Student Information

Full Name: Alperen Oğuz Çakmak
Id Number: 2237162

HTTP & DNS (70 Points)

Type your answers under the appropriate subsections.

1. (8 Points)

Two A request is sent from my computer and they are number 5 and 7. Both requests end up taking the same server address of "ceng.metu.edu.tr".

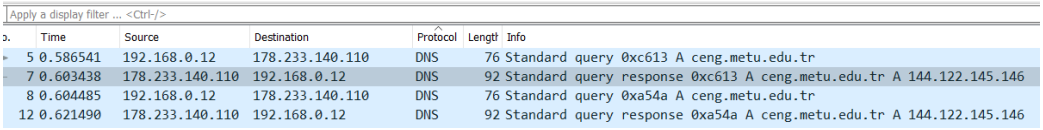

Figure 1: DNS response and requests

2. (10 Points)

Destination of DNS request queries is 178.233.140.110 and it is also shown in figure 1.

2. (Bonus) (10 Bonus Points)

I think DNS queries' location is Ankara because I used a web tool named IP address lookup and it showed the location of the address as Ankara. So looking at the location that I found I don't think that it was cached because if that was the case, IP address would show a closer location (like my local IP address) but address that I found is some other address. Therefore, it was not cached.

3. (15 Points)

The first request sent to "http://ceng.metu.edu.tr" is No:6 and the first response from "http://ceng.metu.edu.tr" is No:9.(Figure below)
For some reason my wireshark captures first TCP request before it could capture DNS response, but TCP request actually uses the address which will

be taken from DNS response. Time difference between them is so low so I assumed it was a thing with wireshark and decided to not bother that difference.

First request and respond is not HTTP of course because HTTP uses TCP. First, a TCP connection is made between server and client. After that, HTTP messages can be transmitted in between.

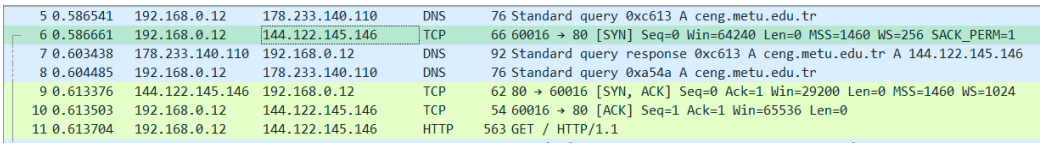

Figure 2: The first response and request to “http://ceng.metu.edu.tr”

4. (15 Points)

Actually I was not expecting to see any cookies because I am cleaning all my browser’s cookies and there should not be any cookies in the first HTTP request because we did not get any set-cookie value yet. However, I think there is a situation about my browser (Firefox) that it actually sends a cookie in first HTTP request. This cookie is called ”has_js” (see Figure 3) and it is used to indicate that my browser, which is sending the HTTP request, is enabled javascript. Therefore there is a cookie which is sent with the first HTTP request but it is related to my browser and not a cookie which is set by server.

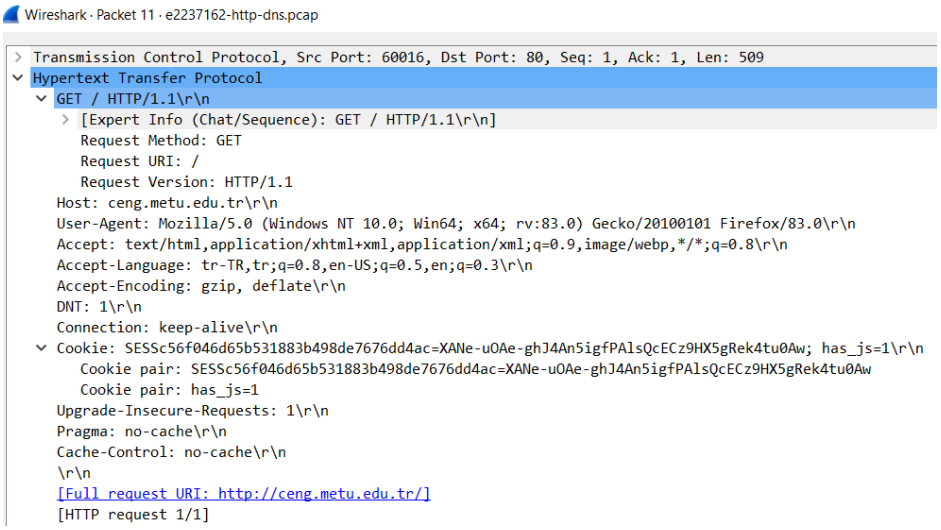

Figure 3: Cookie section of packet 11

5a. (7 Points)

I randomly chose a HTTP request to ceng server which is No:37 and it has a user-agent string "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0\r\n" (see Figure 4).

