

Wireshark Tutorial

Getting Wireshark

Wireshark for Windows and Mac OS X can be easily downloaded from its [official website](#). If you are Linux users, you'll probably find Wireshark in its package repositories.

Detailed installing steps can be found on the Internet, so this tutorial won't cover this part.

Running Wireshark

When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 2 will be displayed. Initially, no data will be displayed in the various windows.

The Wireshark interface has five major components:

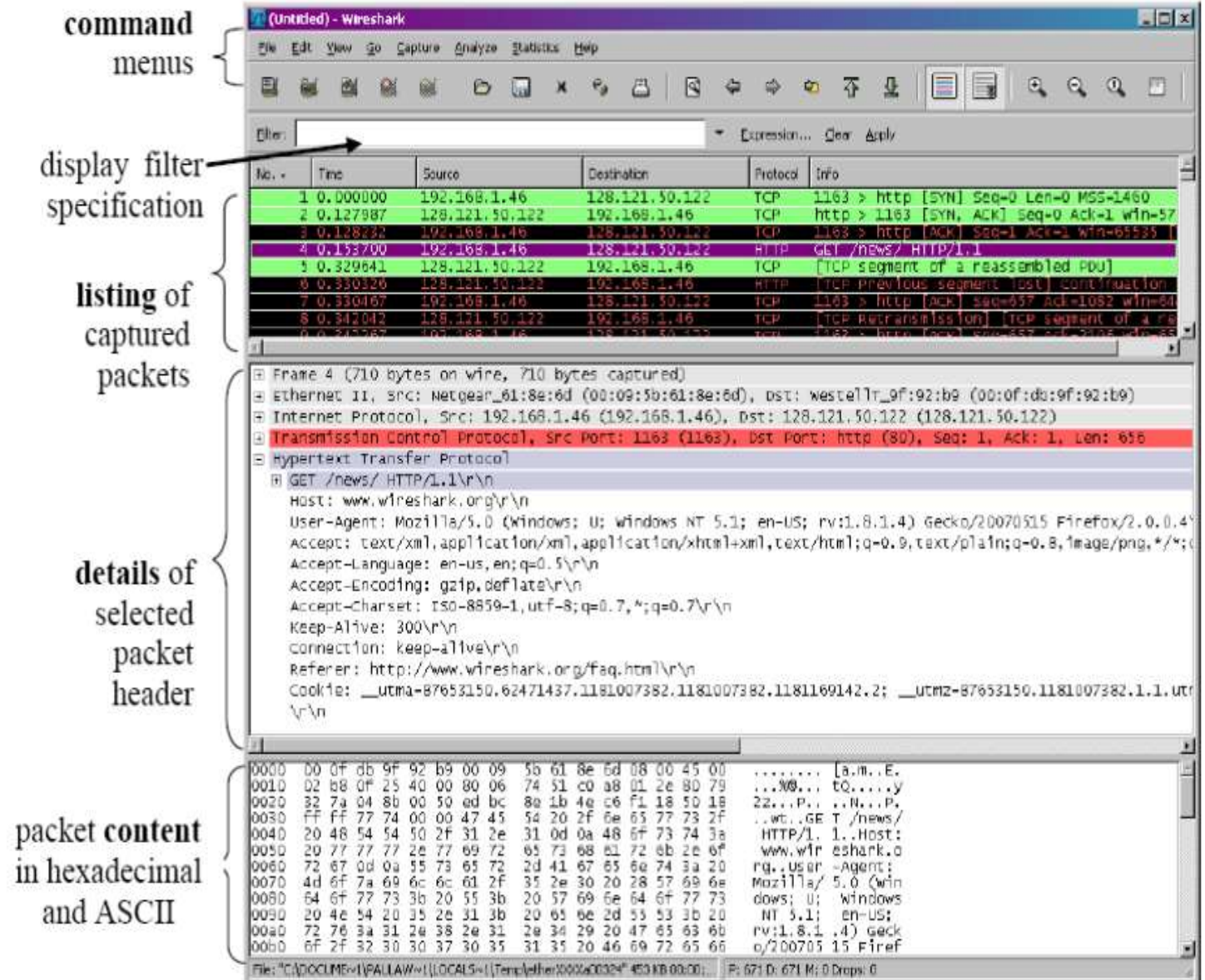


Figure 2

Running Wireshark(cont'd)

- The **command menus** are standard pulldown menus located at the top of the window. Of interest to us now are 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.

Running Wireshark(cont'd)

- The **packet-header details window** provides details about the packet selected (highlighted) in the packet listing window. (To select a packet in the packet listing window, place the cursor over the packet's one-line summary in the packet listing window and click with the left mouse button.). 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.

