WSA 1 – ANSWERS (Orçun BAŞŞİMŞEK / 2098804)

1 -) I could not see any DNS queries to resolve the IP address of http.//ceng.metu.edu.tr. The reason might be that IP address of this site may be stored in my local DNS cache. I checked it on my Windows machine with command "ipconfig/displaydns", and I saw that IP address of http.//ceng.metu.edu.tr stored there. Hence, I think everything was fine to reach this website without DNS query.

2-)

	No	Time
1st	44	4.252858
2nd	61	4.487376
3rd	76	4.527064
4th	77	4.527230
5th	80	4.528403

3-) User-Agent string of my browser : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.97 Safari/537.36

Accept-Language : tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7

I think it accepts Turkish, US English and other types of English.

4-) No. There is no cookie part for my first GET request (which has frame No 44).

5-) I saw little arrows in No. column for matching HTTP request/response packets on Wireshark environment. For example, for HTTP GET Request at frame 61, its matching HTTP Response is at frame 82. This information is also written when double clicking on any packet. Moreover, streams which the pakcets belong to could be shown by right clicking packet, and then clicking Follow and clicking the needed stream (i.e TCP Stream) for this packet.

6-) I could not find any useful statistic for this question on Wireshark. However, when I filtered my packets by looking only HTTP pakcets, I figured out that there is a pattern-like situation between requests and matching responses. For example, by looking frames 157-161-165-168-171-182, there are 6 parallel connections between host and server. And then, five of them responded from the server. Then, new five requests are sent and responded, and again new five requests are sent and finally 6 responses came from server at frames 284-289-293-295-302-308. After that, this pattern-like situation (6 requests-6 responses pattern) continues. Therefore, I think my browser uses 6 parallel connections for one host name at a moment.

Bonus Question:

Username : Palpatine
Password : Order66
Content Of secretfile.txt : ceng435{This-is-why-https-is-important}