5b. (15 Points)

It does not have any other browser name than my browser which is firefox. My user-agent string starts with:
-Mozilla which means the browser is mozilla compatible.
-My platform which is Windows.
-rv which is version of Gecko.
-Gecko/20100101 which indicates the browser engine.
-And lastly, firefox which is my browser.

Although my string does not have, in the case that other browsers are used, there could be more than one browser name at the end of the user-agent string. That is because some websites block users who are using other browsers and to get around that browsers include other browser's name in their user-agent strings. For example, chrome has both chrome and safari included in its user-agent.

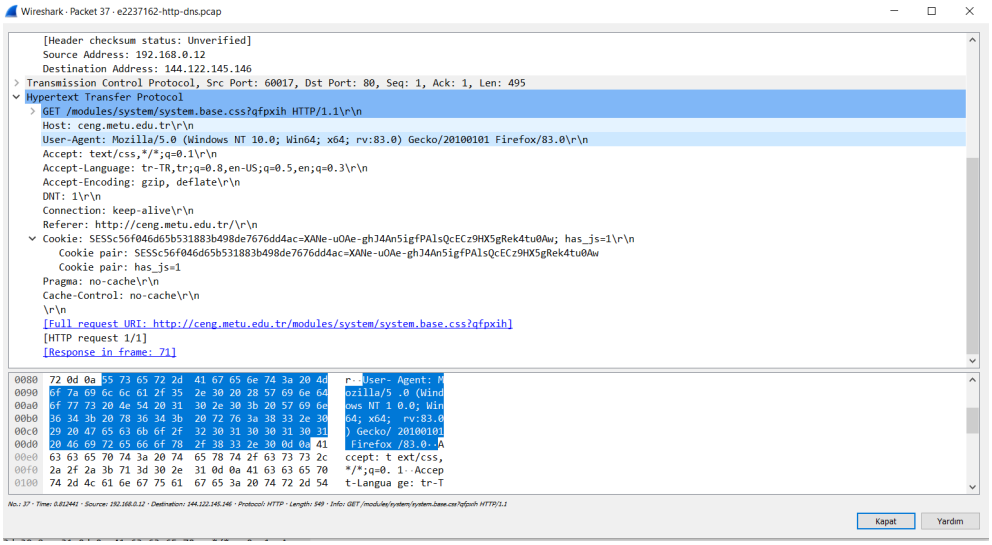

Figure 4: User-agent string

HTTPS & TLS (30 Points)

1. (10 Points)

After getting the server adress of "https://odtuclass.metu.edu.tr", the first request and response is No:17 and No:21 respectively. They are TCP request and response and time difference between them is 0.028885 seconds.

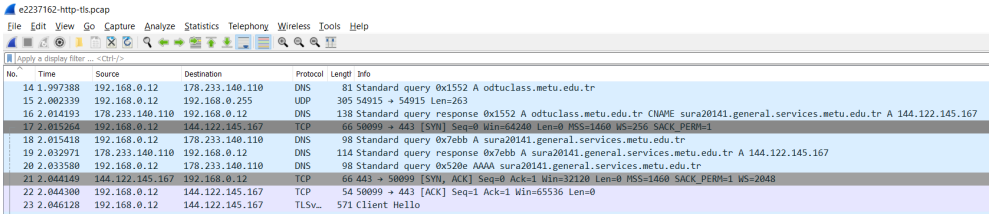

Figure 5: The first response and request to "https://odtuclass.metu.edu.tr"

2. (10 Points)

The first TLS request:
- No:23 - info: 571 Client Hello
The first TLS response:
- No:26 - info: 1514 Server Hello, Change Cipher Spec, Application Data

After server address of odtuclass is taken and TCP connection is made between these addresses, the client and the server are initiates handshake by sending Hello messages. Firstly, the client sends this Hello message (No:23) to the server and the server sends back another Hello message (No:26) containing SSL certificate and chosen cipher suite.

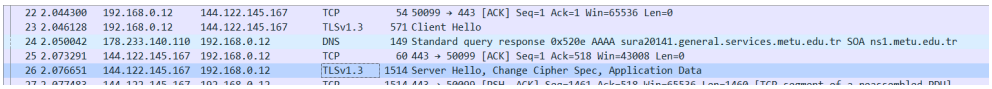

Figure 6: The first TLS request and response

3. (10 Points)

Hello message sent 14 times from client and server. Durng the handshaking several messages are sent between the client and the server until handshaking is done