20CYS114 - Cyber Security Essentials

Lab 5 - Wireshark Fundamentals

For each of the following steps complete the task and include screen captures as needed in your output. Be sure to label your results carefully and organize your results in the order of steps as given here and to answer each question in your report.

Lab Environment:

Download and Install Wireshark from the given link. https://www.wireshark.org/#download

1. Open the given evidence.pcap file. Use display filter to identify only the traffic which are related to PING. (HINT – ICMP). After filtering the respective traffic answer the following questions.
   a. What is the frame number of 1st packet (Ping Request)?
   b. How many packets are available with applied filter?
   c. What is the source and destination IP address of the 1st packet (ping Request)?
   d. What is the data size (in Bytes)?
   e. What is the source and destination MAC address?
   f. Which version of IP is been used here : IPV4 or IPV6?

2. here is some unencrypted web traffic has been captured. Use the appropriate filter to identify that traffic. After filtering the traffic answer the following questions.
   a. How many packets are found after filtering using required filter?
   b. What is the frame number of 1st packet?
   c. What is the source and destination IP address?
   d. What is the source and destination MAC address?
   e. What is the source and destination port numbers?
   f. What is the length of the response packet?
   g. What is the name of the file which is downloaded from that webpage?

3. Find the number of Bluetooth devices captured?
   a. List the MAC address of all Bluetooth devices.
   b. Find the name of Local Bluetooth adapter.
   c. Apply the respective display filter to find out how many packets related to Bluetooth are captured in this evidence.pcap file.

4. Capture live traffic using Wireshark on your own network interface with capture filter as “tcp port http”. Then visit this page http://testphp.vulnweb.com/login.php in your browser with Wireshark running in background. Enter any random username and password in that login page. Then stop the capture in Wireshark. Analyse the packets captured to find the username and password that you have entered in the website.