Student Information

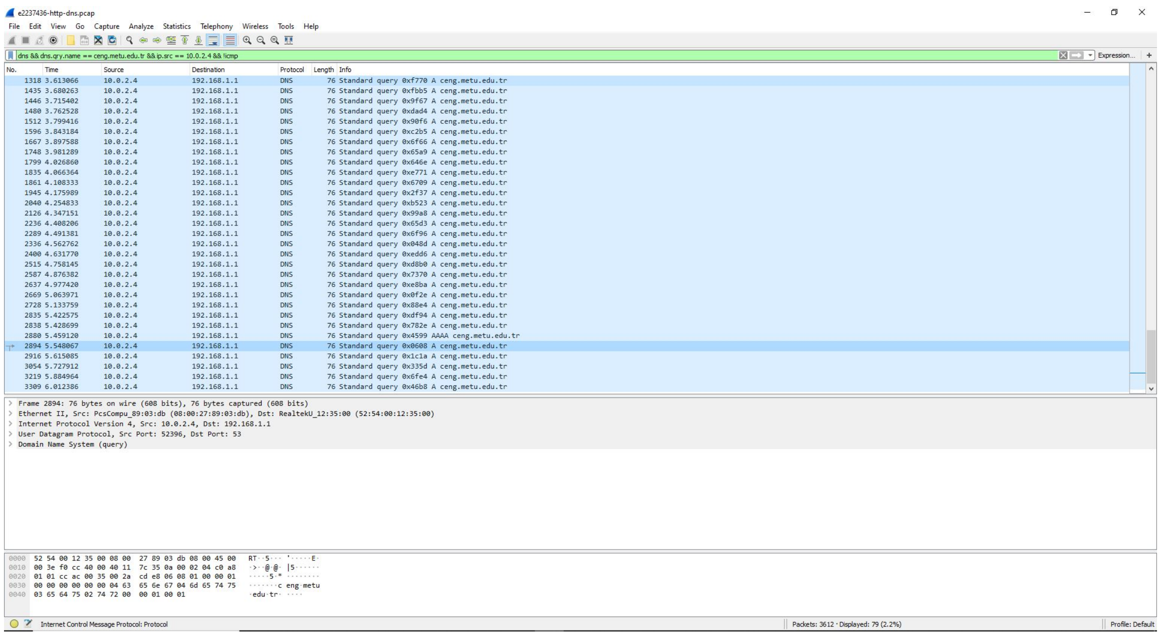
Full Name: Furkan Göksel
Id Number: 2237436

HTTP & DNS (70 Points)

Type your answers under the appropriate subsections.

1. (8 Points)

The number of queries just for ceng.metu.edu.tr is 79.



```
dns && dns.qry.name == ceng.metu.edu.tr && ip.src == 10.0.2.4 && !icmp

No.  Time      Source      Destination   Protocol Length Info
1318 3.613066  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xf770 A ceng.metu.edu.tr
1435 3.680263  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xfbb5 A ceng.metu.edu.tr
1446 3.715402  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x9f67 A ceng.metu.edu.tr
1480 3.762528  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xdad4 A ceng.metu.edu.tr
1512 3.799416  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x90f6 A ceng.metu.edu.tr
1596 3.843184  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xc2b5 A ceng.metu.edu.tr
1667 3.897588  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x6f66 A ceng.metu.edu.tr
1748 3.981289  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x65a9 A ceng.metu.edu.tr
1799 4.026860  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x646e A ceng.metu.edu.tr
1835 4.066364  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xe771 A ceng.metu.edu.tr
1861 4.108333  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x6709 A ceng.metu.edu.tr
1945 4.175989  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x2f37 A ceng.metu.edu.tr
2040 4.254833  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xb523 A ceng.metu.edu.tr
2126 4.347151  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x99a8 A ceng.metu.edu.tr
2236 4.408206  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x65d3 A ceng.metu.edu.tr
2289 4.491381  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x6f96 A ceng.metu.edu.tr
2336 4.562762  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x048d A ceng.metu.edu.tr
2400 4.631770  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xedd6 A ceng.metu.edu.tr
2515 4.758145  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xd8b0 A ceng.metu.edu.tr
2587 4.876382  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x7370 A ceng.metu.edu.tr
2637 4.977420  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xe8ba A ceng.metu.edu.tr
2669 5.063971  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x0f2e A ceng.metu.edu.tr
2728 5.133759  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x88e4 A ceng.metu.edu.tr
2835 5.422575  10.0.2.4    192.168.1.1   DNS      76 Standard query 0xdf94 A ceng.metu.edu.tr
2838 5.428699  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x782e A ceng.metu.edu.tr
2880 5.459120  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x4599 AAAA ceng.metu.edu.tr
2894 5.548067  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x0608 A ceng.metu.edu.tr
2916 5.615085  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x1c1a A ceng.metu.edu.tr
3054 5.727912  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x335d A ceng.metu.edu.tr
3219 5.884964  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x6fe4 A ceng.metu.edu.tr
3309 6.012386  10.0.2.4    192.168.1.1   DNS      76 Standard query 0x46b8 A ceng.metu.edu.tr

> Frame 2894: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Ethernet II, Src: PcsCompu_89:03:db (08:00:27:89:03:db), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
> Internet Protocol Version 4, Src: 10.0.2.4, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 52396, Dst Port: 53
> Domain Name System (query)

0000  52 54 00 12 35 00 08 00  27 89 03 db 08 00 45 00   RT··5···'·····E·
0010  00 3e f0 cc 40 00 40 11  7c 35 0a 00 02 04 c0 a8   ·>··@·@·|5······
0020  01 01 cc ac 00 35 00 2a  cd e8 06 08 01 00 00 01   ·····5·*········
0030  00 00 00 00 00 00 04 63  65 6e 67 04 6d 65 74 75   ·······ceng·metu
0040  03 65 64 75 02 74 72 00  00 01 00 01               ·edu·tr·····

Internet Control Message Protocol: Protocol    Packets: 3612 · Displayed: 79 (2.2%)    Profile: Default
```

