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).

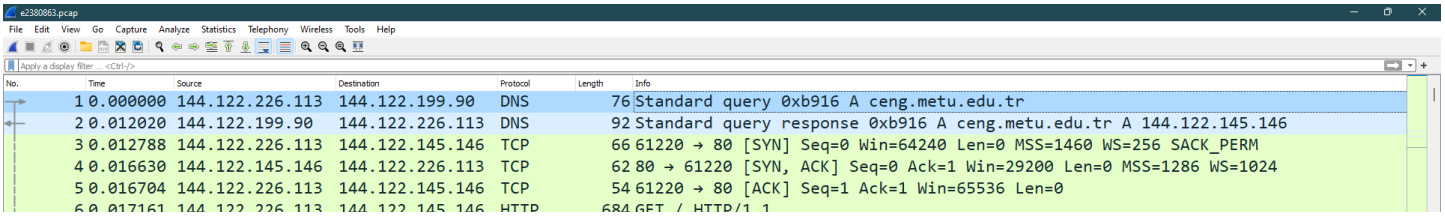


Figure 1: DNS query packet (highlighted)

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).

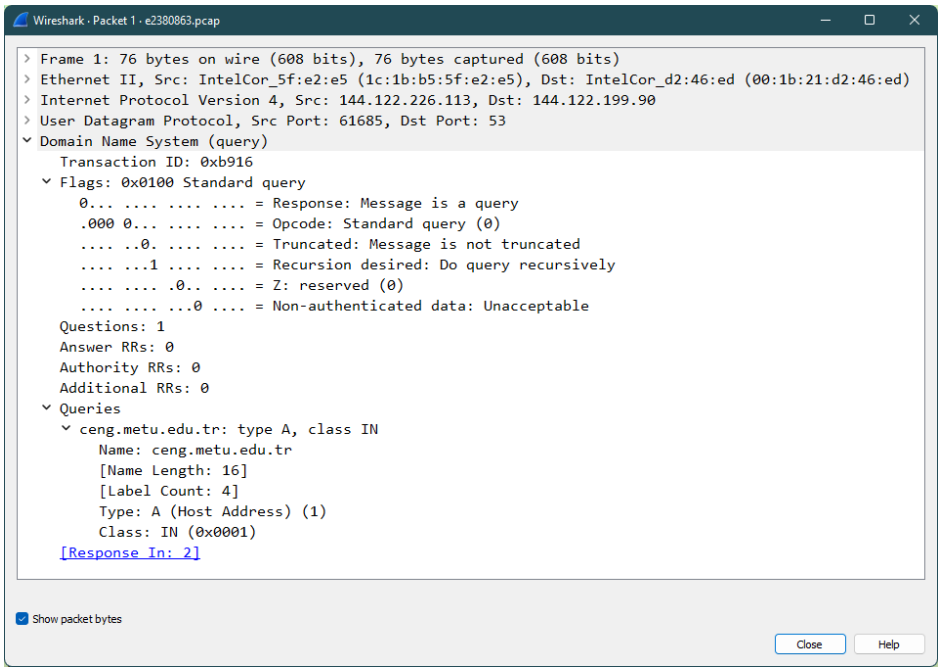


Figure 2: DNS request header details

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).

