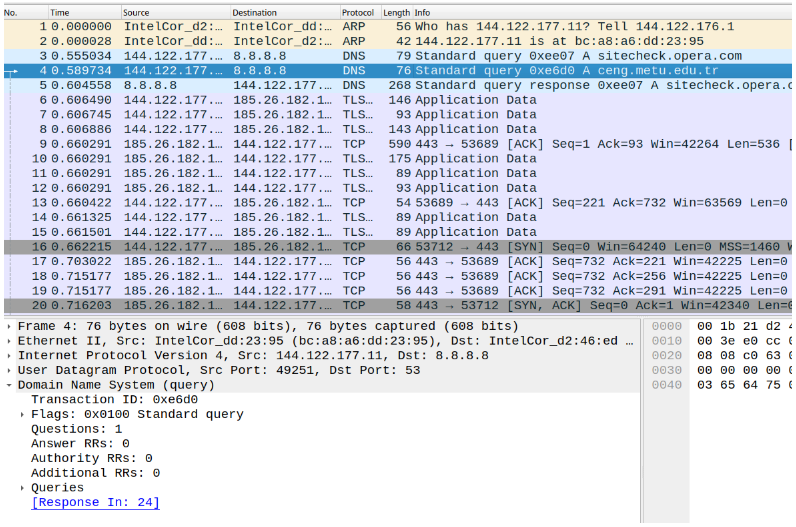
Student Information

Full Name : Ahmet Eren Çolak
Id Number : 2587921

Q. 1

Only 1 query is sent to a DNS server for retrieving the *ceng.metu.edu.tr*'s IP address.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_d2:…	IntelCor_dd:…	ARP	56	Who has 144.122.177.11? Tell 144.122.176.1
2	0.000028	IntelCor_dd:…	IntelCor_d2:…	ARP	42	144.122.177.11 is at bc:a8:a6:dd:23:95
3	0.555034	144.122.177.…	8.8.8.8	DNS	79	Standard query 0xee07 A sitecheck.opera.com
4	0.589734	144.122.177.…	8.8.8.8	DNS	76	Standard query 0xe6d0 A ceng.metu.edu.tr
5	0.604558	8.8.8.8	144.122.177.…	DNS	268	Standard query response 0xee07 A sitecheck.opera.c
6	0.606490	144.122.177.…	185.26.182.1…	TLS…	146	Application Data
7	0.606745	144.122.177.…	185.26.182.1…	TLS…	93	Application Data
8	0.606886	144.122.177.…	185.26.182.1…	TLS…	143	Application Data
9	0.660291	185.26.182.1…	144.122.177.…	TCP	590	443 → 53689 [ACK] Seq=1 Ack=93 Win=42264 Len=536 [
10	0.660291	185.26.182.1…	144.122.177.…	TLS…	175	Application Data
11	0.660291	185.26.182.1…	144.122.177.…	TLS…	89	Application Data
12	0.660291	185.26.182.1…	144.122.177.…	TLS…	93	Application Data
13	0.660422	144.122.177.…	185.26.182.1…	TCP	54	53689 → 443 [ACK] Seq=221 Ack=732 Win=63569 Len=0
14	0.661325	144.122.177.…	185.26.182.1…	TLS…	89	Application Data
15	0.661501	144.122.177.…	185.26.182.1…	TLS…	89	Application Data
16	0.662215	144.122.177.…	185.26.182.1…	TCP	66	53712 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
17	0.703022	185.26.182.1…	144.122.177.…	TCP	56	443 → 53689 [ACK] Seq=732 Ack=221 Win=42225 Len=0
18	0.715177	185.26.182.1…	144.122.177.…	TCP	56	443 → 53689 [ACK] Seq=732 Ack=256 Win=42225 Len=0
19	0.715177	185.26.182.1…	144.122.177.…	TCP	56	443 → 53689 [ACK] Seq=732 Ack=291 Win=42225 Len=0
20	0.716203	185.26.182.1…	144.122.177.…	TCP	58	443 → 53712 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0

```
› Frame 4: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)            0000  00 1b 21 d2
› Ethernet II, Src: IntelCor_dd:23:95 (bc:a8:a6:dd:23:95), Dst: IntelCor_d2:46:ed …  0010  00 3e e0 cc
› Internet Protocol Version 4, Src: 144.122.177.11, Dst: 8.8.8.8                 0020  08 08 c0 63
› User Datagram Protocol, Src Port: 49251, Dst Port: 53                          0030  00 00 00 00
⌄ Domain Name System (query)                                                     0040  03 65 64 75
    Transaction ID: 0xe6d0
  › Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  › Queries
    [Response In: 24]
```

Q. 2

Only 1 server is queried for the DNS request.