e2237436-http-dns.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

Figure 1: DNS Queries

2. (10 Points)

The destination address for the DNS queries is 192.168.1.1 .

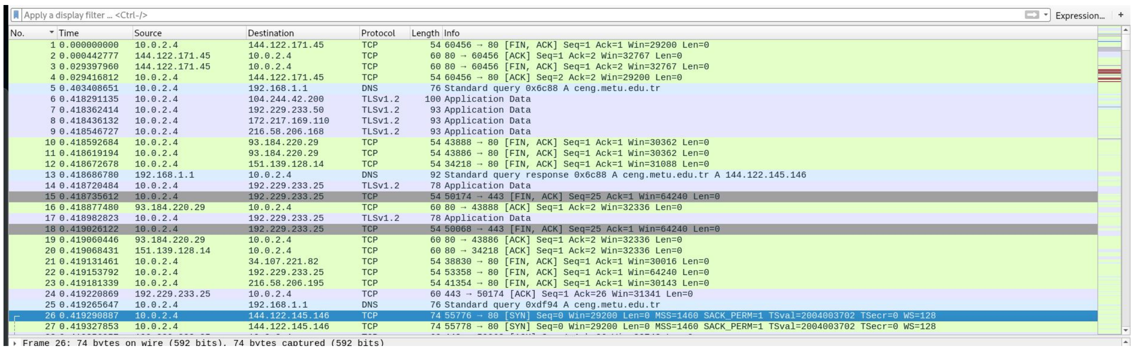
2. (Bonus) (10 Bonus Points)

The address is from my local network and it belongs to my router. According to the pcap file, my computer asked directly without using its local cache.

Also, I think in order to speed up DNS, my router set itself as my DNS server. In this way, it can do its own caching. In my opinion, since in the assignment we were visiting the website twice, the first time it may cached the result and the second time, it may returned the IP address from its cache.

3. (15 Points)

