भारतीय सूचना प्रौद्योगिकी संस्थान, पुणे

Indian Institute of Information Technology, Pune

(An Autonomous Institute of National Importance under act of Parliament)

BT23104: Computer Network
Lab Assignment 2: 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 assigned to group of student (refer to Table 1 below). Each student 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 in 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: (Total Marks 20)

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. Mention and explain the observed values for at least 5 fields of the packets of each layer. Example: Source or destination IP address, port number, Ethernet address, protocol number, etc. (1+4 =5 marks)

2. Mention the important functionalities of the application as many as you can discover. (Two example functionalities for each application is given in Table 1). Explain which

protocols are being used by which functionalities of the application. Give reason why those protocols are used for the functionalities. (1+5=6 marks)

3. For any two functionalities of the application (mentioned in question 2), show the sequence of messages (attach screenshot) exchanged to achieve those functionalities. Explain those message sequences. Check whether there are any handshaking sequences in the messages, and briefly explain the reason. (1+3+1 =5 marks)

4. Calculate the following statistics from your traces while performing experiments at three different times (morning, afternoon, night) of the day: a) Throughput, b) RTT, c) Packet size, d) Number of packets lost, e) Number of UDP & TCP packets, f) Number of responses received with respect to one request sent. Report the observed values in your answer, preferably using tables. (0.5*6 =3 marks)

5. Check whether the content is being sent/fetched by the application to/from the same or different destination(s)/source(s) during the three different times of the day used in question 4. If multiple destinations /sources exist, list out their IP addresses, and explain the reason behind this. (1 marks)

Method of submission:

- Submit a soft copy of the report in PDF format only, together with your collected traces in a zip file on Google class. The name of the zip file should be like “Your_MIS NO.zip” (example: “190101002.zip”).
- Files submitted without proper naming format will not be evaluated.
- If your trace file size is so large that you are not able to upload the file on Google class, in that case you are advised to provide the OneDrive/Google Drive link of the traces in your report.

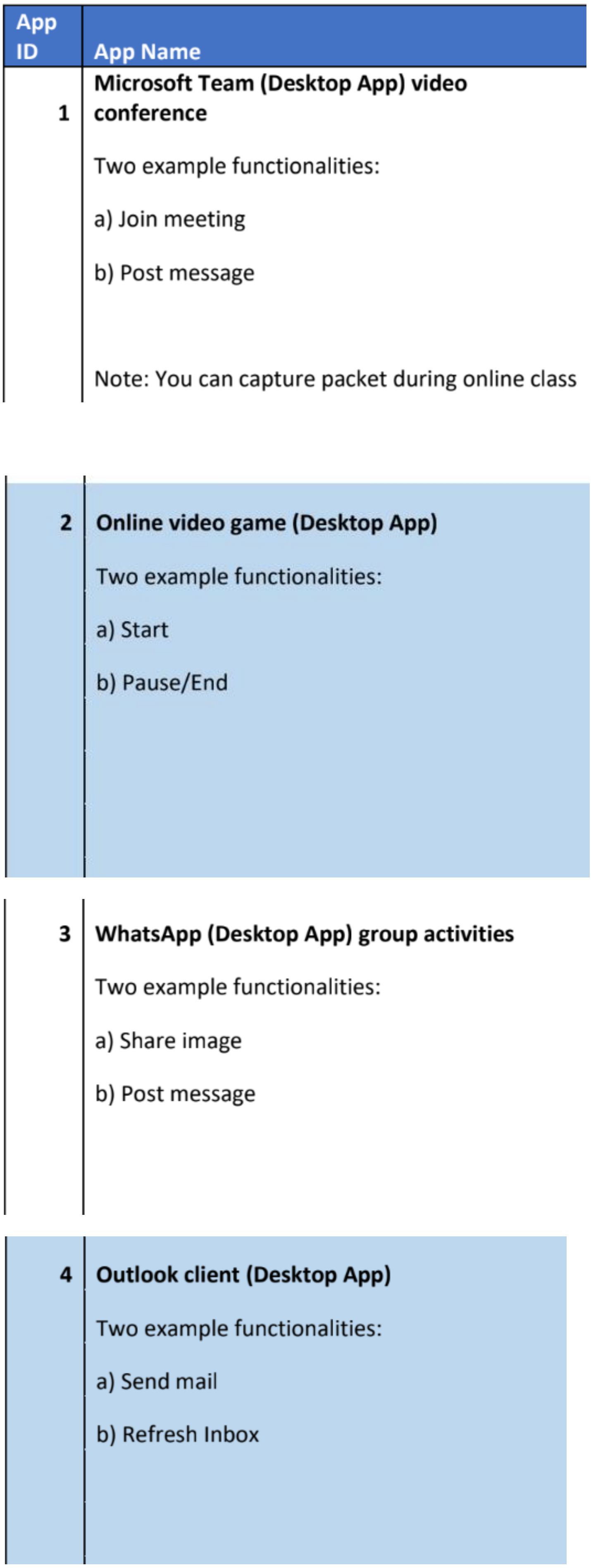
Note:

The deadline for submission must be strictly followed. Any submission done after the deadline will not be considered for evaluation.

The report should not contain more than 5-6 pages.

Plagiarism (copy cases) and other unfair means will be strictly punished by awarding NEGATIVE marks (equal to the maximum marks for the assignment).

Table 1: Application allocation to Students



App ID	App Name
1	**Microsoft Team (Desktop App) video conference** Two example functionalities: a) Join meeting b) Post message Note: You can capture packet during online class
2	**Online video game (Desktop App)** Two example functionalities: a) Start b) Pause/End
3	**WhatsApp (Desktop App) group activities** Two example functionalities: a) Share image b) Post message
4	**Outlook client (Desktop App)** Two example functionalities: a) Send mail b) Refresh Inbox

5	**GitHub client (Desktop App)** Two example functionalities: a) Clone a repository b) Submit a file
6	**Skype (Desktop App) video conference** Two example functionalities: a) Initiate call b) Terminate call
7	**OneDrive (Desktop App)** Two example functionalities: a) Create a folder b) Download/Upload file
8	**YouTube live video** Two example functionalities: a) Start watching b) Pause/Go live
9	**FortiClient VPN (Desktop App)** Two example functionalities: a) Establish connection b) ssh remote machine