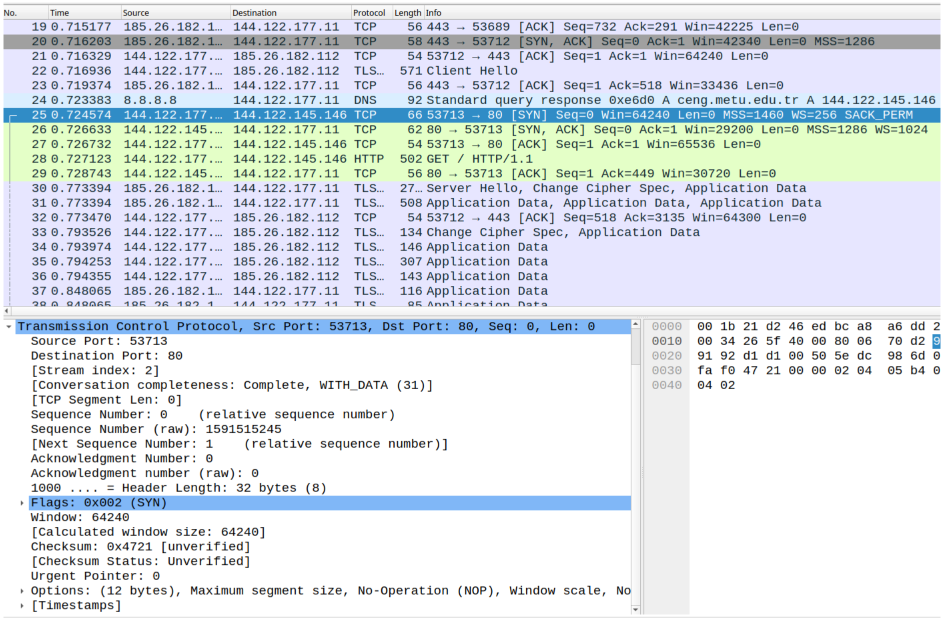
Q. 3

IP address of the queried DNS server is 8.8.8.8

Q. 4

It is not possible to tell whether the response is cached or not. If there were multiple DNS requests, then it would be possible to tell whether it is cached by comparing TTL times of responses.

