Assignment- wireshark tool

1. Traceroute and ICMP packet analysis using wireshark

   Objective- To analyze ICMP packets generated by traceroute command and study changes in IP header field using wireshark

   a. Open command prompt/terminal
   b. Run traceroute www.google.com
   c. Start wireshark and select active network interface
   d. Apply the filter ICMP
   e. Capture packets while traceroute is running
   f. Select the first ICMP echo request sent by your computer
   g. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer

   h. Describe the pattern you see in the values in the Identification field of the IP datagram Next (with the packets still sorted by source address) find the series of ICMP TTL exceeded replies sent to your computer by the nearest (first hop) router.

   i. What is the value in the Identification field and the TTL field?

   j. Which fields stay constant? Which of the fields must stay constant? Which fields must change?

2. Use Wireshark to analyse features of the HTTP protocol.

   Start Wireshark

   Enter the URL in the browser

   http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

   Apply the filter HTTP

   Answer the following questions, based on your Wireshark experimentation:

a. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window.
b. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)
c. What is the Internet address of the gaia.cs.umass.edu (also known as wwwnet.cs.umass.edu)? What is the mac address of your computer?
d. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK.
e. Explain wireshark and provide the screenshots of the experimental results.

3. TCP 3-way handshake analysis

Capture packets while opening a website

Identify SYN, SYN-ACK, ACK packets

Analyze sequence and acknowledgement number

4. DNS query and respond analysis

Capture DNS packets

Analyze query type (A, AAAA, CNAME)

Measure DNS response time

5. HTTPs vs HTTP analysis

Capture traffic for HTTP an HTTPs website

Compare visibility of payload data