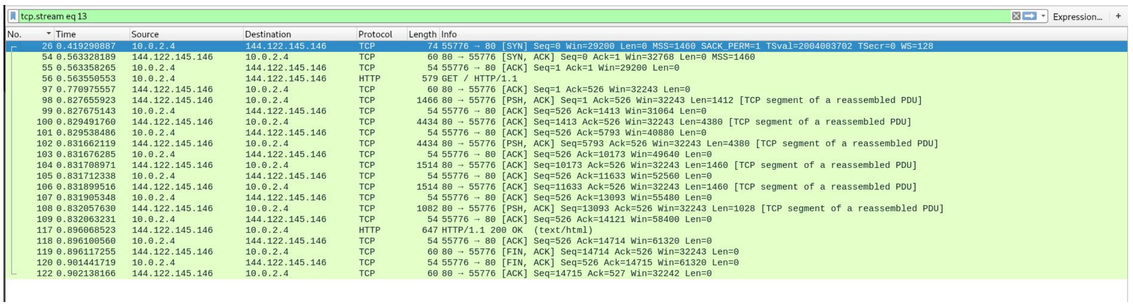
144.122.145.146 was the DNS response and it is the IP address of ceng.metu.edu.tr . As we can see from Figure 2, request packet no is 26.



```
Apply a display filter ... <Ctrl-/>                                                    Expression... +
No.  Time          Source           Destination      Protocol Length Info
   1 0.000000000   10.0.2.4         144.122.171.45   TCP        54 60456 → 80 [FIN, ACK] Seq=1 Ack=1 Win=29200 Len=0
   2 0.000442777   144.122.171.45   10.0.2.4         TCP        60 80 → 60456 [ACK] Seq=1 Ack=2 Win=32767 Len=0
   3 0.029397960   144.122.171.45   10.0.2.4         TCP        60 80 → 60456 [FIN, ACK] Seq=1 Ack=2 Win=32767 Len=0
   4 0.029416812   10.0.2.4         144.122.171.45   TCP        54 60456 → 80 [ACK] Seq=2 Ack=2 Win=29200 Len=0
   5 0.403408651   10.0.2.4         192.168.1.1      DNS        76 Standard query 0x6c88 A ceng.metu.edu.tr
   6 0.418291135   10.0.2.4         104.244.42.200   TLSv1.2   100 Application Data
   7 0.418362414   10.0.2.4         192.229.233.50   TLSv1.2    93 Application Data
   8 0.418436132   10.0.2.4         172.217.169.110  TLSv1.2    93 Application Data
   9 0.418546727   10.0.2.4         216.58.206.168   TLSv1.2    93 Application Data
  10 0.418592684   10.0.2.4         93.184.220.29    TCP        54 43888 → 80 [FIN, ACK] Seq=1 Ack=1 Win=30362 Len=0
  11 0.418619194   10.0.2.4         93.184.220.29    TCP        54 43886 → 80 [FIN, ACK] Seq=1 Ack=1 Win=30362 Len=0
  12 0.418672678   10.0.2.4         151.139.128.14   TCP        54 34218 → 80 [FIN, ACK] Seq=1 Ack=1 Win=31088 Len=0
  13 0.418686780   192.168.1.1      10.0.2.4         DNS        92 Standard query response 0x6c88 A ceng.metu.edu.tr A 144.122.145.146
  14 0.418720484   10.0.2.4         192.229.233.25   TLSv1.2    78 Application Data
  15 0.418735612   10.0.2.4         192.229.233.25   TCP        54 50174 → 443 [FIN, ACK] Seq=25 Ack=1 Win=64240 Len=0
  16 0.418877480   93.184.220.29    10.0.2.4         TCP        60 80 → 43888 [ACK] Seq=1 Ack=2 Win=32336 Len=0
  17 0.418982823   10.0.2.4         192.229.233.25   TLSv1.2    78 Application Data
  18 0.419026122   10.0.2.4         192.229.233.25   TCP        54 50068 → 443 [FIN, ACK] Seq=25 Ack=1 Win=64240 Len=0
  19 0.419060446   93.184.220.29    10.0.2.4         TCP        60 80 → 43886 [ACK] Seq=1 Ack=2 Win=32336 Len=0
  20 0.419068431   151.139.128.14   10.0.2.4         TCP        60 80 → 34218 [ACK] Seq=1 Ack=2 Win=32336 Len=0
  21 0.419131461   10.0.2.4         34.107.221.82    TCP        54 38830 → 80 [FIN, ACK] Seq=1 Ack=1 Win=30016 Len=0
  22 0.419153792   10.0.2.4         192.229.233.25   TCP        54 53358 → 80 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
  23 0.419181339   10.0.2.4         216.58.206.195   TCP        54 41354 → 80 [FIN, ACK] Seq=1 Ack=1 Win=30143 Len=0
  24 0.419220869   192.229.233.25   10.0.2.4         TCP        60 443 → 50174 [ACK] Seq=1 Ack=26 Win=31341 Len=0
  25 0.419265647   10.0.2.4         192.168.1.1      DNS        76 Standard query 0xdf94 A ceng.metu.edu.tr
  26 0.419290887   10.0.2.4         144.122.145.146  TCP        74 55776 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2004003702 TSecr=0 WS=128
  27 0.419327853   10.0.2.4         144.122.145.146  TCP        74 55778 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2004003702 TSecr=0 WS=128
› Frame 26: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
```

Figure 2: Packet that was sent first to the server

After finding the request, in order to find its response, I just followed its TCP Stream. Output is Figure 3. So, its packet no is 54.