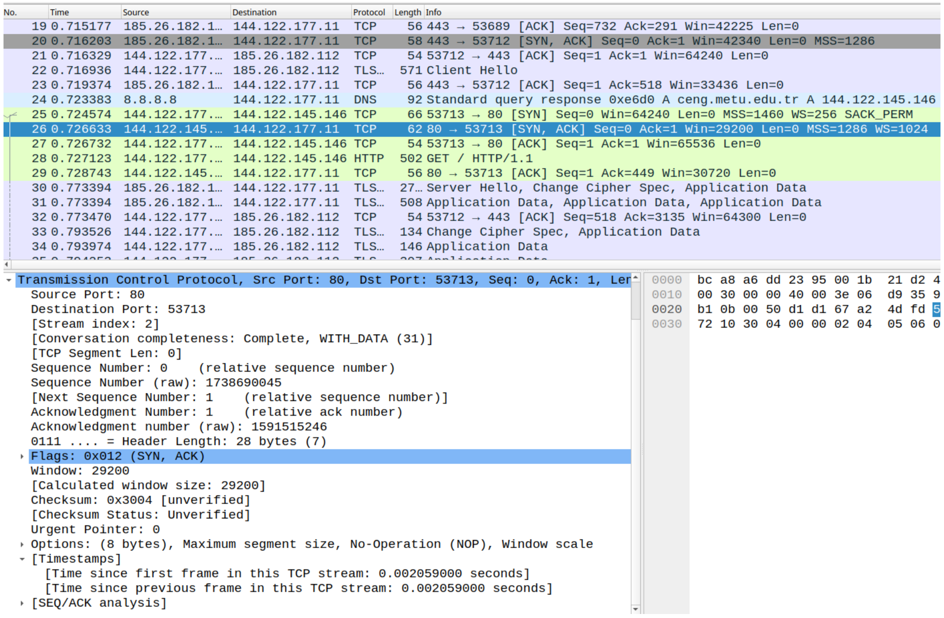
Q. 5



```
No.  Time     Source           Destination      Protocol Length Info
  19 0.715177 185.26.182.1…    144.122.177.11   TCP        56 443 → 53689 [ACK] Seq=732 Ack=291 Win=42225 Len=0
  20 0.716203 185.26.182.1…    144.122.177.11   TCP        58 443 → 53712 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1286
  21 0.716329 144.122.177.…    185.26.182.112   TCP        54 53712 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  22 0.716936 144.122.177.…    185.26.182.112   TLS…      571 Client Hello
  23 0.719374 185.26.182.1…    144.122.177.11   TCP        56 443 → 53712 [ACK] Seq=1 Ack=518 Win=33436 Len=0
  24 0.723383 8.8.8.8          144.122.177.11   DNS        92 Standard query response 0xe6d0 A ceng.metu.edu.tr A 144.122.145.146
  25 0.724574 144.122.177.…    144.122.145.146  TCP        66 53713 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  26 0.726633 144.122.145.…    144.122.177.11   TCP        62 80 → 53713 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024
  27 0.726732 144.122.177.…    144.122.145.146  TCP        54 53713 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  28 0.727123 144.122.177.…    144.122.145.146  HTTP      502 GET / HTTP/1.1
  29 0.728743 144.122.145.…    144.122.177.11   TCP        56 80 → 53713 [ACK] Seq=1 Ack=449 Win=30720 Len=0
  30 0.773394 185.26.182.1…    144.122.177.11   TLS…      27… Server Hello, Change Cipher Spec, Application Data
  31 0.773394 185.26.182.1…    144.122.177.11   TLS…      508 Application Data, Application Data, Application Data
  32 0.773470 144.122.177.…    185.26.182.112   TCP        54 53712 → 443 [ACK] Seq=518 Ack=3135 Win=64300 Len=0
  33 0.793526 144.122.177.…    185.26.182.112   TLS…      134 Change Cipher Spec, Application Data
  34 0.793974 144.122.177.…    185.26.182.112   TLS…      146 Application Data
  35 0.794253 144.122.177.…    185.26.182.112   TLS…      307 Application Data
  36 0.794355 144.122.177.…    185.26.182.112   TLS…      143 Application Data
  37 0.848065 185.26.182.1…    144.122.177.11   TLS…      116 Application Data
  38 0.848065 185.26.182.1…    144.122.177.11   TLS…       85 Application Data
```

```
Transmission Control Protocol, Src Port: 53713, Dst Port: 80, Seq: 0, Len: 0
  Source Port: 53713
  Destination Port: 80
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0    (relative sequence number)
  Sequence Number (raw): 1591515245
  [Next Sequence Number: 1    (relative sequence number)]
  Acknowledgment Number: 0
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
  Flags: 0x002 (SYN)
  Window: 64240
  [Calculated window size: 64240]
  Checksum: 0x4721 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No
  [Timestamps]
```

```
0000  00 1b 21 d2 46 ed bc a8  a6 dd 2
0010  00 34 26 5f 40 00 80 06  70 d2 9
0020  91 92 d1 d1 00 50 5e dc  98 6d 0
0030  fa f0 47 21 00 00 02 04  05 b4 0
0040  04 02
```



```
No.  Time     Source           Destination      Protocol Length Info
  19 0.715177 185.26.182.1…    144.122.177.11   TCP        56 443 → 53689 [ACK] Seq=732 Ack=291 Win=42225 Len=0
  20 0.716203 185.26.182.1…    144.122.177.11   TCP        58 443 → 53712 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1286
  21 0.716329 144.122.177.…    185.26.182.112   TCP        54 53712 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  22 0.716936 144.122.177.…    185.26.182.112   TLS…      571 Client Hello
  23 0.719374 185.26.182.1…    144.122.177.11   TCP        56 443 → 53712 [ACK] Seq=1 Ack=518 Win=33436 Len=0
  24 0.723383 8.8.8.8          144.122.177.11   DNS        92 Standard query response 0xe6d0 A ceng.metu.edu.tr A 144.122.145.146
  25 0.724574 144.122.177.…    144.122.145.146  TCP        66 53713 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  26 0.726633 144.122.145.…    144.122.177.11   TCP        62 80 → 53713 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024
  27 0.726732 144.122.177.…    144.122.145.146  TCP        54 53713 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  28 0.727123 144.122.177.…    144.122.145.146  HTTP      502 GET / HTTP/1.1
  29 0.728743 144.122.145.…    144.122.177.11   TCP        56 80 → 53713 [ACK] Seq=1 Ack=449 Win=30720 Len=0
  30 0.773394 185.26.182.1…    144.122.177.11   TLS…      27… Server Hello, Change Cipher Spec, Application Data
  31 0.773394 185.26.182.1…    144.122.177.11   TLS…      508 Application Data, Application Data, Application Data
  32 0.773470 144.122.177.…    185.26.182.112   TCP        54 53712 → 443 [ACK] Seq=518 Ack=3135 Win=64300 Len=0
  33 0.793526 144.122.177.…    185.26.182.112   TLS…      134 Change Cipher Spec, Application Data
  34 0.793974 144.122.177.…    185.26.182.112   TLS…      146 Application Data
```

```
Transmission Control Protocol, Src Port: 80, Dst Port: 53713, Seq: 0, Ack: 1, Ler
  Source Port: 80
  Destination Port: 53713
  [Stream index: 2]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 0]
  Sequence Number: 0    (relative sequence number)
  Sequence Number (raw): 1738690045
  [Next Sequence Number: 1    (relative sequence number)]
  Acknowledgment Number: 1    (relative ack number)
  Acknowledgment number (raw): 1591515246
  0111 .... = Header Length: 28 bytes (7)
  Flags: 0x012 (SYN, ACK)
  Window: 29200
  [Calculated window size: 29200]
  Checksum: 0x3004 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  Options: (8 bytes), Maximum segment size, No-Operation (NOP), Window scale
  [Timestamps]
    [Time since first frame in this TCP stream: 0.002059000 seconds]
    [Time since previous frame in this TCP stream: 0.002059000 seconds]
  [SEQ/ACK analysis]
```

```
0000  bc a8 a6 dd 23 95 00 1b  21 d2 4
0010  00 30 00 00 40 00 3e 06  d9 35 9
0020  b1 0b 00 50 d1 d1 67 a2  4d fd 5
0030  72 10 30 04 00 00 02 04  05 06 0
```

