Wireshark basics

Getting to know Wireshark

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. As the name suggests, a packet sniffer captures (``sniffs'') messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages . A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/received from/by application and protocols executing on your machine.

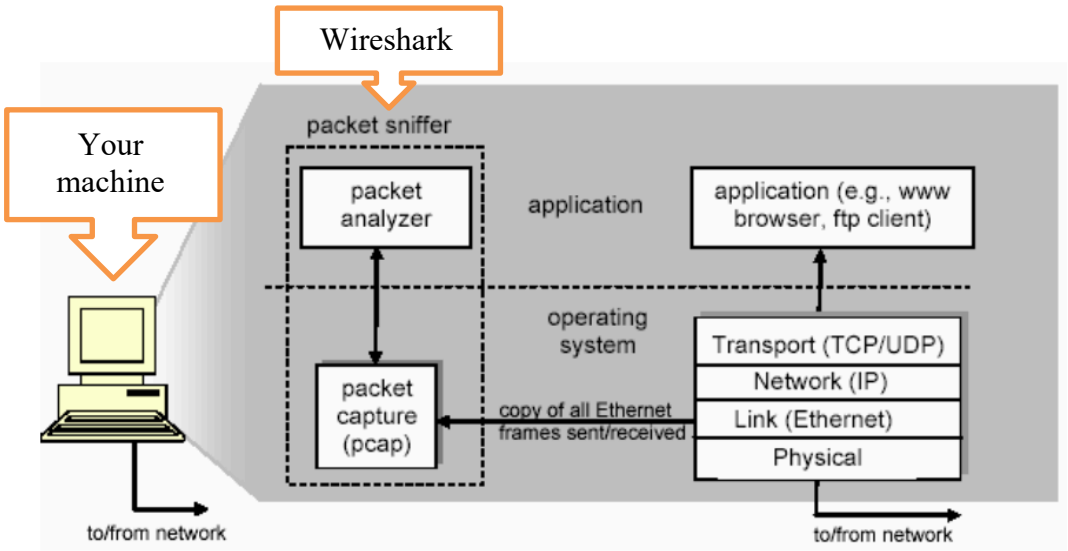

Figure 1. Packet Sniffer Structure.

Getting Wireshark

The Wireshark tool is available for the most popular platforms. You can download the software in your machine and follow the instructions to proceed with the installation.

https://www.wireshark.org/download.html

Starting Wireshark

After downloading and installing Wireshark, you can launch it and click the name of an interface to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface.

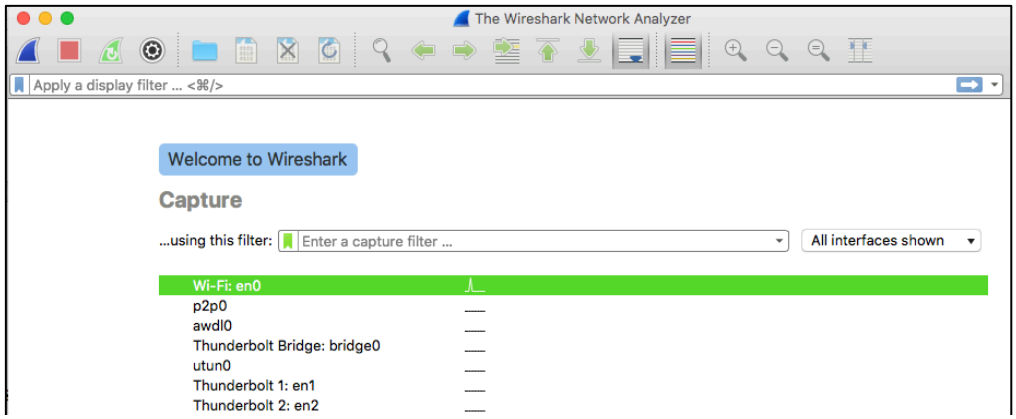

Figure 2. Capture Interfaces in Wireshark.

After to set the interface the capture program will start to collect the packet and display them on the interface. In particular, the Wireshark interface has five major components (see Figure 3):

The command **menus** are standard pulldown menus located at the top of the window. Of interest to us now is the File and Capture menus. The File menu allows you to save captured packet data or open a file containing previously captured packet data and exit the Wireshark application. The Capture menu allows you to begin packet capture.