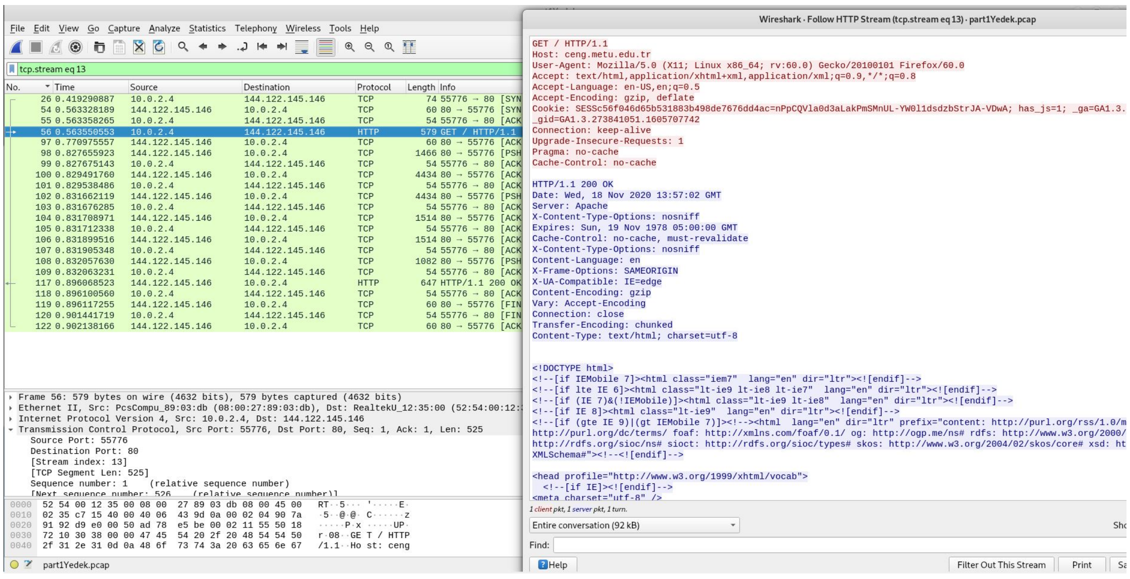
```
tcp.stream eq 13                                                                       Expression... +
No.  Time          Source           Destination      Protocol Length Info
  26 0.419290887   10.0.2.4         144.122.145.146  TCP        74 55776 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2004003702 TSecr=0 WS=128
  54 0.563328189   144.122.145.146  10.0.2.4         TCP        60 80 → 55776 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
  55 0.563358265   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
  56 0.563550553   10.0.2.4         144.122.145.146  HTTP      579 GET / HTTP/1.1
  97 0.770975557   144.122.145.146  10.0.2.4         TCP        60 80 → 55776 [ACK] Seq=1 Ack=526 Win=32243 Len=0
  98 0.827655923   144.122.145.146  10.0.2.4         TCP      1466 80 → 55776 [PSH, ACK] Seq=1 Ack=526 Win=32243 Len=1412 [TCP segment of a reassembled PDU]
  99 0.827675143   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=526 Ack=1413 Win=31064 Len=0
 100 0.829491760   144.122.145.146  10.0.2.4         TCP      4434 80 → 55776 [ACK] Seq=1413 Ack=526 Win=32243 Len=4380 [TCP segment of a reassembled PDU]
 101 0.829538486   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=526 Ack=5793 Win=40880 Len=0
 102 0.831662119   144.122.145.146  10.0.2.4         TCP      4434 80 → 55776 [PSH, ACK] Seq=5793 Ack=526 Win=32243 Len=4380 [TCP segment of a reassembled PDU]
 103 0.831676285   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=526 Ack=10173 Win=49640 Len=0
 104 0.831708971   144.122.145.146  10.0.2.4         TCP      1514 80 → 55776 [ACK] Seq=10173 Ack=526 Win=32243 Len=1460 [TCP segment of a reassembled PDU]
 105 0.831712338   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=526 Ack=11633 Win=52560 Len=0
 106 0.831899516   144.122.145.146  10.0.2.4         TCP      1514 80 → 55776 [ACK] Seq=11633 Ack=526 Win=32243 Len=1460 [TCP segment of a reassembled PDU]
 107 0.831905348   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=526 Ack=13093 Win=55480 Len=0
 108 0.832057630   144.122.145.146  10.0.2.4         TCP      1082 80 → 55776 [PSH, ACK] Seq=13093 Ack=526 Win=32243 Len=1028 [TCP segment of a reassembled PDU]
 109 0.832063231   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=526 Ack=14121 Win=58400 Len=0
 117 0.896068523   144.122.145.146  10.0.2.4         HTTP      647 HTTP/1.1 200 OK  (text/html)
 118 0.896100560   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [ACK] Seq=526 Ack=14714 Win=61320 Len=0
 119 0.896117255   144.122.145.146  10.0.2.4         TCP        60 80 → 55776 [FIN, ACK] Seq=14714 Ack=526 Win=32243 Len=0
 120 0.901441719   10.0.2.4         144.122.145.146  TCP        54 55776 → 80 [FIN, ACK] Seq=526 Ack=14715 Win=61320 Len=0
 122 0.902138166   144.122.145.146  10.0.2.4         TCP        60 80 → 55776 [ACK] Seq=14715 Ack=527 Win=32242 Len=0
```

Figure 3: TCP stream of first request to the server

The reason why it was not a HTTP request and response pair is that HTTP uses and relies on TCP protocol services. In other words, It communicates over TCP Sockets. Before starting the HTTP protocol, it needs to first set up the TCP communication, and these two packets are the part of TCP handshake. After TCP handshake, communication over HTTP protocol was started as it can be seen from Figure 3.