a.

Protocol of these requests is TCP.

b.

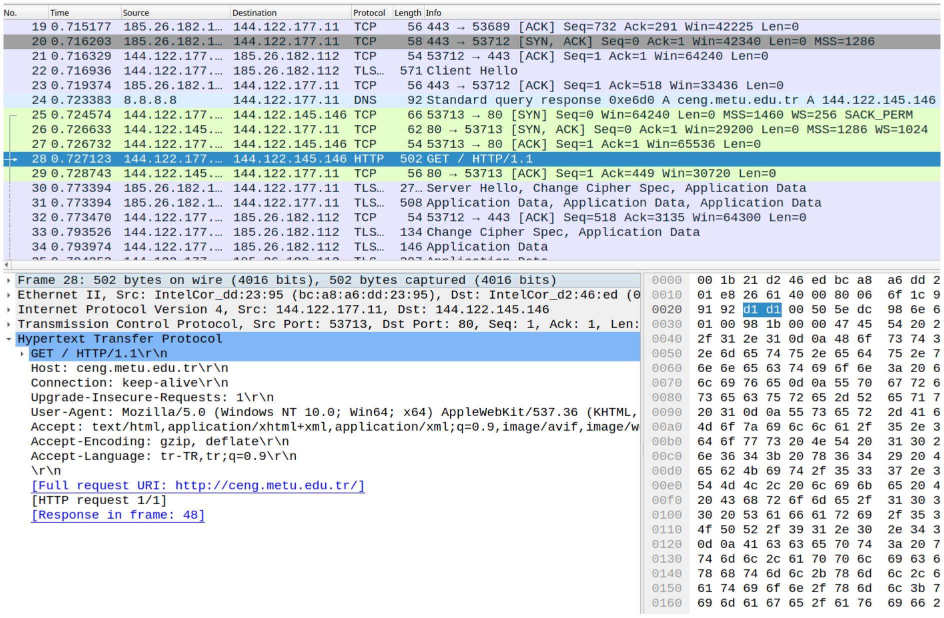
HTTP is relies on TCP. Thus, a TCP connection must be established before exchanging HTTP messages. Because of that the protocol used in first request and response pair is TCP.

c.

It is 0.002059 seconds.

