WIRESHARK ASSIGNMENT #1

Onur Can ÜNAL
2095966

1) There is only one DNS query to resolve the domain name. The destination IP for the first DNS query is 144.122.199.93. The transaction ID is 0xc924.

2)

No: 105	Time: 11.719410
No: 143	Time: 11.994359
No: 144	Time: 11.994492
No: 145	Time: 11.995108
No: 146	Time: 11.995741

3) User-Agent string: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0\r\n
Accept-Language: en-US,en;q=0.5\r\n

4) Yes, it is:
Cookie:
SESSc56f046d65b531883b498de7676dd4ac=VTcbcpaf6KAeHCDwO5MIA3YPfBIAKtBF47QLppu64AI\r\n

5) Request and response pairs are matched by their Source and Destination Ports of Transmission Control Protocol. If one of the request packets have same destination port with one of the response packets' source ports, they are matched.

6) My browser uses 8 parallel connections. I understand that by counting consecutive flags that are in TCP. SYN flag is meant set, and FIN flag is meant not set. I counted the number of SYN flags that are consecutive without FIN flag. Thus, I found that it is 8.

Bonus Question) I downloaded the target_capture.pcap file and searched the keyword string “username”. The first match is with a password=”NotSecurePass”, so I skipped it. The other match with username=Palpatine and password=Order66. The host was hbostann.com. Then, I observed that he downloaded /supersecret.zip. I exported objects as HTTP and observed them. I found supersecret.zip and save it to my computer. I opened it, and there was written that “ceng435{This-is-why-https-is-important}”. I thought that it was written because HTTP is not secure, and it can be easily accessible. However, HTTPS is more secure.