4. (15 Points)

First HTTP request is can be seen from Figure 3 whose packet no is 56, we can see the same result by filtering the packets belong the HTTP protocol. After following the HTTP stream, output is as follows.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 13

```
No.   Time        Source           Destination      Protocol  Length Info
   26 0.419290887 10.0.2.4         144.122.145.146  TCP         74 55776 → 80 [SYN
   54 0.563328189 144.122.145.146  10.0.2.4         TCP         60 80 → 55776 [SYN
   55 0.563358265 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
   56 0.563550553 10.0.2.4         144.122.145.146  HTTP       579 GET / HTTP/1.1
   97 0.770975557 144.122.145.146  10.0.2.4         TCP         60 80 → 55776 [ACK
   98 0.827655923 144.122.145.146  10.0.2.4         TCP       1466 80 → 55776 [PSH
   99 0.827675143 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
  100 0.829491760 144.122.145.146  10.0.2.4         TCP       4434 80 → 55776 [ACK
  101 0.829538486 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
  102 0.831662119 144.122.145.146  10.0.2.4         TCP       4434 80 → 55776 [PSH
  103 0.831676285 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
  104 0.831708971 144.122.145.146  10.0.2.4         TCP       1514 80 → 55776 [ACK
  105 0.831712338 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
  106 0.831899516 144.122.145.146  10.0.2.4         TCP       1514 80 → 55776 [ACK
  107 0.831905348 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
  108 0.832057630 144.122.145.146  10.0.2.4         TCP       1082 80 → 55776 [PSH
  109 0.832063231 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
  117 0.896068523 144.122.145.146  10.0.2.4         HTTP       647 HTTP/1.1 200 OK
  118 0.896100560 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [ACK
  119 0.896117255 144.122.145.146  10.0.2.4         TCP         60 80 → 55776 [FIN
  120 0.901441719 10.0.2.4         144.122.145.146  TCP         54 55776 → 80 [FIN
  122 0.902138166 144.122.145.146  10.0.2.4         TCP         60 80 → 55776 [ACK

▸ Frame 56: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits)
▸ Ethernet II, Src: PcsCompu_89:03:db (08:00:27:89:03:db), Dst: RealtekU_12:35:00 (52:54:00:12:
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 144.122.145.146
▾ Transmission Control Protocol, Src Port: 55776, Dst Port: 80, Seq: 1, Ack: 1, Len: 525
    Source Port: 55776
    Destination Port: 80
    [Stream index: 13]
    [TCP Segment Len: 525]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 526    (relative sequence number)]

0000  52 54 00 12 35 00 08 00  27 89 03 db 08 00 45 00   RT··5···'·····E·
0010  02 35 c7 15 40 00 40 06  43 9d 0a 00 02 04 90 7a   ·5··@·@·C······z
0020  91 92 d9 e0 00 50 ad 78  e5 be 00 02 11 55 50 18   ·····P·x·····UP·
0030  72 10 30 38 00 00 47 45  54 20 2f 20 48 54 54 50   r·08··GET / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 63 65 6e 67   /1.1··Host: ceng
```

part1Yedek.pcap
Wireshark · Follow HTTP Stream (tcp.stream eq 13) · part1Yedek.pcap

```
GET / HTTP/1.1
Host: ceng.metu.edu.tr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: SESSc56f046d65b531883b498de7676dd4ac=nPpCQVla0d3aLakPmSMnUL-YW0l1dsdzbStrJA-VDwA; has_js=1; _ga=GA1.3.
_gid=GA1.3.273841051.1605707742
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Wed, 18 Nov 2020 13:57:02 GMT
Server: Apache
X-Content-Type-Options: nosniff
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Cache-Control: no-cache, must-revalidate
X-Content-Type-Options: nosniff
Content-Language: en
X-Frame-Options: SAMEORIGIN
X-UA-Compatible: IE=edge
Content-Encoding: gzip
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8


<!DOCTYPE html>
<!--[if IEMobile 7]><html class="iem7"  lang="en" dir="ltr"><![endif]-->
<!--[if lte IE 6]><html class="lt-ie9 lt-ie8 lt-ie7"  lang="en" dir="ltr"><![endif]-->
<!--[if (IE 7)&(!IEMobile)]><html class="lt-ie9 lt-ie8"  lang="en" dir="ltr"><![endif]-->
<!--[if IE 8]><html class="lt-ie9"  lang="en" dir="ltr"><![endif]-->
<!--[if (gte IE 9)|(gt IEMobile 7)]><!--><html  lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/m
http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/
http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: ht
XMLSchema#"><!--<![endif]-->

<head profile="http://www.w3.org/1999/xhtml/vocab">
  <!--[if IE]><![endif]-->
<meta charset="utf-8" />
```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (92 kB)

Figure 4: First HTTP Request Stream

Cookies are sent in the Cookie header in the HTTP request. Therefore, yes cookies were sent as it can be seen in Figure 4.