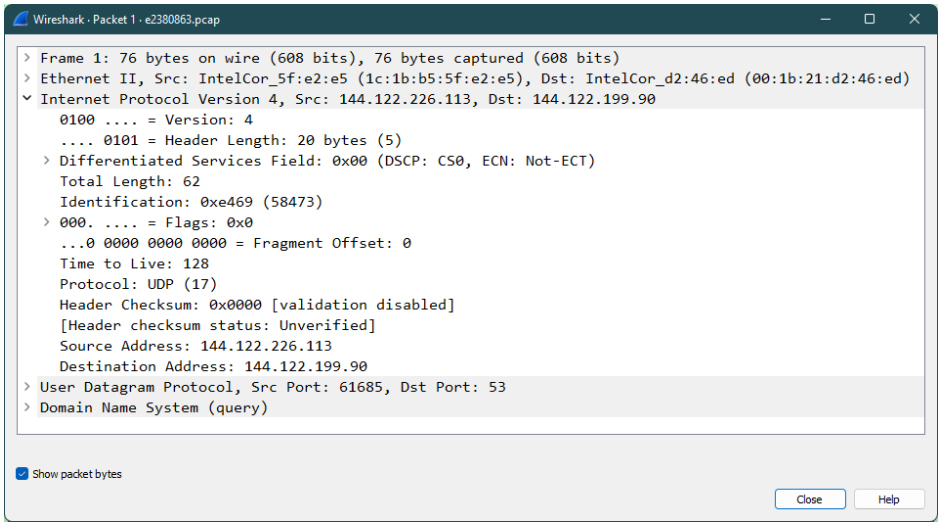


Figure 3: DNS request network layer header details

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.

