Exercises on Wireshark

Exercise1:

Start Sniffing: Perform a Live Capture of Network Traffic

Exercise 2:

Use the statistics menu to determine the answers to the following questions.

- How many udp packets did Wireshark capture?
- What was the average IP packet size?
- How many packets did Wireshark drop?
- What does a flow graph show?
- List the flow graph options.

Exercise 3:

Select a TCP packet in the **Packet List Window**.

- Expand the **Ethernet** section (Click the **+** symbol to the left of **Ethernet**) of the **Packet Details Window**.
- Determine the following Ethernet frame values for the selected packet: o Destination MAC address.
- Source MAC address

Exercise 4:

Select a TCP packet in the **Packet List Window**.
Use the **Packet Details Window** to determine the following IP header values for the TCP packet:

- Version
- Internet Header Length (IHL)
- Identification
- Reserved bit
- Do not fragment bit
- More fragments bit

- Fragment offset
- Time To Live (TTL)
- Protocol
- Checksum
- Source IP Address
- Destination IP Address

Exercise 5:

Start a capture.

• Use combination of two filter statements with the and keyword. Apply a filter to display only http traffic traveling to or from your ip address. (Example: If your IP address is 10.10.10.2 enter ip.addr==10.10.10.2 and http.)
• Visit https://www.google.com and perform any search.
• Visit the first site on the list.
• Return to Wireshark and stop the capture. Analyze the packet data and answer the following questions:

- Are the identities of the web sites you visit private?
- Are the identities of the search keywords you enter private?
- Why do you think you are unable to find any traffic from your search?

Start another capture, or resume the same capture.

• Visit another website, say www.stack overflow.com and perform a search using the bar in the upper right hand corner.
• Return to Wireshark and stop the capture. Analyze the packet data and answer the following questions:

- Are the identities of the web sites you visit private?
- Are the identities of the search keywords you enter private?
- Why are you able to view the traffic from the Stack Overflow search, but not the Google search?

Exercise 6:

Start a capture, continue until you see the first 26 packets listed.

- What is the IP address of the client that initiates the conversation?
- Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.
- What is happening in frames 3, 4, and 5?
- What is happening in frames 6 and 7?
- Ignore frame eight. However, for your information, frame eight is used to manage flow control.
- What is happening in frames nine and ten? How are these two frames related?
- What happens in packet 11?