CS 558: Computer Systems Lab
(January-May 2024)

Assignment –2 : Network Protocol Analysis Using Wireshark

Submission deadline: 11:55 PM, Wednesday, 31st January, 2024

Wireshark is a free and open-source packet sniffer and network protocol analyser tool. It helps to capture network packets and understand the structure of different networking protocols.

Instructions:

- Install Wireshark (download from www.wireshark.org), and learn how to capture packets and filter the required content.
- A specific application is assigned to groups (refer to Task Allocation Table). Each group needs to perform various activities according to functionalities available in the assigned application and collect the traces for the application using Wireshark. Application-specific activities, if any, are mentioned in the table.
- You should carry out your experiments across different network conditions including different time(s) of the day and locations (e.g., lab or hostel, etc.).
- It is advisable to provide only trace-based descriptions while answering the questions. While answering, provide snapshots of the traces in the report and highlight the content as and when required.
- If something is missing/incorrect in a problem description, clearly mention the assumption with your answer.
- Submit a soft copy of the report, preferably in PDF format, together with your collected traces in a zip file by the deadline. The ZIP file's name should be the same as your group number - for example, "Group_4.zip", "Group_4.rar", or "Group_4.tar.gz".
- Only one member from a group needs to submit this form by uploading the file: **(https://forms.gle/3o8bZ7eVAd3sCWFdA)**
- If your trace file size is larger than 2 MB, you are advised to provide the OneDrive/Google Drive/Dropbox link of the traces in your report.
- The assignment will be evaluated offline/through viva voce during your lab session. where you will need to explain your answers before the evaluator.
- A plagiarism detection tool will be used and any detection of unfair means will be penalised by awarding NEGATIVE marks (equal to the maximum marks for the assignment).
- Marking will be done for the group as a whole.

Questions:

1. List out all the protocols used by the application 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 time 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.

Task Allocation Table

Group No.		Application
1	10	Whatsapp
2	11	Google Drive
4	12	Zoom
5	13	Live Sport Streaming
6	14	Youtube- uploading video
7	15	MS-Teams
8	16	Youtube- downloading and buffering
9	17	Twitch (live streaming video platform) or Hotstar video streaming

Note:

1. 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 is outside LAN) and do the required analysis.
2. Make sure that videos uploading and downloading analysis is done with videos that are more than 20 mins in length.
3. To get near-accurate analysis, try to turn traffic towards unwanted servers off which include advertisements and suggestions.
4. Do not open any other sites or applications that use the Internet while the packet capture is in progress.
5. 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.
6. Do not ignore Layer 2 protocols in your analysis.

IMPORTANT: Report should be brief and should not contain any unnecessary explanation of protocols like their packet format and functionality. Rather it should contain only those points which you have analysed about protocols from your traces. Submit your traces along with your report. Use screenshots selectively only when required to conclude something. The report should not have only screenshots.