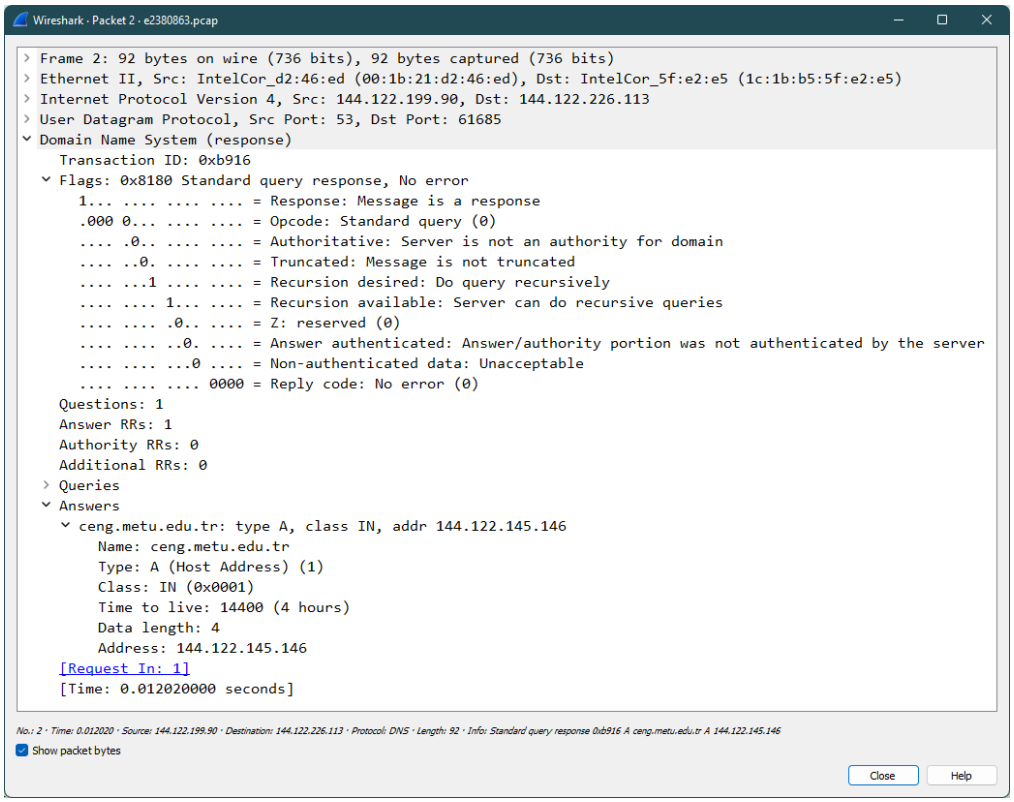


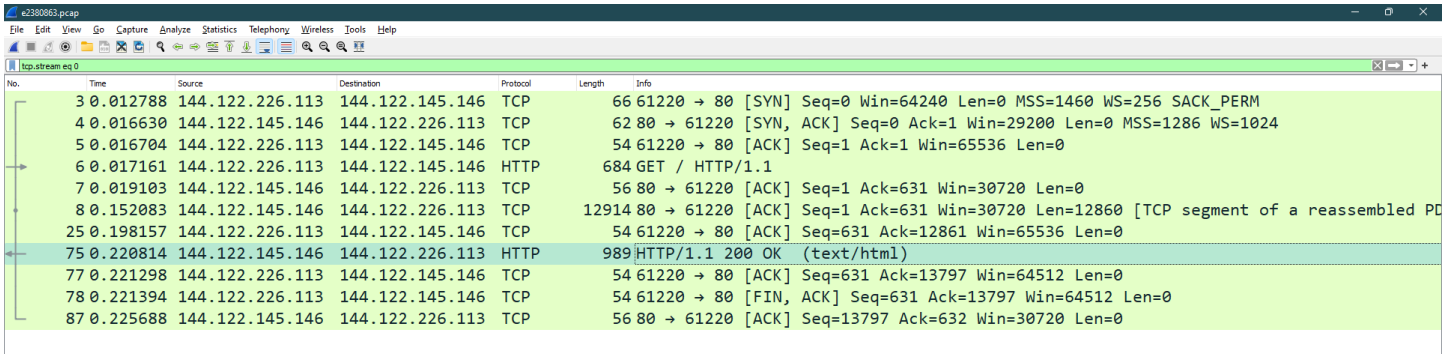
Figure 4: DNS response header details

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.



No.	Time	Source	Destination	Protocol	Length	Info
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	144.122.226.113	TCP	62	80 → 61220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1286 WS=1024
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 → 61220 [ACK] Seq=1 Ack=631 Win=30720 Len=0
8	0.152083	144.122.145.146	144.122.226.113	TCP	12914	80 → 61220 [ACK] Seq=1 Ack=631 Win=30720 Len=12860 [TCP segment of a reassembled PD
25	0.198157	144.122.226.113	144.122.145.146	TCP	54	61220 → 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] Seq=631 Ack=13797 Win=64512 Len=0
78	0.221394	144.122.226.113	144.122.145.146	TCP	54	61220 → 80 [FIN, ACK] Seq=631 Ack=13797 Win=64512 Len=0
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 = M18gqukejeoflLtgCwkxuav13an6VIMXbzPiiSFOJjw`
   - `_ga = GA1.3.1319364894.1667052211`
   - `_gid = GA1.3.609654226.1667052211`