Q. 6

No, there is not any cookies sent with the first HTTP request.



```
No.  Time      Source          Destination     Protocol Length Info
  19 0.715177  185.26.182.1…   144.122.177.11  TCP       56 443 → 53689 [ACK] Seq=732 Ack=291 Win=42225 Len=0
  20 0.716203  185.26.182.1…   144.122.177.11  TCP       58 443 → 53712 [SYN, ACK] Seq=0 Ack=1 Win=42340 Len=0 MSS=1286
  21 0.716329  144.122.177.…   185.26.182.112  TCP       54 53712 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  22 0.716936  144.122.177.…   185.26.182.112  TLS…     571 Client Hello
  23 0.719374  185.26.182.1…   144.122.177.11  TCP       56 443 → 53712 [ACK] Seq=1 Ack=518 Win=33436 Len=0
  24 0.723383  8.8.8.8         144.122.177.11  DNS       92 Standard query response 0xe6d0 A ceng.metu.edu.tr A 144.122.145.146
  25 0.724574  144.122.177.…   144.122.145.146 TCP       66 53713 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  26 0.726633  144.122.145.…   144.122.177.11  TCP       62 80 → 53713 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024
  27 0.726732  144.122.177.…   144.122.145.146 TCP       54 53713 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  28 0.727123  144.122.177.…   144.122.145.146 HTTP     502 GET / HTTP/1.1
  29 0.728743  144.122.145.…   144.122.177.11  TCP       56 80 → 53713 [ACK] Seq=1 Ack=449 Win=30720 Len=0
  30 0.773394  185.26.182.1…   144.122.177.11  TLS…     27… Server Hello, Change Cipher Spec, Application Data
  31 0.773394  185.26.182.1…   144.122.177.11  TLS…     508 Application Data, Application Data, Application Data
  32 0.773470  144.122.177.…   185.26.182.112  TCP       54 53712 → 443 [ACK] Seq=518 Ack=3135 Win=64300 Len=0
  33 0.793526  144.122.177.…   185.26.182.112  TLS…     134 Change Cipher Spec, Application Data
  34 0.793974  144.122.177.…   185.26.182.112  TLS…     146 Application Data
```

```
› Frame 28: 502 bytes on wire (4016 bits), 502 bytes captured (4016 bits)
› Ethernet II, Src: IntelCor_dd:23:95 (bc:a8:a6:dd:23:95), Dst: IntelCor_d2:46:ed (0
› Internet Protocol Version 4, Src: 144.122.177.11, Dst: 144.122.145.146
› Transmission Control Protocol, Src Port: 53713, Dst Port: 80, Seq: 1, Ack: 1, Len:
⌄ Hypertext Transfer Protocol
  › GET / HTTP/1.1\r\n
    Host: ceng.metu.edu.tr\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9\r\n
    \r\n
    [Full request URI: http://ceng.metu.edu.tr/]
    [HTTP request 1/1]
    [Response in frame: 48]
```

```
0000  00 1b 21 d2 46 ed bc a8  a6 dd 2
0010  01 e8 26 61 40 00 80 06  6f 1c 9
0020  91 92 d1 d1 00 50 5e dc  98 6e 6
0030  01 00 98 1b 00 00 47 45  54 20 2
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3
0050  2e 6d 65 74 75 2e 65 64  75 2e 7
0060  6e 6e 65 63 74 69 6f 6e  3a 20 6
0070  6c 69 76 65 0d 0a 55 70  67 72 6
0080  73 65 63 75 72 65 2d 52  65 71 7
0090  20 31 0d 0a 55 73 65 72  2d 41 6
00a0  4d 6f 7a 69 6c 6c 61 2f  35 2e 3
00b0  64 6f 77 73 20 4e 54 20  31 30 2
00c0  6e 36 34 3b 20 78 36 34  29 20 4
00d0  65 62 4b 69 74 2f 35 33  37 2e 3
00e0  54 4d 4c 2c 20 6c 69 6b  65 20 4
00f0  20 43 68 72 6f 6d 65 2f  31 30 3
0100  30 20 53 61 66 61 72 69  2f 35 3
0110  4f 50 52 2f 39 31 2e 30  2e 34 3
0120  0d 0a 41 63 63 65 70 74  3a 20 7
0130  74 6d 6c 2c 61 70 70 6c  69 63 6
0140  78 68 74 6d 6c 2b 78 6d  6c 2c 6
0150  61 74 69 6f 6e 2f 78 6d  6c 3b 7
0160  69 6d 61 67 65 2f 61 76  69 66 2
```

Q. 7

a.

It is: ”User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36 OPR/91.0.4516.77”

b.

User-agent string include the browser I used which was Opera. It can be seen at the end of the string (”OPR/91.0.4516.77”). It also mentions about Safari and Chrome. This is probably because Opera wants web servers to identify itself as Chrome or Safari as well.

DNS

It is not possible to send an email to *merkel@de*. Because domain name of the email server (”de”) lacks a top level domain. Therefore DNS servers will not be able to resolve it.