5a. (7 Points)

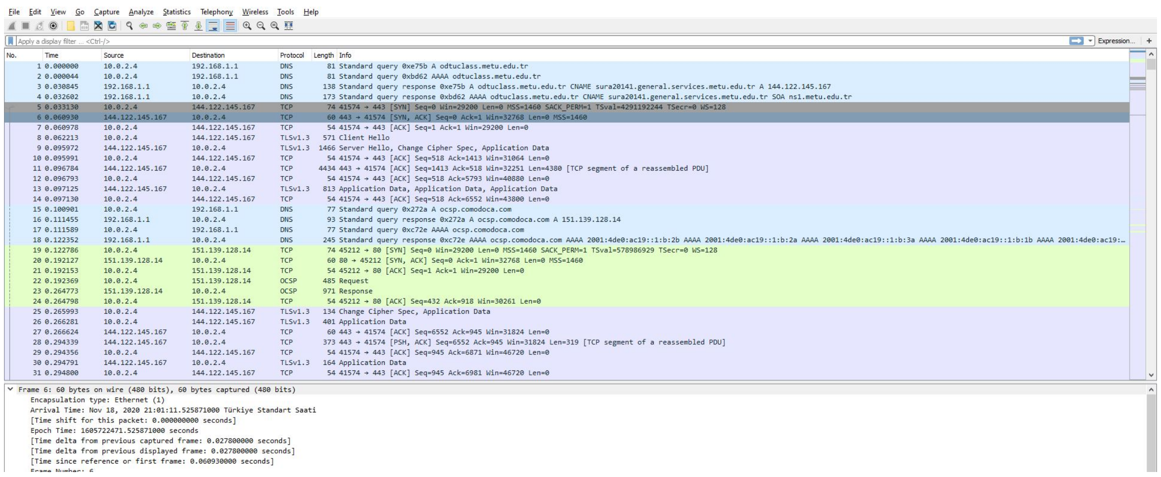
So I chose the first request it is already shown in Figure 4. User-agent string is Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

5b. (15 Points)

I'm using Firefox, and the user agent string includes it. At the beginning of the user agent string, it says Mozilla/5.0 which is a general token that says the browser is Mozilla compatible to eliminate the possibility of being blocked from getting the content (for a historical reason), and it says Gecko version which is the layout engine that displays the formatted content. Also, with the Linux keyword it says, the browser is running on the Linux platform. However, it doesn't include any other browser.

HTTPS & TLS (30 Points)

1. (10 Points)


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

```
No.    Time      Source           Destination      Protocol Length Info
     1 0.000000  10.0.2.4         192.168.1.1      DNS        81 Standard query 0xe75b A odtuclass.metu.edu.tr
     2 0.000044  10.0.2.4         192.168.1.1      DNS        81 Standard query 0xbd62 AAAA odtuclass.metu.edu.tr
     3 0.030845  192.168.1.1      10.0.2.4         DNS       138 Standard query response 0xe75b A odtuclass.metu.edu.tr CNAME sura20141.general.services.metu.edu.tr A 144.122.145.167
     4 0.032602  192.168.1.1      10.0.2.4         DNS       173 Standard query response 0xbd62 AAAA odtuclass.metu.edu.tr CNAME sura20141.general.services.metu.edu.tr SOA ns1.metu.edu.tr
     5 0.033130  10.0.2.4         144.122.145.167  TCP        74 41574 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=4291192244 TSecr=0 WS=128
     6 0.060930  144.122.145.167  10.0.2.4         TCP        60 443 → 41574 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
     7 0.060978  10.0.2.4         144.122.145.167  TCP        54 41574 → 443 [ACK] Seq=1 Ack=1 Win=29200 Len=0
     8 0.062213  10.0.2.4         144.122.145.167  TLSv1.3   571 Client Hello
     9 0.095972  144.122.145.167  10.0.2.4         TLSv1.3  1466 Server Hello, Change Cipher Spec, Application Data
    10 0.095991  10.0.2.4         144.122.145.167  TCP        54 41574 → 443 [ACK] Seq=518 Ack=1413 Win=31064 Len=0
    11 0.096784  144.122.145.167  10.0.2.4         TCP      4434 443 → 41574 [ACK] Seq=1413 Ack=518 Win=32251 Len=4380 [TCP segment of a reassembled PDU]
    12 0.096793  10.0.2.4         144.122.145.167  TCP        54 41574 → 443 [ACK] Seq=518 Ack=5793 Win=40880 Len=0
    13 0.097125  144.122.145.167  10.0.2.4         TLSv1.3   813 Application Data, Application Data, Application Data
    14 0.097130  10.0.2.4         144.122.145.167  TCP        54 41574 → 443 [ACK] Seq=518 Ack=6552 Win=43800 Len=0
    15 0.100901  10.0.2.4         192.168.1.1      DNS        77 Standard query 0x272a A ocsp.comodoca.com
    16 0.111455  192.168.1.1      10.0.2.4         DNS        93 Standard query response 0x272a A ocsp.comodoca.com A 151.139.128.14
    17 0.111589  10.0.2.4         192.168.1.1      DNS        77 Standard query 0xc72e AAAA ocsp.comodoca.com
    18 0.122352  192.168.1.1      10.0.2.4         DNS       245 Standard query response 0xc72e AAAA ocsp.comodoca.com AAAA 2001:4de0:ac19::1:b:2b AAAA 2001:4de0:ac19::1:b:2a AAAA 2001:4de0:ac19::1:b:3a AAAA 2001:4de0:ac19::1:b:1b AAAA 2001:4de0:ac19:…
    19 0.122786  10.0.2.4         151.139.128.14   TCP        74 45212 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=578986929 TSecr=0 WS=128
    20 0.192127  151.139.128.14   10.0.2.4         TCP        60 80 → 45212 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
    21 0.192153  10.0.2.4         151.139.128.14   TCP        54 45212 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
    22 0.192369  10.0.2.4         151.139.128.14   OCSP      485 Request
    23 0.264773  151.139.128.14   10.0.2.4         OCSP      971 Response
    24 0.264798  10.0.2.4         151.139.128.14   TCP        54 45212 → 80 [ACK] Seq=432 Ack=918 Win=30261 Len=0
    25 0.265993  10.0.2.4         144.122.145.167  TLSv1.3   134 Change Cipher Spec, Application Data
    26 0.266281  10.0.2.4         144.122.145.167  TLSv1.3   401 Application Data
    27 0.266624  144.122.145.167  10.0.2.4         TCP        60 443 → 41574 [ACK] Seq=6552 Ack=945 Win=31824 Len=0
    28 0.294339  144.122.145.167  10.0.2.4         TCP       373 443 → 41574 [PSH, ACK] Seq=6552 Ack=945 Win=31824 Len=319 [TCP segment of a reassembled PDU]
    29 0.294356  10.0.2.4         144.122.145.167  TCP        54 41574 → 443 [ACK] Seq=945 Ack=6871 Win=46720 Len=0
    30 0.294791  144.122.145.167  10.0.2.4         TLSv1.3   164 Application Data
    31 0.294800  10.0.2.4         144.122.145.167  TCP        54 41574 → 443 [ACK] Seq=945 Ack=6981 Win=46720 Len=0

v Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 18, 2020 21:01:11.525871000 Türkiye Standart Saati
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1605722471.525871000 seconds
    [Time delta from previous captured frame: 0.027800000 seconds]
    [Time delta from previous displayed frame: 0.027800000 seconds]
    [Time since reference or first frame: 0.060930000 seconds]
    Frame Number: 6
```