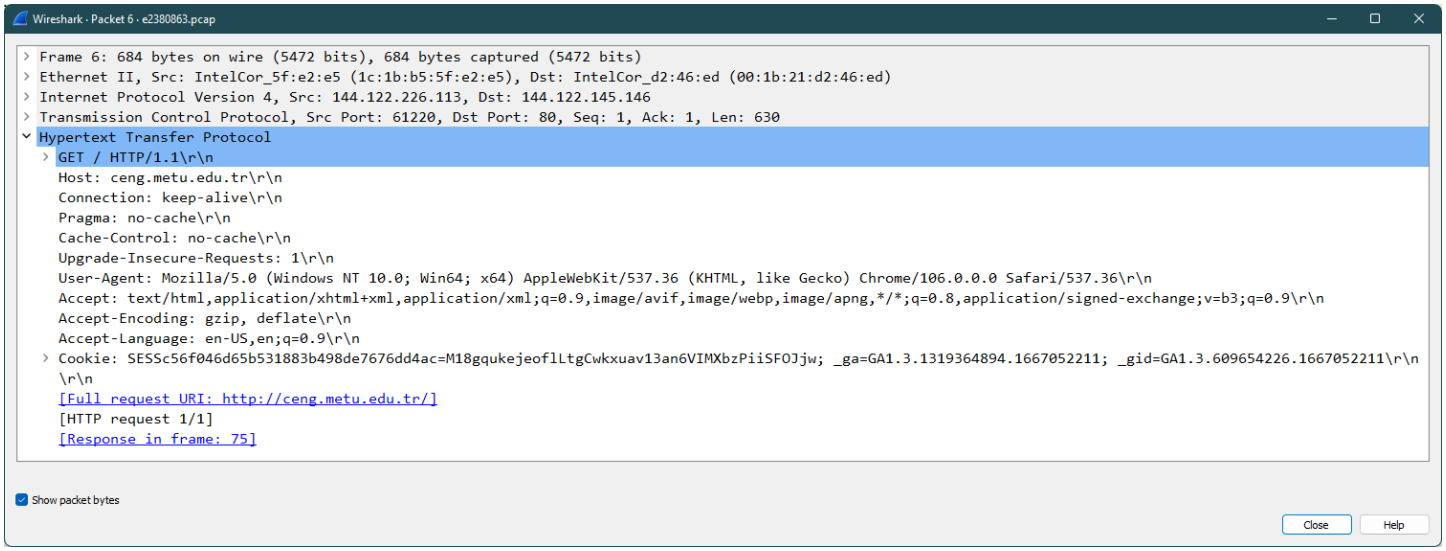


Figure 6: HTTP request header details

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`.

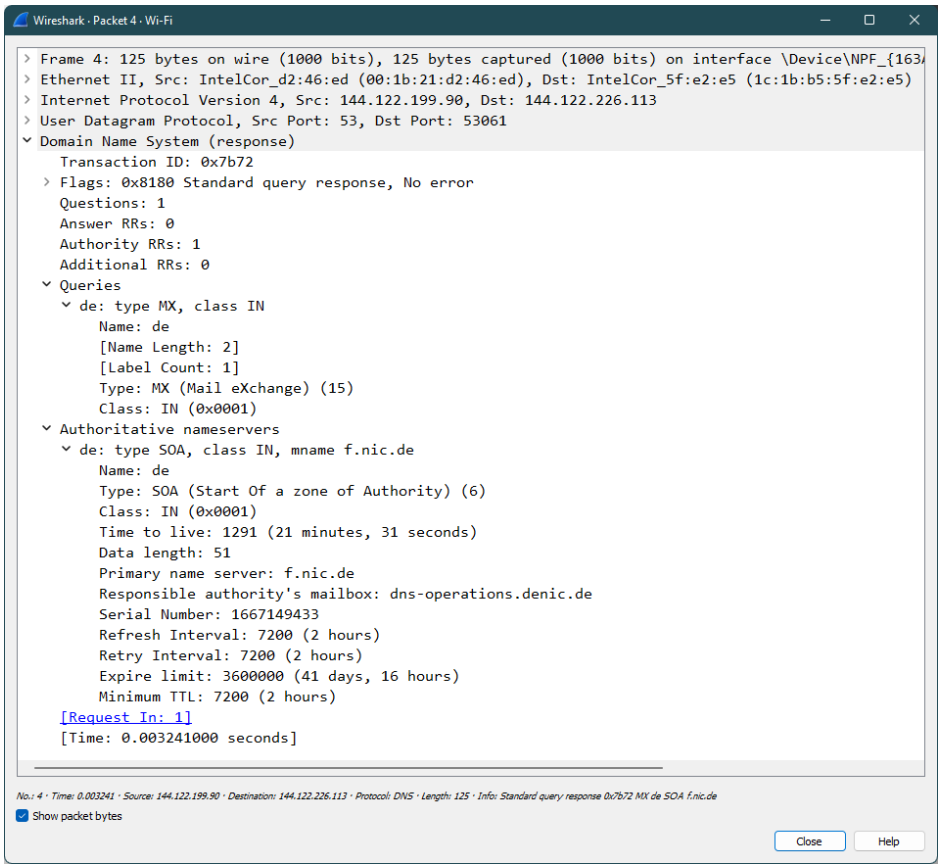


Figure 7: DNS request header details

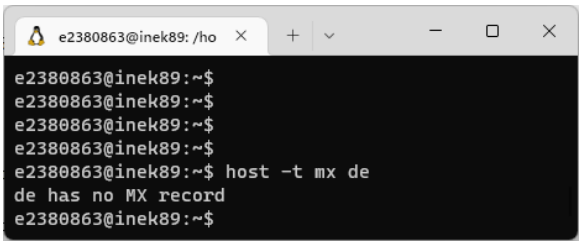


Figure 8: DNS lookup results for `de` of type MX