address) (1)
          Class: IN (0x0001)
          Time to live: 14400 (4 hours)
          Data length: 4
          Address: 144.122.145.146
    [Request In: 8]
    [Time: 0.017778000 seconds]
```

2.5)



```
11 1.437545   144.122.199.90    144.122.244.164 DNS   256 Standard query response 0x8167 A platform.twitter.com CNAME cs472.wac.edgecastcdn.net CNAME cs1-apr-8315.wac.edgecastcdn.ne
12 1.437545   144.122.199.90    144.122.244.164 DNS   147 Standard query response 0x738f A syndication.twitter.com A 104.244.42.136 A 104.244.42.200 A 104.244.42.72 A 104.244.42.8
13 1.440956   144.122.244.164   144.122.199.90  DNS    83 Standard query 0xaa14 A syndication.twitter.com
14 1.440961   144.122.244.164   144.122.199.90  DNS    85 Standard query 0xff9c A cs491.wac.edgecastcdn.net
15 1.441144   144.122.199.90    144.122.244.164 DNS    92 Standard query response 0x5964 A ceng.metu.edu.tr A 144.122.145.146
16 1.444732   144.122.244.164   144.122.145.146 TCP    66 59140 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17 1.445818   144.122.244.164   144.122.145.146 TCP    66 59141 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
18 1.445894   144.122.244.164   144.122.199.90  DNS    76 Standard query 0xddd5 AAAA ceng.metu.edu.tr
19 1.453010   144.122.199.90    144.122.244.164 DNS   101 Standard query response 0xff9c A cs491.wac.edgecastcdn.net A 192.229.233.25
20 1.453010   144.122.199.90    144.122.244.164 DNS   147 Standard query response 0xaa14 A syndication.twitter.com A 104.244.42.200 A 104.244.42.72 A 104.244.42.8 A 104.244.42.136
21 1.455683   144.122.244.164   144.122.199.90  DNS    85 Standard query 0x7bd7 AAAA cs491.wac.edgecastcdn.net
22 1.455769   144.122.244.164   144.122.199.90  DNS    83 Standard query 0xc25f AAAA syndication.twitter.com
23 1.537721   144.122.145.146   144.122.244.164 TCP    62 80 → 59140 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024
24 1.537721   144.122.145.146   144.122.244.164 TCP    62 80 → 59141 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024
25 1.537721   144.122.199.90    144.122.244.164 DNS   123 Standard query response 0xddd5 AAAA ceng.metu.edu.tr SOA ns03.ceng.metu.edu.tr
26 1.537721   144.122.199.90    144.122.244.164 DNS   113 Standard query response 0x7bd7 AAAA cs491.wac.edgecastcdn.net AAAA 2606:2800:234:46c:e8b:1e2f:2bd:694
27 1.537721   144.122.199.90    144.122.244.164 DNS   155 Standard query response 0xc25f AAAA syndication.twitter.com SOA ns1.p26.dynect.net
28 1.538253   144.122.244.164   144.122.145.146 TCP    54 59140 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
```

First succesful Request and response pair (Picture 2)

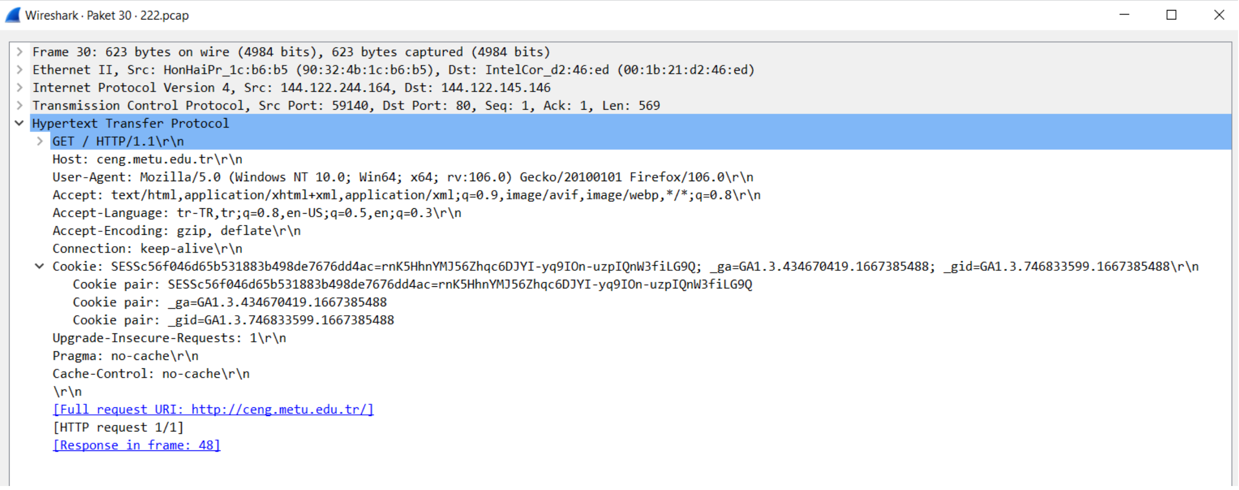
A) Both are TCP

B) TCP is used because since it is the first time we need a secure and strong connection to server without leaving place for errors.TCP only sends data to the listenings clients. It guarantees a reliable tranport between sender and have fail safe protocols like sequencing mechanisms fort o send data correctly and the ACK message that is received when the package is safely delivered. There are flow control so that the receiver wouldn't be overwhelmed and the congestiontion control to arrange the data’s intact arrival without damage and duplication, it also prevent data from arriving out of order.

C) From Picture 2,

1.537721- 1.444732 = 0.092989 s

2.6) Yes, there was we can see the cookie that were sent below.

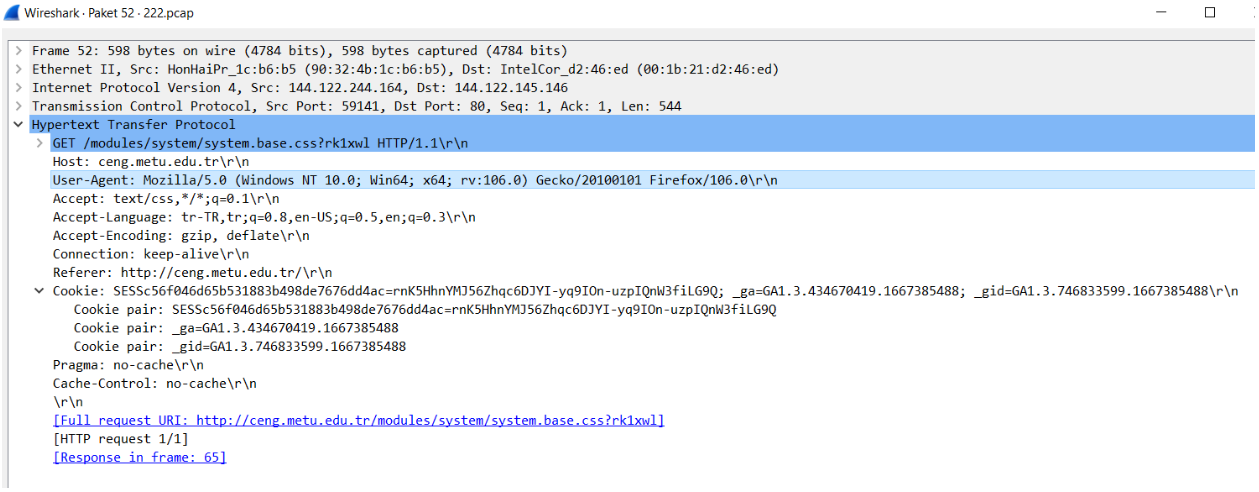


Wireshark · Paket 30 · 222.pcap