Running Wireshark(cont'd)

- The **packet-contents window** displays the entire contents of the captured frame, in both ASCII and hexadecimal format.
- Towards the top of the Wireshark graphical user interface, is the **packet display filter field**, into which a protocol name or other information can be entered in order to filter the information displayed in the packet-listing window (and hence the packet-header and packet-contents windows). In the example below, we'll use the packet-display filter field to have Wireshark hide (not display) packets except those that correspond to HTTP messages.

Test Run

The best way to learn about any new piece of software is to try it out! First, you need to know the network interconnections in the lab. The IP addresses are shown in Table 1. The 11 PCs are connected in the following fashion. $(1 \leftrightarrow 2)$, $(3 \leftrightarrow 4)$, $(5 \leftrightarrow 6)$, $(7 \leftrightarrow 8)$, $(9 \leftrightarrow 2)$, $(9 \leftrightarrow 1)$, $(10 \leftrightarrow 3)$, $(10 \leftrightarrow 4)$, $(11 \leftrightarrow 5)$, and $(11 \leftrightarrow 6)$. For ex $(1 \leftrightarrow 2)$ means Pc1 and Pc2 are connected to the same switch. So PC1 and PC2 can communicate with each other. To perform the following steps, identify the two PCs for your test run.

Test Run(cont'd)

Do the following:

1. Start up your favorite web browser.
2. Start up the Wireshark software. You will initially see a window like shown in Figure 3, except that no packet data will be displayed in the packet listing, packet-header, or packet-contents window, since Wireshark has not yet begun capturing packets. Make sure you check “Don't show this message again” and press “ok” on the small dialog box that pops up.
3. To begin packet capture, select the Capture pull down menu and select Interfaces. This will cause the “Wireshark: Capture Interfaces” window to be displayed, as in Figure 4.
4. The network interfaces (i.e., the physical connections) that your computer has to the network are shown. The attached snapshot was taken from my computer. You may not see the exact same entries when you perform a capture in the lab. You will notice that eth0 and eth1 will be displayed. Click “Start” for interface eth0. Packet capture will now begin - all packets being sent / received from/by your computer are now being captured by Wireshark!

