Continuous Evaluation (CE4)

Download Wireshark software in your PC. You may view the following video as a tutorial on Wireshark: https://www.youtube.com/watch?v=Mys_kwuQUhc.

Perform network analysis as mentioned in the following steps.

Step 1: Start Wireshark and select the appropriate interface.

Step 2: Open a Browser window and go to “www.wikipedia.org.”

Step 3: Stop capturing packets. Use filters to capture the instance containing TCP and ip address of www.wikipedia.org.

Step 4: Observe the SYN, SYN-ACK and ACK between you and wikipedia server and answer the following questions:

1) What is your IP address and port number?

2) What is “www.wikipedia.org” ip address and port number?

3) What is the raw sequence number of the first SYN packet sent from you to wikipedia’s server?

4) What is the raw sequence number of the first SYN-ACK packet sent from wikipedia’s server to you?

5) What was the window size shared by client to server in first SYN packet?

6) What was the window size shared by server to client in next SYN-ACK packet?

7) What was the time difference between sending a SYN packet and receiving SYN-ACK?

8) What was the ‘time to live’ value in network header?

9) What was the ipv4 header length?

10) What is the difference between raw sequence number and relative sequence number in wireshark.

Please submit a single pdf file containing two informations:

(a) Answers to above 10 questions.

(b) The screenshot of the wireshark screen from which your responses to the above questions can be validated.

Note: In this assignment no two students can have all similar answers. Your answers depend on the experiment conducted on your PC. If two students are found to have all similar responses then they may get zero marks.