Assignments:

1. List down the network interfaces connected to your host . Identify the Ethernet interface .

2. Check whether the network interface of your machine is in Promiscuous mode. If it is not in promiscuous mode, change it in to promiscuous mode.

3. Configure the capture stop option of the Wireshark in following settings
   - Stop after 100 packets and store in to a file “pcap100pkt”.
   - Stop after 200 Kb and store in to a file “pcap200kb”.
   - Stop after 5 minutes and store in to a file “pcap5min” .

4. Capture live traffic from a particular host (e.g www.google.com) and store the captured file as “pcaphost.pcap”.

5. Capture live traffic from a particular port (eg: 80) and store the captured file as “pcapport.pcap”.

6. Capture all non ARP traffic using capturing filter operators and store the captured file as “nonarp.pcap”.

7. Display the summary of the following

   * No. of packet captured, total bytes transferred
   * Average packets/sec, average packet size
   * Bandwidth usage (Average bytes/ sec)

8. Use the “dump1.sample” file filter all http traffic.

9. Use the “challengescan.pcapng” file show all packets having ttl value is equal to 32.

Use the challengewhatsup.pcapng for solving the problems from 10 to 13

10. How many different IP hosts is A’s machine is communicating with?

11. What is the average packets per second rate seen in trace file?

12. How many HTTP POST requests did A's machine send?

13. What application appears to be generating the GET/POST requests?

14. Find the user name and password in dump1.sample file.
    hint : - user name and password is in Caesar cipher

15. Find the packet number and source IP of given string in the dump .