Indian Institute of Technology Jodhpur
Computer Science and Engineering Department
Lab 5
CSL6010 - Cyber Security

Date 09.03.2023 **Marks: 20**

Aim: Understanding TCP (Wireshark)

Late submission penalty: 1 mark per day

Plagiarism: Do not do it. Write little but by yourself.

Lab description: This lab is intended to familiarize you with a popular open-source packet analyzer, *Wireshark*. Please download and install it if you have not done so already. It would help you take a deeper look into the functioning of various networking protocols as well as observe TCP/IP protocol stack in action. The tasks for this lab assignment are given below.

Submission instructions: This is an individual assignment. You must do it yourself. If a part of your code is found to be similar to your colleagues, it would be considered plagiarism. You must submit a report (not handwritten) in PDF format containing your observations for each task. Please attach relevant screenshots. The name of the file should be in the following format; <your_id>_lab5.pdf

1. Start packet capture in Wireshark on your wireless interface. What do you observe?

2. Now visit a local website, say www.iitj.ac.in. Subsequently stop the packet capture and record your observations. Are you able to see the DNS request? What about TCP and HTTP? What is the IP address of the IITJ server? Are you able to see different HTTP requests/responses? Please justify your answer with relevant screenshots.

3. What does a packet highlighted in `black' color signify?

4. Explore at least 5 different filters in Wireshark (https://wiki.wireshark.org/DisplayFilters). Ex. "http" would give you only HTTP traffic.

5. What is the filter command for listing all outgoing traffic?

6. Start a new packet capture to now visit an external website, say www.cricinfo.com. Can you show the 3-way TCP handshake happening? Can you see your IITJ proxy in between? What is its IP address?

7. Why does DNS follow the UDP stream while HTTP follows the TCP stream?

8. Run your socket program (both server and client) and show the TCP communication happening at different ports.

9. Perform an SSH to your IITJ home folder and show the relevant screenshots captured using Wireshark.