Ceng 435 - Wireshark Assignment 1

Beyazit Yalcinkaya - 2172138

Answer 1

- There are no DNS queries for the website. The reason for this is the DNS cache handled by the operating system. That is, since I had reached to the website prior to the capturing of packets, the operating system cached the IP address of the website in its DNS cache. Hence, no DNS queries can be observed.

Answer 2

- First HTTP Request Packet: Number = 8, Time = 0.047982
- Second HTTP Request Packet: Number = 26, Time = 0.264885
- Third HTTP Request Packet: Number = 54, Time = 0.360482
- Forth HTTP Request Packet: Number = 55, Time = 0.360569
- Fifth HTTP Request Packet: Number = 56, Time = 0.360646

Answer 3

- User-Agent String = Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36
- Accepted-Language = en-US,en;q=0.9

Answer 4

- Yes. Truncated Cookie: _ga=GA1.3.1301299981.1552044756; _APP_LOCALE=EN; __utma=128467795.1301299981.1552044756.1566462816.1566462816.1; __utmz=128467795.1566462816.1.1.utmcsr=math.metu.edu.tr|utmccn=(referral)|utmcmd=referral|utmcct=/en/full

Answer 5

- A request and response packet can be matched by checking the Next Sequence Number of the request and the Acknowledgment Number of the response. That is, in the Transmission Control Protocol field, the Next Sequence Number of the request must match with the Acknowledgment Number of the response. Also, Wireshark puts right-left arrows for each request-response pair in the GUI. This can also be used to match these pairs.

Answer 6

- Number of parallel connections may vary, i.e., it is not a constant number. When I checked the TCP packets sent around a HTTP GET command, I saw that at most 6 different port numbers are used for receiving and sending packets. When I searched for the reason for this, I learned that Chrome Browser uses at most 6 parallel connections which supports my observation. In conclusion, my browser uses 6 parallel connections.

Bonus

- Username = Palpatine
- Password = Order66
- Contents of the zip file = secretfile.txt
  - Contents of the secretfile.txt file = ceng435{This-is-why-https-is-important}