Computer Networks, Fall 2020
Instructor: Jitendra Bhatia

Lab 3 & 4: Exploring TCPDUMP and Wireshark Packet analyzer and Dissect the packets.

Note: For each question, Give the screenshot of the captured packets in Wireshark.

Tutorial on basics of Wireshark packet sniffer tools is available for download here. You need to first install Linux version of Wireshark software in your computer which is available for download at **http://www.wireshark.org/.**

In this assignment, you will be evaluated for your familiarity in using Tcpdump and Wireshark utility for packet capture and analysis.

Start packet capature in wireshark application and then open your web browser and type in an URL of website of your choice (**www.ahduni.edu.in**, **www.google.com**, etc).

Q1. Answer the following questions, based on your experimentation:

1) Using tcpdump utility, capture only http packets
2) list the source and destination ip and port address
3) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received for the webpage you visited in your web browser?
4) What is the Internet (IP) address of the URL you visited and what is the Internet address of your computer?
5) Capture the packets in file and give the extention your_enrollment.pcap.

Q2. In Wireshark Open the packets which you have captured in your_enrollment.pcap.

-What HTTP version is your browser and the server running ?
-check the contents of the tcp stream
-What is the size of the content in terms of bytes?

Q3. Configure the Webserver in your local machine (e.g.,Apache web server) and deploy the server side scripting page which validates your userid and password. Design a client side html page which prompts for user id and password.

Trace the step by step transactional flow between client and webserver (i.e., dns, http and tcp stream) when you press submit on client page. Find the user id and password from the tcp stream. Summarize the flow in your own words.

Q4. Given the following frame which came from the bottom window of wireshark, and consists of an ethernet header (without preamble or checksum), a IP header, a TCP header, and an SMTP header, answer the following questions

```
0000   ac 2b 6e de fd b4 00 1e a6 83 2d a8 08 00 45 00
0010   00 68 29 14 00 00 7a 06 c6 d3 4a 7d 44 1b c0 a8
0020   01 68 00 19 d5 80 07 b6 50 f4 ea 03 7a 91 80 18
0030   01 00 f2 ad 00 00 01 01 08 0a b5 0b d9 2f 00 3a
0040   38 89 32 32 30 20 6d 78 2e 67 6f 6f 67 6c 65 2e
0050   63 6f 6d 20 45 53 4d 54 50 20 78 33 30 73 69 34
0060   35 33 32 38 33 34 70 67 65 2e 33 32 20 2d 20 67
0070   73 6d 74 70 0d 0a
```

1. What is the source ethernet address?

2. What is the destination ethernet address?

3. What is the source IP address?

4. What is the destination IP address?

6. What TCP port was used on the source system?

7. What TCP port was used on the destination system?

8. What is the SMTP command?

Please give all numbers in decimal except the ethernet addresses.

Q5. Start capturing the packets for traceroute command.

Open the terminal and type

traceroute 108.174.10.10 and press enter.

When the tracert command execution stops, stop capturing the packets. You will see many ICMP (a layer 3 protocol) packets. Select the first one.

Answer the following questions:

a. What is the version of the IP? What is the IP address of your host?
b. What is the value of the upper layer protocol within the IP header?
c. What is the size of the IP header? What is the payload size of the IP datagram?
d. Has this IP datagram been fragmented? How you can determine this?