CS341

Computer Networks Lab

Assignment 1

Network Protocol Analysis Using Wireshark

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 given in (refer to Table 1 below). 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 description 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.
- Be precise with your answers; there is no credit for being unnecessarily verbose (may award you negative marks for the same). Unless specified otherwise, do not describe the tool or application or protocol in general.

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 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 protocol(s) used by the application is relevant for its functioning.
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.

Method of submission:

- → Submit a soft copy of the report, preferably in PDF format, together with your collected traces in a zip file on teams. The name of the zip file should be like "Your_Groupno.zip" (example: "Group11.zip").
- → Files submitted without proper naming format will not be evaluated.
- → 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.

Zoom
Live Sport Streaming
Youtube- uploading video
Youtube- downloading and buffering
NPTEL video lectures
Twitch (live streaming video platform) or Hotstar video streaming
MS-Teams
P2P connectivity using Remote desktop and softwares like Team Viewer
Online games
Dropbox

1. For video and audio chat related applications collect traces with different host locations, (with both the clients within same network and with one of them is outside LAN) and do the required analysis.

2. Make sure that videos uploading and downloading analysis are done with videos over 20 mins.

3. For the application involving Online games, try playing games against opponents residing both within LAN and outside LAN.

4. To get near-accurate analysis, try to turn traffic towards unwanted servers off which include advertisements and suggestions.

5. Do not open any other sites or applications that use the Internet while the packet capture is in progress.

6. 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.

7. 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.