1. 1 DNS query was done to resolve the address “ceng.metu.edu.tr” to “144.122.145.146”. Destination IP for the query is 8.8.8.8 which is my default DNS server that I defined on my personal computer. Query has the transaction ID:0X9c01 and has the response “A ceng.metu.edu.tr A 144.122.145.146.” 7 other DNS queries made for the googleapis, twitter, twimg, Microsoft and yahoo sites.
2. 1. No: 12 Time: 0.246818  
    2. No: 73 Time: 0.495063

3. No: 75 Time: 0.495912

4. No: 77 Time: 0.499109

5. No: 79 Time: 0.500214

1. User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.97 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3

Accept-Encoding: gzip, deflate

Accept-Language: tr,en-US;q=0.9,en;q=0.8,en-GB;q=0.7  
  
Accepts languages Turkish and English(US and UK)

1. First GET request which is No:12 does not send any cookies while requests after sends cookies.
2. Request packets’ stream number can be followed through with their TCP stream number. “tcp.stream eq #” or right click -> follow -> tcp stream will allow us to see tcp transactions and finishing of the file requested with “FIN” flag.
3. With “tcp.flags.syn==1 || tcp.flags.fin==1” filter I can see that until the first tcp stream ends Chrome browser which is capable of 6 parallel connections makes 6 conections with different stream numbers and source ports.

**BONUS QUESTION ANSWER:**

With a “password” string search I can find the parameters in No:701: username=lowly\_peasant password=NotSecurePass  
  
But after following the tcp stream of “supersecret.zip” I can see that another login was made before accessing the file with: username=Palpatine&password=Order66  
  
Which makes me believe that we are spying on the Supreme Chancellor. “Its treason then”.   
After exporting the supersecret.zip object from I can see the secret “ceng435{This-is-why-https-is-important}”