CENG 435 - Data Communications and Networking Fall 2022-2023

THE - 1

Sezgin, Mustafa e2380863@ceng.metu.edu.tr

October 30, 2022

HTTP

1. Only one DNS query was sent to the DNS server to get the IP address of ceng.metu.edu.tr (see Figure 1).

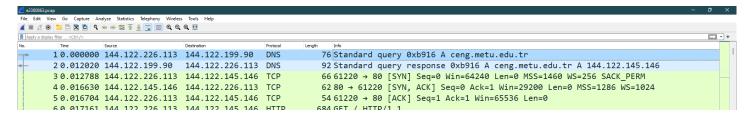


Figure 1: DNS query packet (highlighted)

2. Only one DNS server was queried. This is a standard query with Recursion Desired (RD) flag set and the queried Resource Record (RR) is of type A (see Figure 1 and Figure 2).

```
Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
  Ethernet II, Src: IntelCor_5f:e2:e5 (1c:1b:b5:5f:e2:e5), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
  Internet Protocol Version 4, Src: 144.122.226.113, Dst: 144.122.199.90
  User Datagram Protocol, Src Port: 61685, Dst Port: 53

    Domain Name System (query)

    Transaction ID: 0xb916
   Flags: 0x0100 Standard query
      0... .... = Response: Message is a query
       .000 0... = Opcode: Standard query (θ)
       .....0. .... = Truncated: Message is not truncated
       \dots .... 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
   Oueries
     v ceng.metu.edu.tr: tvpe A, class IN
        Name: ceng.metu.edu.tr
         [Name Length: 16]
         [Label Count: 4]
         Type: A (Host Address) (1)
         Class: IN (0x0001)
    [Response In: 2]
Show packet bytes
                                                                                    Close
```

Figure 2: DNS request header details

3. The IP address of the queried DNS server is 144.122.199.90 as seen in the destination address field in the IP header of the DNS request (see Figure 3).

```
Wireshark · Packet 1 · e2380863.pcap
  Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
  Ethernet II, Src: IntelCor_5f:e2:e5 (1c:1b:b5:5f:e2:e5), Dst: IntelCor_d2:46:ed (00:1b:21:d2:46:ed)
Internet Protocol Version 4, Src: 144.122.226.113, Dst: 144.122.199.90
     0100 .... = Version: 4
       .. 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 62
     Identification: 0xe469 (58473)
    000. .... = Flags: 0x0
      ..0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 128
Protocol: UDP (17)
     Header Checksum: 0x0000 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 144.122.226.113
     Destination Address: 144.122.199.90
  User Datagram Protocol, Src Port: 61685, Dst Port: 53
  Domain Name System (query)
Show packet bytes
                                                                                          Close
```

Figure 3: DNS request network layer header details

4. Time to live (TTL) field of the answer has a value of 14400 as seen in the header of the DNS response (see Figure 4). This tells us that the answer is valid for 14400 seconds (4 hours) and it is probably cached in the local DNS server and/or my computer to be used in the next 4 hours after the query. However, we cannot say anything about whether the Resource Record (RR) was cached before and comes from a cache DNS server.

```
Frame 2: 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: IntelCor_5f:e2:e5 (1c:1b:b5:5f:e2:e5)
  Internet Protocol Version \overline{4}, Src: 144.122.199.90, Dst: 144.122.226.113 User Datagram Protocol, Src Port: 53, Dst Port: 61685

    Domain Name System (response)

     Transaction ID: 0xb916

    Flags: 0x8180 Standard query response, No error

             .... = Response: Message is a response
        .000 0...... = Opcode: Standard query (0) ..... 0..... = Authoritative: Server is not an authority for domain
        ..... ..0. .... = Truncated: Message is not truncated
        .... ...1 .... = Recursion desired: Do query recursively
        \ldots 1... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
        \dots .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... 0 .... = Non-authenticated data: Unacceptable
        .... .... 0000 = Reply code: No error (0)
     Questions: 1
     Answer RRs: 1
     Authority RRs: 0
     Additional RRs: 0

  Δnswers

      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: 1]
     [Time: 0.012020000 seconds]
No.; 2 · Time: 0.012020 · Source: 144.122.199.90 · Destination: 144.122.256.113 · Protocol: DNS · Length: 92 · Info: Standard query response 0:b916 A ceng.metu.edu.tr A 144.122.145.146
Show packet bytes
                                                                                                            Close
                                                                                                                         Help
```

