CS558: Computer Systems Lab
(January–May 2025)
Assignment - 3

Submission Deadline: 11:55 pm, Saturday, 22nd March, 2025

Wireshark is a free and open-source packet sniffer and network protocol analyzer tool. It helps to capture network packets and understand the structure of different networking protocols. A tutorial for the same can be found here .

1 Questions

1. List out all the protocols used by the allocated application (in the task-allocation table for your group) at different layers (only those which you can figure out from traces). Study and briefly describe their packet formats.

2. Highlight and explain the observed values for various fields of the protocols. Example: Source or destination IP address and port number, Ethernet address, protocol number, etc.

3. Explain the sequence of messages exchanged by the application for using the available functionalities in the application. For example: upload, download, play, pause, etc. Check whether there are any handshaking sequences in the application. Briefly explain the handshaking message sequence, if any.

4. Explain how the particular protocol(s) used by the application is relevant for functioning of the application.

5. Calculate the following statistics from your traces while performing experiments at different times of the day: Throughput, RTT, Packet size, Number of packets lost, Number of UDP
   TCP packets, Number of responses received with respect to one request sent. Report the observed values in your answer, preferably using tables.

6. Check whether the whole content is being sent from the same location/source. List out the IP addresses of content providers if multiple sources exist, and explain the reason behind this.

Group No.	**Application**
1,9,18,	Whatsapp
2,10,19	Google Drive
3,11,20	Zoom
4,12,21	Live Sport Streaming
5,13,22	Youtube - Uploading Video
6,14,23	MS-Teams
7,15,24,26	Youtube - Downloading and Buffering
8,16,25,27	Twitch (Live Streaming) or Hotstar Video Streaming

Table 1: Task Allocation Table for Wireshark Experiment

2 Additional Notes

- For video and audio chat-related applications, collect traces with different host locations, (with both the clients within the same network and with one of them outside the LAN) and perform the required analysis.
- Ensure that video uploading and downloading analysis is done with videos that are more than 20 minutes in length.
- To get near-accurate analysis, try to turn off traffic towards unwanted servers, including advertisements and suggestions.
- Do not open any other sites or applications that use the Internet while the packet capture is in progress.
- Use TCPDUMP with necessary filters for actual capture and Wireshark for analysis. Capturing directly with Wireshark causes packets to be lost due to insufficient memory.
- Do not ignore Layer 2 protocols in your analysis.