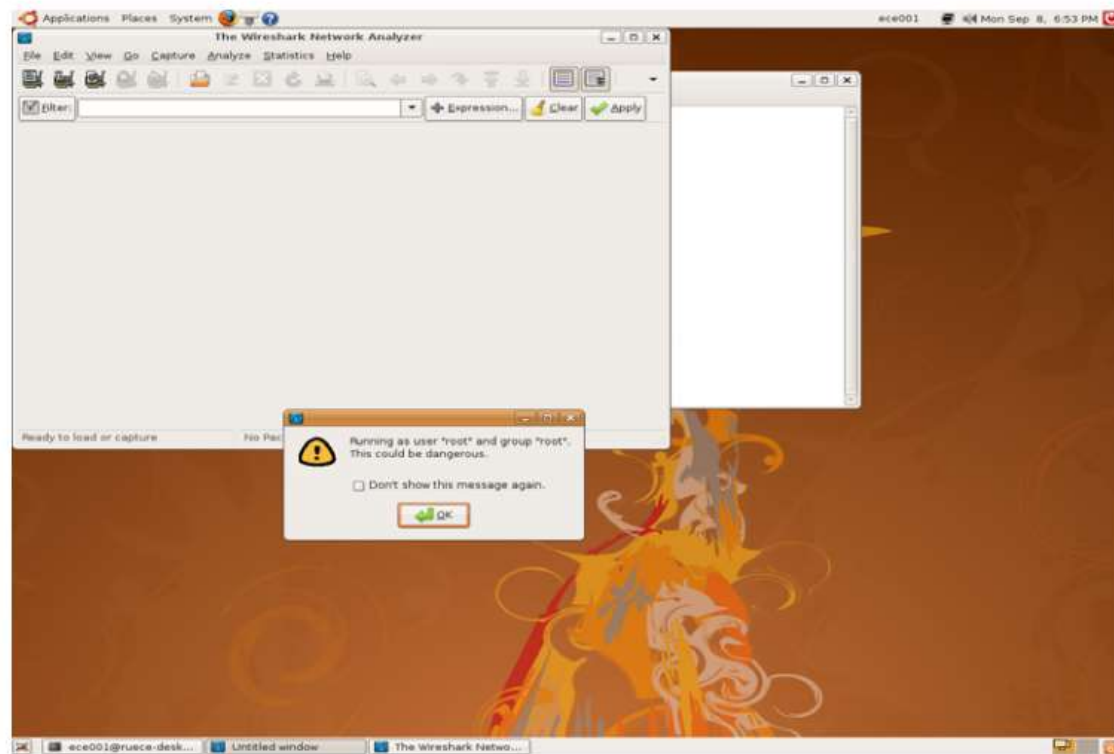


Fig. 3 Wireshark GUI

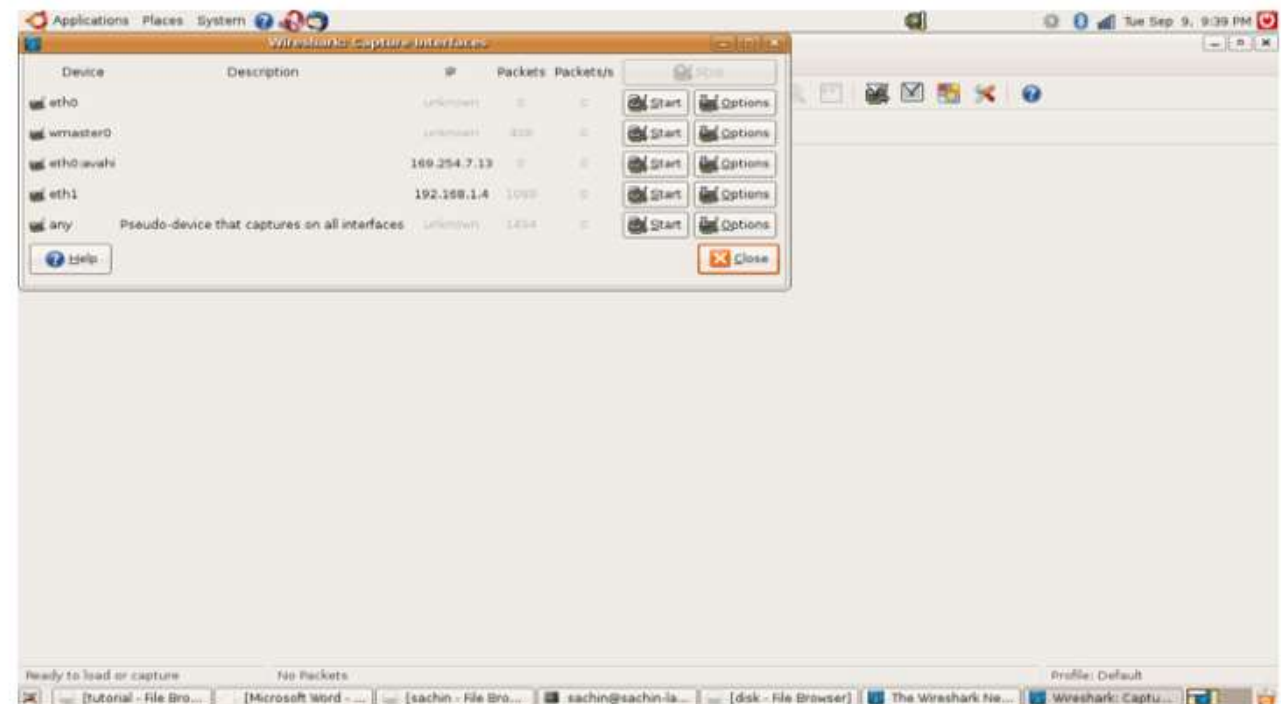


Figure 4: Wireshark Capture Interfaces Window

Test Run(cont'd)

5. If you started your Web browser on PC1, you can only connect to PC2 and PC9 (refer to the interconnections listed at the start of this section). If you want to connect to PC2, refer to Table 1, and identify the IP address of eth0. The IP address is 10.0.1.3. If you wanted to connect to PC9, the IP address would be 10.0.1.17. While Wireshark is running, enter the URL: `http://10.0.1.3/INTRO.htm` to connect to the web server in PC2 and have that page displayed in your browser. In order to display this page, your browser will contact the HTTP server at 10.0.1.3(PC2) and exchange HTTP messages with the server in order to download this page. The Ethernet frames containing these HTTP messages will be captured by Wireshark.

Test Run(cont'd)

6. After your browser has displayed the intro.htm page, stop Wireshark packet capture by selecting stop in the Wireshark capture window. This will cause the Wireshark capture window to disappear and the main Wireshark window to display all packets captured since you began packet capture. The main Wireshark window should now look similar to Figure 2. You now have live packet data that contains all protocol messages exchanged between your computer and other network entities! The HTTP message exchanges with the PC2 web server should appear somewhere in the listing of packets captured. But there will be many other types of packets displayed as well (see, e.g., the many different protocol types shown in the Protocol column in Figure 2). Even though the only action you took was to download a web page, there were evidently many other protocols running on your computer that are unseen by the user.
7. Type in “http” (without the quotes, and in lower case – all protocol names are in lower case in Wireshark) into the display filter specification window at the top of the main Wireshark window. Then select Apply (to the right of where you entered “http”). This will cause only HTTP message to be displayed in the packet-listing window.