Figure 5: First request response pair (5-6)

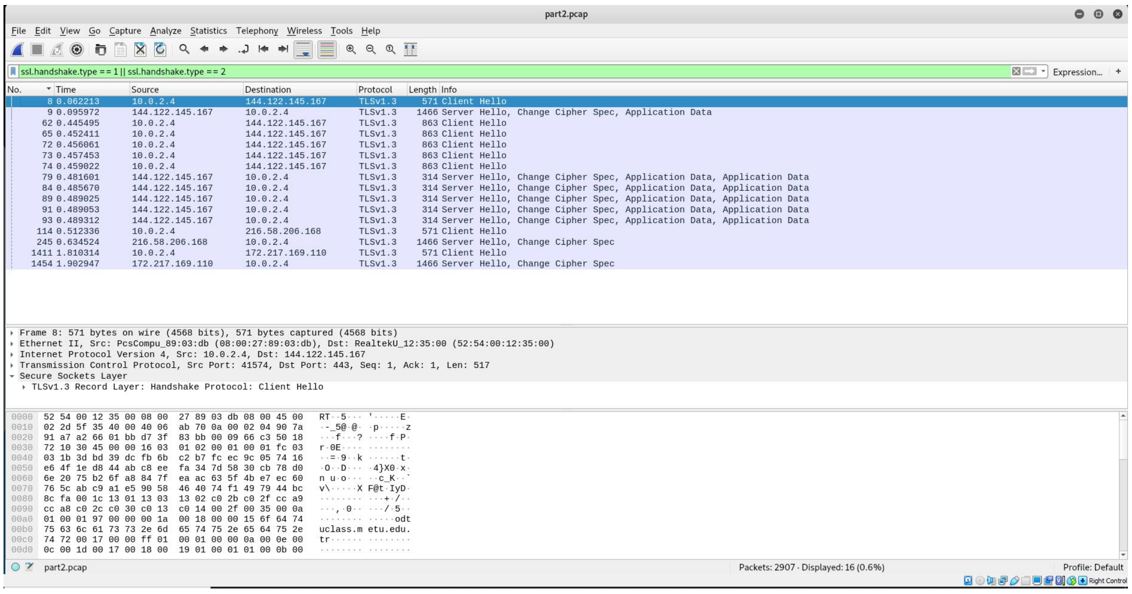
DNS returns us the IP address of it, and it is 144.122.145.167. Then the first request response pair is TCP packet pairs (5-6 No). Time difference is 0.0278 seconds.

