Department of Computer Science and Engineering
Computer Network Lab (CS39006)
Assignment 1

1. Start the wireshark to capture the packets
2. Enter the following link to open the web page on your browser (Google Chrome)
   http://10.5.16.177
3. Wait for approximately 20 seconds and refresh the page.
4. Open an Incognito window (File -> New Incognito Window) and then again enter the above link to open the web page in your browser.
5. Save the packet capture in wireshark in a folder called CS39006_<Your_Roll_Number>/Assignment_1/ (*create it on the desktop of the machine that you are using*). Name the saved packet capture as Assignment_1.pcap.
6. Close the browser windows.
7. By looking at the information in the **HTTP** Request and Response message, answer the following questions in a text file.
   a. What version of the HTTP the server is running?
   b. What is the status code returned from the server to your browser?
   c. What HTTP method is used by the client?
   d. When was the file that you are retrieving last modified at the server?
   e. How many bytes of content are being returned to your browser for each of the three accesses (initial access, refresh, access over incognito window)?
   f. What information can be inferred about the client system and browser?
   g. Write the exact timestamp when the above HTTP request has been sent.
   h. Calculate the time between request transmission and first response byte for each of the requests you see.
   i. Identify TCP three way handshake used to establish the connection with the Apache server. Specify SYN, SYN-ACK, ACK packets and write the sequence number for each of the three accesses.
   j. What are the source and destination port numbers used for the connection for each of the three accesses?
   k. Which TCP flags are set for each of the three accesses?
   l. What is the received window size in the SYN packet from your system for each of the three accesses?
   m. What is the Maximum Segment Size (MSS) for your connection for each of the three accesses?
   n. Calculate the timestamp difference between sending the TCP SYN packet and receiving the corresponding SYN-ACK packet for each of the three accesses.

Note:- Ensure that the captured packet trace is saved on your system in .pcap format.