Wireshark

What is Wireshark?

Wireshark is a network protocol analyzer. It provides us the tool for capturing, displaying, and analyzing messages that are exchanged in a network.

Installation

The Wireshark package can be downloaded from http://www.wireshark.org/download.html. Download the latest version. Note that in some computing environments, such as MS Windows, it is necessary to install a separate file capture utility (WinPcap for MS Windows). This utility is included to the latest version of the Wireshark installation package.

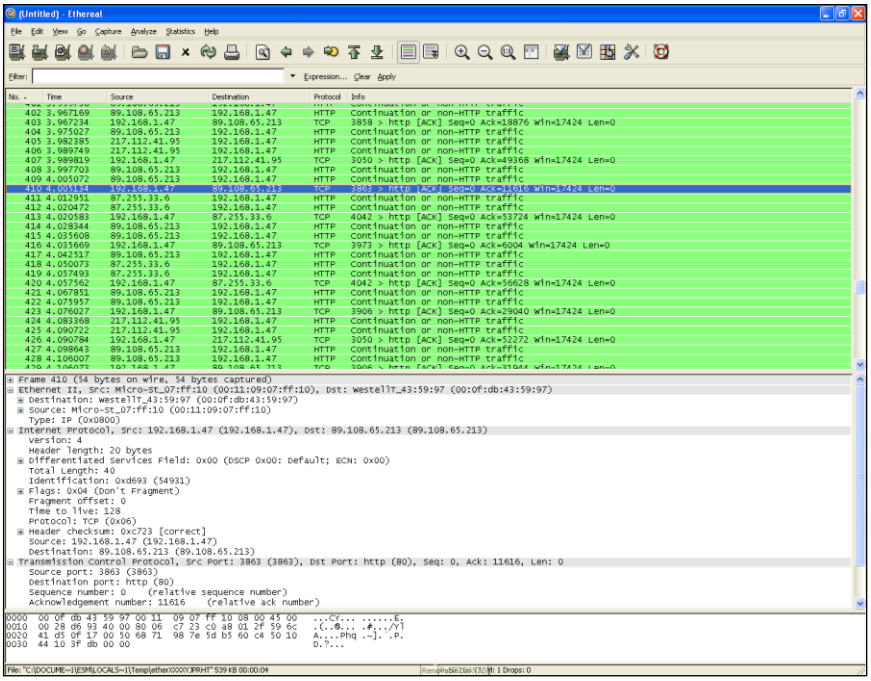
Installing Wireshark for macOS can be found here:
https://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallOSXInstall.html

Using Wireshark

Wireshark manual and introductory videos can be found here: http://www.wireshark.org/docs/

When you run the Wireshark program, the Wireshark graphical user interface will be displayed. Creating a packet capture file is straightforward. Once the Wireshark application (and packet capture utility) is installed, you simply start Wireshark and select the "Capture" menu option. Be sure that the interface option is set to whichever interface your computer uses if more than one is listed.

When you finish capturing packets, the information about the captured traffic will be shown on your screen:



The upper part of the screen shows the information about all packets transmitted or received by your device. You can use filters to display only specified patterns. When a packet is highlighted in the upper pane of the main window, the lower panes will show you more detailed information about a given packet. It will show each protocol layer of the selected packet: the physical layer frame, the Ethernet frame and its headers, the Internet Protocol datagram and its headers, Transport layer protocol datagram and its headers, and the Hypertext Transfer Protocol (HTTP) message. For each protocol, you can expand the information even further. For example, if you expand the IP Layer, you can see each field in the IP header including version, the header length, etc. The lowest part of the main window shows each byte of the data contained in the packet.