Hello Everyone! In this exercise, you will learn about Wireshark, a free tool for Network Monitoring. Wireshark is a packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

As you are aware, there are four layers of the TCP/IP model: network access, internet, transport, and application. Used together, these layers are a suite of protocols. The TCP/IP model passes data through these layers in a particular order when a user sends information, and then again in reverse order when the data is received. We use Wireshark which is a network protocol analyzer or an application that captures packets from a network connection.

When you first open Wireshark, you'll be presented with the start screen. There are four primary areas to the start screen.

The Main Menu
The Main Toolbar
The Filter Toolbar
The Interface List

Wireshark's main menu, is located at the top of the window when run on Windows and Linux, and the top of the screen when run on macOS.

The Menu displays 11 different items:

File to open/Merge capture files, save, print, export, and quit Wireshark

Edit to Find, time reference, or mark a packet. Handle configuration profiles. Set preferences.
View to Change display of capture data such as colorization of packets, showing packet in another window, zooming font, and collapsing and expanding trees.
Go to go to a specific packet
Capture to Edit capture filters and start and stop captures.
Analyze to Alter display filters, configure user specific decodes, enable or disable dissection of protocols, and follow TCP streams
Statistics to Display statistic windows, summary of captured packets, protocol hierarchy stats, and more
Telephony to Display telephony related stats such as media analysis, flow diagrams, protocol hierarchy stats
Wireless to Display IEE 802.11 wireless and Bluetooth statistics
Tools shows Various tools such as creating Firewall ACL rules and
Help to View basic help, manuals of command line tools, etc.
You will be carried over into the working screen once you pick an interface to work capture traffic from.

The Interface List is the area where the interfaces that your device has installed will appear. Before you can see packet data you need to pick one of the interfaces by clicking on it.

This is a quick access toolbar providing easy to use buttons for the most common functions of the main menu. Most of these buttons become active only after you've selected an interface to monitor.

Wireshark filter toolbar allows you to quickly edit and apply display filters to your capture. Display filters allow you to narrow down the packets that you've captured to only those that are relevant to what you're trying to see such as specific IP address sources and destinations, protocols, MAC addresses, etc.

Clicking on an interface or opening an existing capture file will take you to the working screen:
Primary Areas of the Wireshark Working Screen are
Title Bar
Packet List Pane
Intelligent Scrollbar
Packet Details Pane
Packet Bytes Pane
The Status bar

Every line in packet list pane represents one packet. By default, the pane is broken up into 7 columns, each of which provides useful identification data for each packet and can be sorted to help you better dissect the data. You can remove, add, and reorder the columns to suit your needs. Selecting a packet will show more details in the Packet Details Pane and Packet Bytes Pane.
The No. column assigns a unique number to each packet. It can also display a symbol to help identify the relationship between packets if you click on a packet.
Time Displays the timestamp for when the packet was captured. The format of this timestamp is customizable.

Source Displays the source IP or MAC address that the packet originated from.
Destination Displays the destination IP or MAC address that the packet was heading to.
Protocol Displays abbreviated protocol information for the packet.
Length Displays the packet length and
Info Displays additional information related to the packet.

If you are interested in a specific IP address you can use the filter ip.addr, which shows all packets
that define this IP address as the source or the destination. The snapshot shows an example, where the packets to and from an ip address 192.168.0.45 are being displayed.

It's very easy to apply a filter for a particular protocol also . Just write the name of that protocol in the filter tab and hit enter. In the example results for http protocol are displayed using this filter:

Here are two more examples for the protocols tcp and udp. Read the step-by-step manual for Wireshark, to get more understanding of this tool.

Thank You!