2. (10 Points)

Their packets nos are 8 and 9. In the request, ”Client hello” is written, and in the response, ”Server Hello, Change Cipher Spec, Application Data” is written. They are in handshake part of TLS protocol since TLS protocol is initiated by the hello message from client and hello and other information included message from the server.

3. (10 Points)

There are 12 (last four of them are not OdtuClass in screenshot) hello messages in my pcap as you can see from Fig 6. It is more than one because when my browser navigates the main page, the server sends a response that contains the HTML content of the page. However, there are some JS scripts, images, and other data in that content and in order to display the website properly, my browser sends new requests to get these resources using HTTPS. This is why it is more than one.



ssl.handshake.type == 1 || ssl.handshake.type == 2

```
No.     Time        Source            Destination       Protocol  Length Info
      8 0.062213    10.0.2.4          144.122.145.167   TLSv1.3     571 Client Hello
      9 0.095972    144.122.145.167   10.0.2.4          TLSv1.3    1466 Server Hello, Change Cipher Spec, Application Data
     62 0.445495    10.0.2.4          144.122.145.167   TLSv1.3     863 Client Hello
     65 0.452411    10.0.2.4          144.122.145.167   TLSv1.3     863 Client Hello
     72 0.456061    10.0.2.4          144.122.145.167   TLSv1.3     863 Client Hello
     73 0.457453    10.0.2.4          144.122.145.167   TLSv1.3     863 Client Hello
     74 0.459022    10.0.2.4          144.122.145.167   TLSv1.3     863 Client Hello
     79 0.481601    144.122.145.167   10.0.2.4          TLSv1.3     314 Server Hello, Change Cipher Spec, Application Data, Application Data
     84 0.485670    144.122.145.167   10.0.2.4          TLSv1.3     314 Server Hello, Change Cipher Spec, Application Data, Application Data
     89 0.489025    144.122.145.167   10.0.2.4          TLSv1.3     314 Server Hello, Change Cipher Spec, Application Data, Application Data
     91 0.489053    144.122.145.167   10.0.2.4          TLSv1.3     314 Server Hello, Change Cipher Spec, Application Data, Application Data
     93 0.489312    144.122.145.167   10.0.2.4          TLSv1.3     314 Server Hello, Change Cipher Spec, Application Data, Application Data
    114 0.512336    10.0.2.4          216.58.206.168    TLSv1.3     571 Client Hello
    245 0.634524    216.58.206.168    10.0.2.4          TLSv1.3    1466 Server Hello, Change Cipher Spec
   1411 1.810314    10.0.2.4          172.217.169.110   TLSv1.3     571 Client Hello
   1454 1.902947    172.217.169.110   10.0.2.4          TLSv1.3    1466 Server Hello, Change Cipher Spec
```

```
▸ Frame 8: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
▸ Ethernet II, Src: PcsCompu_89:03:db (08:00:27:89:03:db), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
▸ Internet Protocol Version 4, Src: 10.0.2.4, Dst: 144.122.145.167
▸ Transmission Control Protocol, Src Port: 41574, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▾ Secure Sockets Layer
  ▸ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
```

```
0000  52 54 00 12 35 00 08 00  27 89 03 db 08 00 45 00   RT··5··· '·····E·
0010  02 2d 5f 35 40 00 40 06  ab 70 0a 00 02 04 90 7a   ·-_5@·@· ·p·····z
0020  91 a7 a2 66 01 bb d7 3f  83 bb 00 09 66 c3 50 18   ···f···? ····f·P·
0030  72 10 30 45 00 00 16 03  01 02 00 01 00 01 fc 03   r·0E···· ········
0040  03 1b 3d bd 39 dc fb 6b  c2 b7 fc ec 9c 05 74 16   ··=·9··k ······t·
0050  e6 4f 1e d8 44 ab c8 ee  fa 34 7d 58 30 cb 78 d0   ·O··D··· ·4}X0·x·
0060  6e 20 75 b2 6f a8 84 7f  ea ac 63 5f 4b e7 ec 60   n u·o··· ··c_K··`
0070  76 5c ab c9 a1 e5 90 58  46 40 74 f1 49 79 44 bc   v\·····X F@t·IyD·
0080  8c fa 00 1c 13 01 13 03  13 02 c0 2b c0 2f cc a9   ········ ···+·/··
0090  cc a8 c0 2c c0 30 c0 13  c0 14 00 2f 00 35 00 0a   ···,·0·· ···/·5··
00a0  01 00 01 97 00 00 00 1a  00 18 00 00 15 6f 64 74   ········ ·····odt
00b0  75 63 6c 61 73 73 2e 6d  65 74 75 2e 65 64 75 2e   uclass.m etu.edu.
00c0  74 72 00 17 00 00 ff 01  00 01 00 00 0a 00 0e 00   tr······ ········
00d0  0c 00 1d 00 17 00 18 00  19 01 00 01 01 00 0b 00   ········ ········
```

Figure 6: TLS Hello Messages