ASSIGNMENT 1

A. For this assignment, Ping and Trace route tools only are to be used. Every student has to try from their own laptop or desktop computer available in the laboratory. The questions are as follows:

1. What is the IP address of the webserver “www.ndtv.com”?
2. What is the transmission time of the ICMP echo request to any web server, if it is sent from the laptop?
3. What is the propagation time of the ICMP echo request?
4. Is there any packet loss in the route? If yes, what is the percentage?
5. How many routers are in between your laptop (origin of the ICMP echo request) to the destination “www.ndtv.com”? In that route, which router is consuming more time to process?
6. In which operating system, the server is running the domain “www.ndtv.com”? Justify.
7. Is there any congestion that occurs between the source (your laptop) and the destination (www.ndtv.com)? If Yes/No, Justify.
8. Is the web server “www.sbionline.com” has blocked the ICMP echo request by Firewall? Justify.
9. Is the IP address similar for “www.sbionline.com” and “ww.sbi.com”?
10. Could you find any server that needs more than 14 hops to travel from the source? If Yes, pl. report the server name and IP address.

B. Use Wireshark to capture the packets and answer the following questions:

Open multiple tabs in the browser. Open Wireshark and select the network interface that you would like to capture and start capturing the packets. Send the web server requests from each tab in the browser. Open command prompt and send ICMP request to any web server. Please run the wireshark for 5 minutes and capture the packets.

i. Filter the ICMP packets in wireshark. How many bytes are captured for a frame in wire when ICMP request is sent?
ii. If the number of bytes captured for a frame is 'X', then justify how the 'X' value is obtained?
iii. Is the link local address shown in any of the captured packets?
iv. If Yes for (iii), in which layer the address is shown and what is the size?
v. If No for (iii), why it is not shown?
vi. To view only the ping requests and responses of my local machine, what is the name of the filter to be used?
vii. Select the first ICMP request PDU frames in the top section of Wireshark and does the source MAC address match your PC interface?
viii. Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?
ix. Highlight a DNS packet in the captured traffic. How to find whether the highlighted packet is a request packet or reply packet from the transport layer information?
x. Use Wireless access (IEEE 802.11) to connect to the Access Point. Is the frame captured is 802.11 or 802.3? Justify.

Deadline for the submission: 28, January, 2019 (23.59 hrs) Tuesday.

***