```
> Frame 30: 623 bytes on wire (4984 bits), 623 bytes captured (4984 bits)
> Ethernet II, Src: HonHaiPr_1c:b6:b5 (90:32:4b:1c:b6:b5), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.244.164, Dst: 144.122.145.146
> Transmission Control Protocol, Src Port: 59140, Dst Port: 80, Seq: 1, Ack: 1, Len: 569
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: ceng.metu.edu.tr\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
  v Cookie: SESSc56f046d65b531883b498de7676dd4ac=rnK5HhnYMJ56Zhqc6DJYI-yq9IOn-uzpIQnW3fiLG9Q; _ga=GA1.3.434670419.1667385488; _gid=GA1.3.746833599.1667385488\r\n
      Cookie pair: SESSc56f046d65b531883b498de7676dd4ac=rnK5HhnYMJ56Zhqc6DJYI-yq9IOn-uzpIQnW3fiLG9Q
      Cookie pair: _ga=GA1.3.434670419.1667385488
      Cookie pair: _gid=GA1.3.746833599.1667385488
    Upgrade-Insecure-Requests: 1\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://ceng.metu.edu.tr/]
    [HTTP request 1/1]
    [Response in frame: 48]
```

2.7) For this question I will use the http request that has the No 52.

A)



Wireshark · Paket 52 · 222.pcap

```
> Frame 52: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits)
> Ethernet II, Src: HonHaiPr_1c:b6:b5 (90:32:4b:1c:b6:b5), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.244.164, Dst: 144.122.145.146
> Transmission Control Protocol, Src Port: 59141, Dst Port: 80, Seq: 1, Ack: 1, Len: 544
v Hypertext Transfer Protocol
  > GET /modules/system/system.base.css?rk1xwl HTTP/1.1\r\n
    Host: ceng.metu.edu.tr\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0\r\n
    Accept: text/css,*/*;q=0.1\r\n
    Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Referer: http://ceng.metu.edu.tr/\r\n
  v Cookie: SESSc56f046d65b531883b498de7676dd4ac=rnK5HhnYMJ56Zhqc6DJYI-yq9IOn-uzpIQnW3fiLG9Q; _ga=GA1.3.434670419.1667385488; _gid=GA1.3.746833599.1667385488\r\n
      Cookie pair: SESSc56f046d65b531883b498de7676dd4ac=rnK5HhnYMJ56Zhqc6DJYI-yq9IOn-uzpIQnW3fiLG9Q
      Cookie pair: _ga=GA1.3.434670419.1667385488
      Cookie pair: _gid=GA1.3.746833599.1667385488
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://ceng.metu.edu.tr/modules/system/system.base.css?rk1xwl]
    [HTTP request 1/1]
    [Response in frame: 65]
```

B)I was using the Mozilla Firefox. Since this browser developed by Mozilla. The Mozilla and The Firefox is here. Also there is the system information like Windows. Lastly after I looked up, it turned out that the Gecko was also a product of Mozilla and is a browser engine.

3) I researched about the email and email providers. I looked into in what kind of situations that the mail wouldn’t go through. The ‘de’ at the end of ‘merkel@de’ is for de-mail which is a German e-government communications service that makes it possible to exchange electronic documents between citizens, agencies, and businesses over the Internet. So, at this point the problem is whether the mail sent by us will be catched by the system (provider). Providers are generally used by corporations and institutions and provide users with security and ease the communication. The mail is filtered by checking the content of the mail, whether the sender sent tons of mail to many non-existing receivers.