Alper KOCAMAN - 2169589

Wireshark Assignment 1

1- Did your browser perform any DNS queries to resolve the IP address of http://ceng.metu.edu.tr?

YES.

If so answer the questions below. If not, why it might be the case?

- How many DNS queries did it take to resolve the domain name?

  2 DNS query was taken in order to resolve domain name.

- What is the destination IP for the first DNS query?

  192.168.43.1

- What is the transaction ID for your query(-ies) and its response(s)?

  0xd31b

  0x90a0

2- What are the Number and Time of the first 5 HTTP request packets sent to server?

	Number	Time
1-	**55**	**2.306792252**
2-	**74**	**2.614502513**
3-	**83**	**2.696608060**
4-	**88**	**2.697132557**
5-	**93**	**2.698353989**

3- What is your browser's User-Agent string, what languages does it accept on response?

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

4- Did you send any Cookies with your first GET request to server?

No, I haven’t sent any cookie with my first GET request.

5- How could a request and response packet be matched on a Wireshark environment?

Stream index of the request and stream index of the response are same.

6- How many parallel connections does your browser use? Explain briefly.

I set the source ip as 192.168.43.231(my ip) and destination ip as 144.122.145.146(ceng.metu.edu.tr). This can be done with apply ip.src==192.168.43.231 && ip.dst==144.122.145.146 filter.

Then I counted the number of SYNs and FINs.(SYN means that connection is starting and FIN indicates that connection is finished). By looking opened connections and counting them, I decided that my browser uses 4 parallel connections at the same time.

Bonus Question

Content of the super secret zip :
ceng435{This-is-why-https-is-important}

username - Palpatine
password – Order66