CS358 2023 Assignment 1 - Export PCAP via Wireshark

Mayank Agarwal

Deadline: 29 Aug, 2023. 23:59. All of your git repos shall be pulled after that. That will be the version which will be checked.

Doubts: All Doubts relating to CS358 2023 Assignment shall be posted on Google Form https://docs.google.com/forms/d/e/1FAIpQLSdVylWbeelAnQKYDCfqoyxcqSwm_FiVJDbzszV2Mpg-zZCfU viewform?usp=sf_link

I will respond to the queries here:
https://docs.google.com/spreadsheets/d/1jHhkLLGrRSToYZH857D6hM3SY8BiOLoTtqDZ-rNrvGw/ edit?usp=sharing

Please avoid email / wa / dm

So common doubts can be solved and we shall be able to keep track in an organized manner.

Pull This Git Repo - https://github.com/cs358/308_CS359 and copy the tut01 to your repo folder.

Task: Lab 1 Every roll has a website associated given in the following sheet. Use Wireshark to observe the packets and export it.

https://docs.google.com/spreadsheets/d/1EO1pIEfwAMmKHXOdHMyTXEjlBm4kAUC8c9wqJ8i2NUk/ edit#gid=0

Task 1) TCP 3 way handshake for initiation for the website associated with your roll

Task 2) TCP closing handshake for initiation for the website associated with your roll

Task 3) 2 TCP Packets (any source – destination and vice versa. If 1st packet is from A to B, second should be from B to A)

Task 4) 2 UDP Packets (any source – destination and vice versa. If 1st packet is from A to B, second should be from B to A)

Save the pcap in the output folder. The output folder should have only the required number of packets. Like Task 1) the output PCAP should have exactly 3 packets., and so on. In Wireshark export you have an option to exported selected pakcets.

Output File:

TCP_3_way_handshake_start_Roll_Num.pcap

TCP_handshake_close_Roll_Num.pcap

TCP_Packets_Roll_Num.pcap

UDP_Packets_Roll_Num.pcap