Figure 4: DNS response header details

- 5. The first successful pair consists of a GET request to the home page of ceng.metu.edu.tr and a response with the status code 200 (OK) containing the HTML file. This communication can be seen in Figure 5 from start to end of the TCP connection between my computer and the server.
 - (a) The request and response uses Hypertext Transfer Protocol (HTTP) version 1.1 on top of TCP/IP.
 - (b) HTTP is an application layer protocol that is used for transferring web objects. In this case, the object is an HTML file containing the CENG website data, and the most suitable protocol for transferring this HTML file is HTTP
 - (c) The request and response occur respectively at 0.017161 seconds and 0.220814 seconds from the start of the whole capture (see Figure 5). Therefore, the time difference between the request and the response is 0.203653 seconds.

```
E Edit View Co Capture Analyze Statistics Telephony Wireless Jools
                                                                                                                                                      X - +
     3 0.012788 144.122.226.113 144.122.145.146 TCP
                                                                 66 61220 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM
     4 0.016630 144.122.145.146
                                                                 62 80 → 61220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024
                                  144.122.226.113
     5 0.016704 144.122.226.113 144.122.145.146
                                                    TCP
                                                                 54 61220 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
     6 0.017161 144.122.226.113
                                  144.122.145.146 HTTP
                                                                684 GET / HTTP/1.1
     7 0.019103 144.122.145.146 144.122.226.113 TCP
                                                                 56.80 \rightarrow 61220 [ACK] Seq=1 Ack=631 Win=30720 Len=0
                                                              12914 80 → 61220 [ACK] Seq=1 Ack=631 Win=30720 Len=12860 [TCP segment of a reassembled PC
     8 0 . 15 2 0 8 3 1 4 4 . 1 2 2 . 1 4 5 . 1 4 6 1 4 4 . 1 2 2 . 2 2 6 . 1 1 3
                                                    TCP
    25 0.198157 144.122.226.113
                                  144.122.145.146
                                                    TCP
                                                                 54 61220 \rightarrow 80 [ACK] Seq=631 Ack=12861 Win=65536 Len=0
    75 0.220814 144.122.145.146 144.122.226.113 HTTP
                                                                989 HTTP/1.1 200 OK
                                                                                      (text/html)
    77 0.221298 144.122.226.113 144.122.145.146
                                                    TCP
                                                                 54 61220 → 80 [ACK] Seg=631 Ack=13797 Win=64512 Len=0
                                                                 54 61220 → 80 [FIN, ACK] Seq=631 Ack=13797 Win=64512 Len=0
    78 0.221394 144.122.226.113 144.122.145.146
    87 0.225688 144.122.145.146 144.122.226.113 TCP
                                                                 56 80 → 61220 [ACK] Seq=13797 Ack=632 Win=30720 Len=0
```

Figure 5: The first HTTP request-response pair (filtered to avoid confusion with other connections)

- 6. The first HTTP request contains three cookies in the header (even though I perform a hard reload in a private browser window) (see Figure 6):
 - SESSc56f046d65b531883b498de7676dd4ac = M18gqukejeoflLtgCwkxuav13an6VIMXbzPiiSF0Jjw
 - _ga = GA1.3.1319364894.1667052211
 - _gid = GA1.3.609654226.1667052211

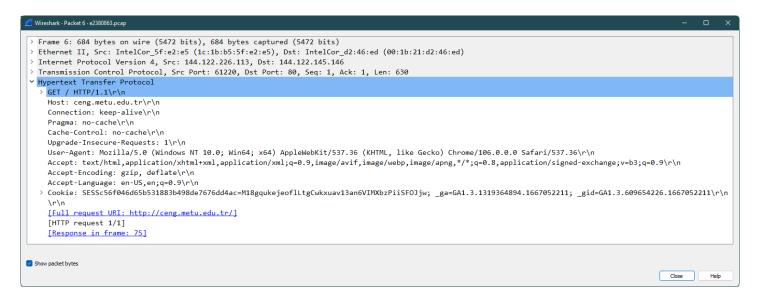


Figure 6: HTTP request header details

- 7. (a) In the HTTP request header, user-agent string provided in the User-Agent parameter is Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36 (see Figure 6).
 - (b) My browser is Google Chrome version 106.0.5249.121, which is included at the end of the user-agent string as Chrome/106.0.0.0. The string also mentions other browsers Mozilla and Safari, and some web engines AppleWebKit, KHTML, and Gecko. This is because browsers prepare those user-agent strings to indicate what they are compatible with.

DNS

1. No. There is no Mail Exchange (MX) record associated with the domain de (see Figure 7 and Figure 8). This means that there is no mail server that handles mails coming to the domain de.

```
Frame 4: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface \Device\NPF_{163}
  Ethernet II, Src: IntelCor_d2:46:ed (00:1b:21:d2:46:ed), Dst: IntelCor_5f:e2:e5 (1c:1b:b5:5f:e2:e5)
Internet Protocol Version 4, Src: 144.122.199.90, Dst: 144.122.226.113
  User Datagram Protocol, Src Port: 53, Dst Port: 53061

→ Domain Name System (response)

     Transaction ID: 0x7b72
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 0
     Authority RRs: 1
     Additional RRs: 0
     Queries
      ∨ de: type MX, class IN
          Name: de
           [Name Length: 2]
           [Label Count: 1]
           Type: MX (Mail eXchange) (15)
          Class: IN (0x0001)

    Authoritative nameservers

      ∨ de: type SOA, class IN, mname f.nic.de
          Name: de
           Type: SOA (Start Of a zone of Authority) (6)
          Class: IN (0x0001)
           Time to live: 1291 (21 minutes, 31 seconds)
          Data length: 51
          Primary name server: f.nic.de
Responsible authority's mailbox: dns-operations.denic.de
           Serial Number: 1667149433
           Refresh Interval: 7200 (2 hours)
           Retry Interval: 7200 (2 hours)
           Expire limit: 3600000 (41 days, 16 hours)
           Minimum TTL: 7200 (2 hours)
     [Request In: 1]
     [Time: 0.003241000 seconds]
No.; 4 · Time: 0.003241 · Source: 144.122.199.90 · Destination: 144.122.226.113 · Protocol: DNS · Length: 125 · Info: Standard query response 0i7b72 MX de SOA f.nic.de
Show packet bytes
                                                                                                      Close Help
```

Figure 7: DNS request header details

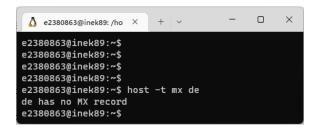


Figure 8: DNS lookup results for de of type MX