Test Run(cont'd)

8. Select the first http message shown in the packet-listing window. This should be the HTTP GET message that was sent from your computer(ex. PC1) to the PC2 HTTP server. When you select the HTTP GET message, the Ethernet frame, IP datagram, TCP segment, and HTTP message header information will be displayed in the packet-header window². By clicking on right pointing and down-pointing arrows heads to the left side of the packet details window, minimize the amount of Frame, Ethernet, Internet Protocol, and Transmission Control Protocol information displayed. Maximize the amount information displayed about the HTTP protocol. Your Wireshark display should now look roughly as shown in Figure 5 (Note, in particular, the minimized amount of protocol information for all protocols except HTTP, and the maximized amount of protocol information for HTTP in the packet-header window).
9. Exit Wireshark

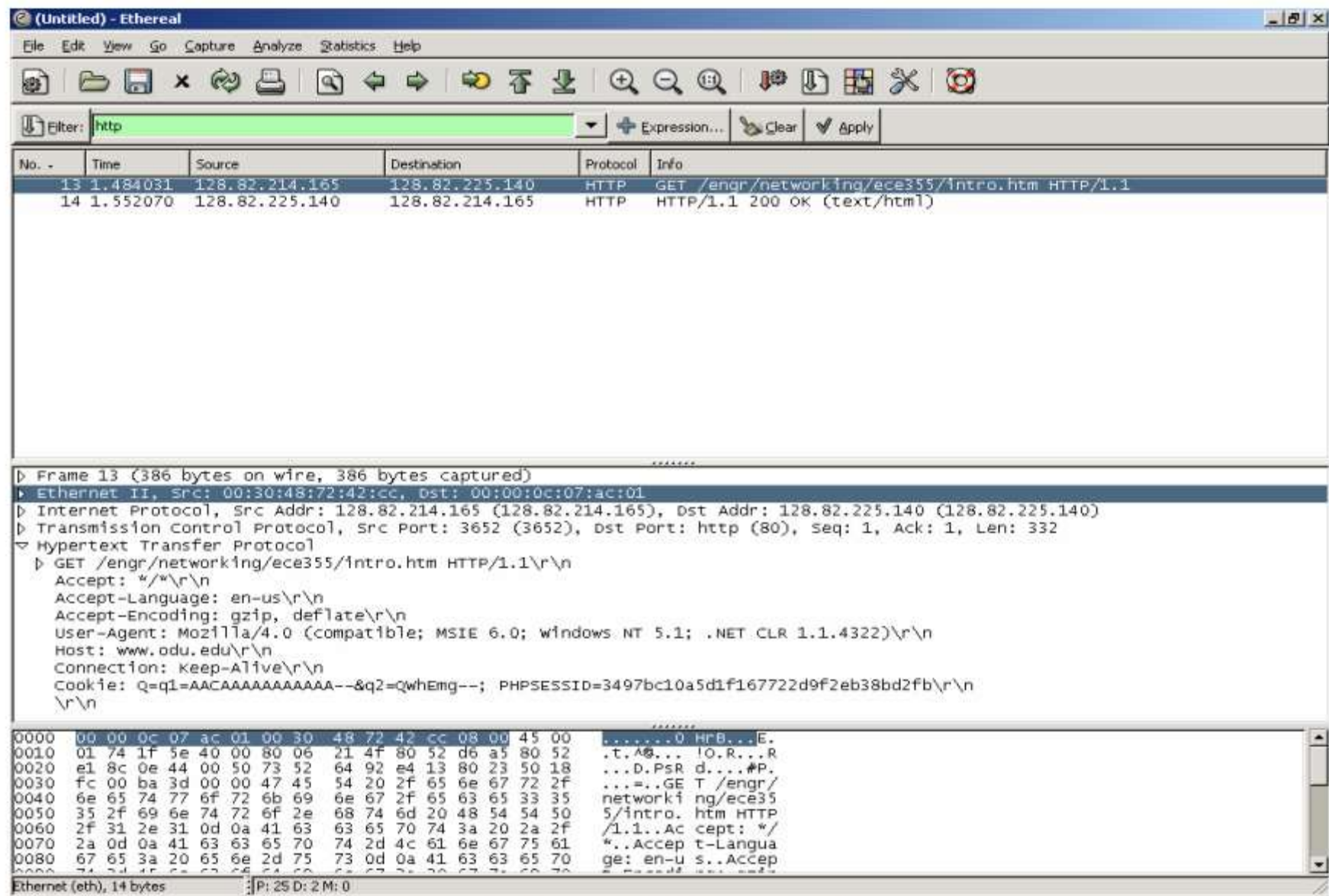


Figure 5: Wireshark display after step 9

More Tutorials

A detailed video tutorial could find in the following link:

<https://www.youtube.com/watch?v=TkCSr30UojM>

Official Tutorial Link:

<https://www.wireshark.org/docs/>