The packet-**listing** window displays a one-line summary for each packet captured, including the packet number (assigned by Wireshark; this is not a packet number contained in any protocol's header), the time at which the packet was captured, the packet's source and destination addresses, the protocol type, and protocol-specific information contained in the packet. The packet listing can be sorted according to any of these categories by clicking on a column name. The protocol type field lists the highest-level protocol that sent or received this packet, i.e., the protocol that is the source or ultimate sink for this packet.
The packet-header **details** window provides details about the packet selected in the packet-listing window. These **details** include information about the Ethernet frame and IP datagram that contains this packet. The amount of Ethernet and IP-layer detail displayed can be expanded or minimized by clicking on the right pointing or down-pointing arrowhead to the left of the Ethernet frame or IP datagram line in the packet details window. If the packet has been carried over TCP or UDP, TCP or UDP details will also be displayed, which can similarly be expanded or minimized. Finally, details about the highest-level protocol that sent or received this packet are also provided.

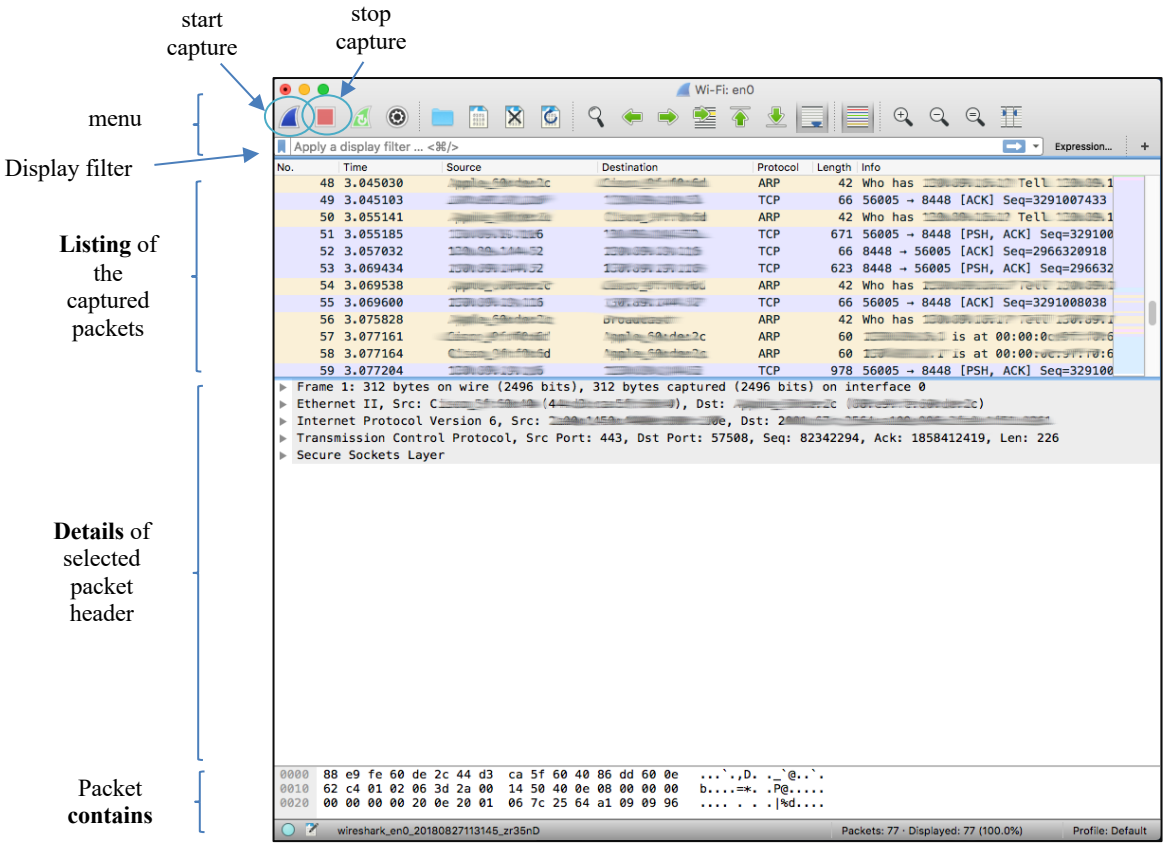

Figure 3. Wireshark Graphical User Interface.