Computer Networks Lab (CS 3272)

Assignment – 3

Assigned date: 4-Feb-2022 Submission date: 11-Feb-2022

The aim of this assignment is to make you familiar with a GUI-based TCP/IP packet capturing (sniffing) tool called *Wireshark*.

Install Wireshark in your computer by following the instructions given in the videos:

- For Linux: https://www.youtube.com/watch?v=2ox10RKeUgI
- For Windows: https://www.youtube.com/watch?v=fpeMCuCKgHA

Read the Wireshark User Manual to learn how to start the tool, capture packets on a particular interface, save and read the packets, use filters as an when required, etc.

Attempt the following tasks related to the Wireshark tool:

1. Analyse the packets (across all layers) exchanged with your computer while executing the following commands: (i) ping, (ii) traceroute, (iii) dig, (iv) arp, (v) wget.

2. Capture the packets while sending/receiving telnet request/response between your computer and a custom server running the telnet daemon. What is your observation while analysing the application layer data?

3. Capture the packets while sending/receiving ssh request/response between your computer and one of the department servers. What is your observation while analysing the application layer data?

4. Enter the URL: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html and capture packets using Wireshark. After your browser has displayed the INTRO-wireshark-file1.html page (it is a simple one line of congratulations), stop Wireshark packet capture. Answer the following from the packets captured:
   a. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?
   b. What is the Internet address of the gaia.cs.umass.edu? What is the Internet address of your computer? Support your answer with an appropriate screenshot from your computer.

5. Start the Wireshark packet capturing service. Enter the URL: https://www.gmail.com on your browser and sign-in to your gmail account by providing credentials (Username/Password). Answer the following from the captured packets:
   a. Is there any difference in the application layer protocol?
   b. How it is different from the HTTP data you analysed in the above problem?