

## Questions

1. Only 1 query was sent from my computer to DNS server to get the address "ceng.metu.edu.tr".

```
> 28 0.678312      144.122.113.108    144.122.199.90    DNS      76 [Standard query 0x8146 AAAA ceng.metu.edu.tr]
```

2. Only 1 DNS server

```
> Frame 29: 123 bytes on wire (984 bits), 123 bytes captured (984 bits)
> Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: RivetNet_c0:fb:b3 (9c:b6:d0:c0:fb:b3)
> Internet Protocol Version 4, Src: 144.122.199.90, Dst: 144.122.113.108
> User Datagram Protocol, Src Port: 53, Dst Port: 54761
▼ Domain Name System (response)
  Transaction ID: 0x8146
  Flags: 0x8180 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 1
  Additional RRs: 0
  ▼ Queries
    > ceng.metu.edu.tr: type AAAA, class IN
  ▼ Authoritative nameservers
    > ceng.metu.edu.tr: type SOA, class IN, mname ns03.ceng.metu.edu.tr
    [Request In: 28]
  [Time: 0.006840000 seconds]
```

## 3.144.122.199.90

```
- 29 0.685152      144.122.199.90    144.122.113.108    DNS      123 [Standard query response 0x8146 AAAA ceng.metu.edu.tr SOA ns03.ceng.metu.edu.tr]
```

4. Yes it is cached since we have Time to live parameter in response packet.

```
  Class: IN (0x0001)
▼ Authoritative nameservers
  ▼ ceng.metu.edu.tr: type SOA, class IN, mname ns03.ceng.metu.edu.tr
    Name: ceng.metu.edu.tr
    Type: SOA (Start Of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 35
    Primary name server: ns03.ceng.metu.edu.tr
    Responsible authority's mailbox: admin.ceng.metu.edu.tr
    Serial Number: 2022110200
```

## 5.

```
[ 4 0.668708      144.122.113.108    144.122.145.146    TCP      66 50345 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  21 0.672644      144.122.145.146    144.122.113.108    TCP      62 80 → 50345 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024]
```

- a) TCP Protocol

b) A TCP handshake SYN-(SYN-ACK) is required in order to establish a connection. After this, data can be sent. Additionally, HTTP is application layer protocol which is on top of TCP(transport layer), that's why we first need TCP handshake.

c)  $0.672644 - 0.668708 = 0.003936$

6) Yes a cookie was sent with the first HTTP request.

```
✓ 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:107.0) Gecko/20100101 Firefox/107.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
  ✓ Cookie: SESSc56f046d65b531883b498de7676dd4ac=2kEoIqXU3fPf1TwUpFd1V95CRT6abJNqHSSEpZIH82w; _ga=GA1.3.1377998770.1667408067; _gid=GA1.3.1993646164.1667408067\r\n
    Cookie pair: SESSc56f046d65b531883b498de7676dd4ac=2kEoIqXU3fPf1TwUpFd1V95CRT6abJNqHSSEpZIH82w
    Cookie pair: _ga=GA1.3.1377998770.1667408067
    Cookie pair: _gid=GA1.3.1993646164.1667408067
  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: 173]
```

7)

a) User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0

```
✓ 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:107.0) Gecko/20100101 Firefox/107.0\r\n
```

b) Yes, the user-agent string includes the browser that I'm using. It also includes operating system that my computer has. "Gecko/20100101" which is rendering engine and its version which Firefox is based on. We also see "Mozilla/5.0" which is a general token that says the browser is Mozilla compatible, and is common to almost every browser today. "Firefox/107.0" which is the browser and its version that was being used.

## DNS

No we can't. Because valid email address has four parts. Recipient name, @ symbol, domain name and top-level domain. For the address "merkel@de", we have recipient name (merkel), @ symbol and country code top-level domain(de), but we don't have domain name which should be after the @ symbol.

For instance: "[merkel@domainname.de](mailto:merkel@domainname.de)" can be a valid email address.