IIT Goa CS212 (Computer Networks LAB)
Instructor: Neha Karanjkar

LAB 2: Examining Packets using Wireshark

- This lab is to be completed in teams of 2 students.
- After completing the lab exercise, create a brief report (pdf) and upload it to Google classroom. Clearly write the question number of each answer. Only one person in the team needs to upload the solutions. The report must contain the names of both persons in the team.
- The report must be named: LAB2<_<NAME1>_<NAME2>.pdf where NAMEs are your names as on Google classroom.
- You can use web search and online resources for completing the lab.
- The instructors may conduct a brief viva to grade your lab exercises.

PACKET SNIFFING USING WIRESHARK

Read up about Wireshark in the introductory reference material provided to you.

1. Find out the IP address of "www.iitgoa.ac.in". Now start up wireshark selecting "any" interface.

Apply a filter "ip.addr == <the ip address you found for iitgoa>" for example, "ip.addr==10.250.36.36". Now, open a web browser and open IIT Goa's website. Observe the traffic captured in Wireshark for this filter.

a) Look out for the SYN, SYN/ACK, ACK sequence of packets. What protocol is being used at the Transport Layer?

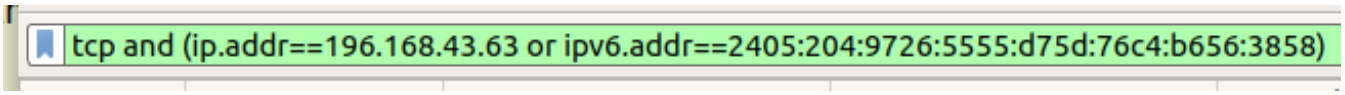
b) Examine the first SYN packet. Observe how the packet corresponding to each layer of the TCP/IP stack is wrapped inside the packet of the lower layers. Examine the IP datagram and its header. What are the source and destination IP addresses for this packet? Check if the destination IP address matches that of iitgoa.ac.in. List your observation.

c) Examine the transport-layer segment in the first SYN packet. What are the source and the destination **port numbers** for the first SYN message?

d) Now remove all filters, and take a broad view of all packets flowing through the interface. What kind of packets make up a majority of the traffic to your computer/device?

2. In wireshark, you can apply a filter that displays packets only belonging to a certain protocol (such as TCP or UDP) as follows:

Two or more conditions can be combined using and/or to create more complex filters. For example:



a) Now, you wish to find out whether **YouTube** operates over the TCP protocol or the UDP protocol. Open YouTube in Firefox browser and filter out its traffic in Wireshark using the appropriate IP address in the filter. Observe the packets. Does YouTube use TCP or UDP?

b) Does your conclusion change if you open YouTube in Google Chrome, instead of Firefox? List your observation. Check if your conclusion is correct, using a web search about what protocol YouTube actually uses.

3. Consider the url of the webpage of some university located outside India. Find out its IP address, and set it as a filter in wireshark. Now, start recording packets and open the url in your browser. Observe the flow of packets.

a) For the first TCP data packet carrying the contents of the webpage, list the protocol and src,dest addresses used in the headers corresponding to each layer in the packet. List them systematically, starting from the application layer to the data link layer.

b) How many DATA packets were received in total for conveying the contents of a single webpage? How much time did it take approximately?

4. **[Bonus question]** Try connecting two different devices in the same network. For example, connect your mobile phone on the same network as your laptop. Apply the filter ip.addr=<other device's IP addr>. Check if you can sniff packets meant for another device on the same local network.

----------END----------