Lab Exercise 1: Sniffing HTTP Traffic with Wireshark (10 pts.)

What You Need

- A Computer running any OS. The instructions are written for Windows 7.

Installing Wireshark

Click the **Start** button. In the Search box, type **WIRESHARK**. If Wireshark is found, that means it's already installed and you can skip the following steps. If it is not found, go to **http://www.wireshark.org/download.html** to download and install it. It will also install WinPCap.

Capturing All Network Traffic With WireShark

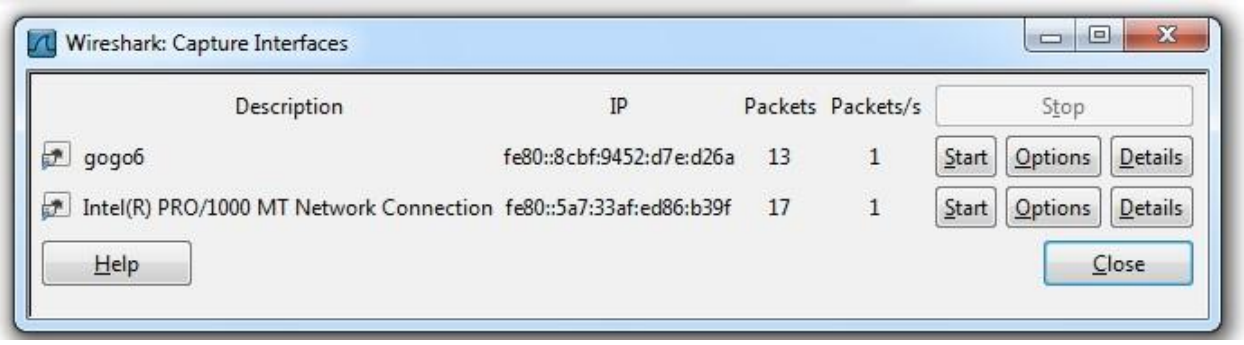
Click the **Start** button. In the Search box, type **WIRE**

At the top of the menu, a Wireshark item appears. Right-click **Wireshark** and click **"Run as Administrator"**. If a User Account Control box appears, allow the program to run.

Wiresharks opens, as shown below.

In the upper left of the Wireshark window, click "**Interface List**".

A list of network interfaces appears. Each interface has an IP address and a count of Packets, as shown below.

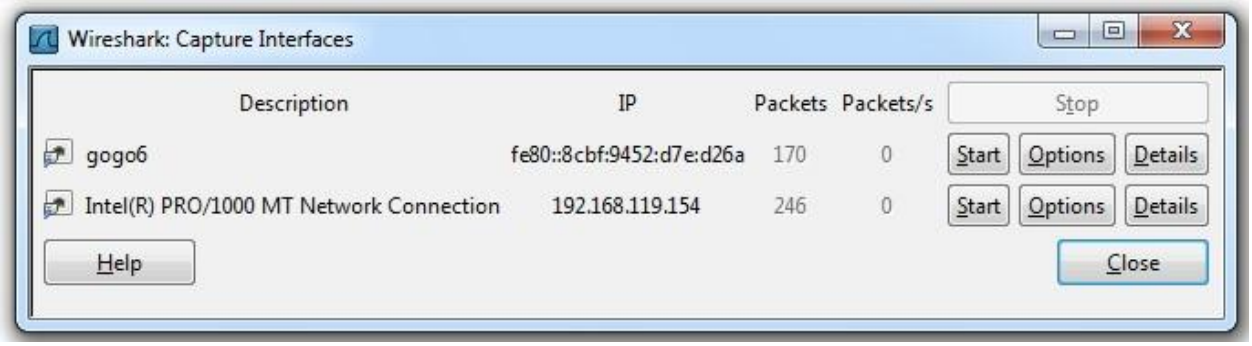


At first, all the IP addresses start with fe80: -- these are "Link-Local IPv6 Addresses", and they very useful.

Find the network interface with the most rapidly increasing number of packets--this is the interface that connects to the Internet. Click its IP address.

Wireshark will show the other addresses of this interface.

After one or more clicks, you should see the IPv4 address of the interface, which is four values separated by periods, as shown below:

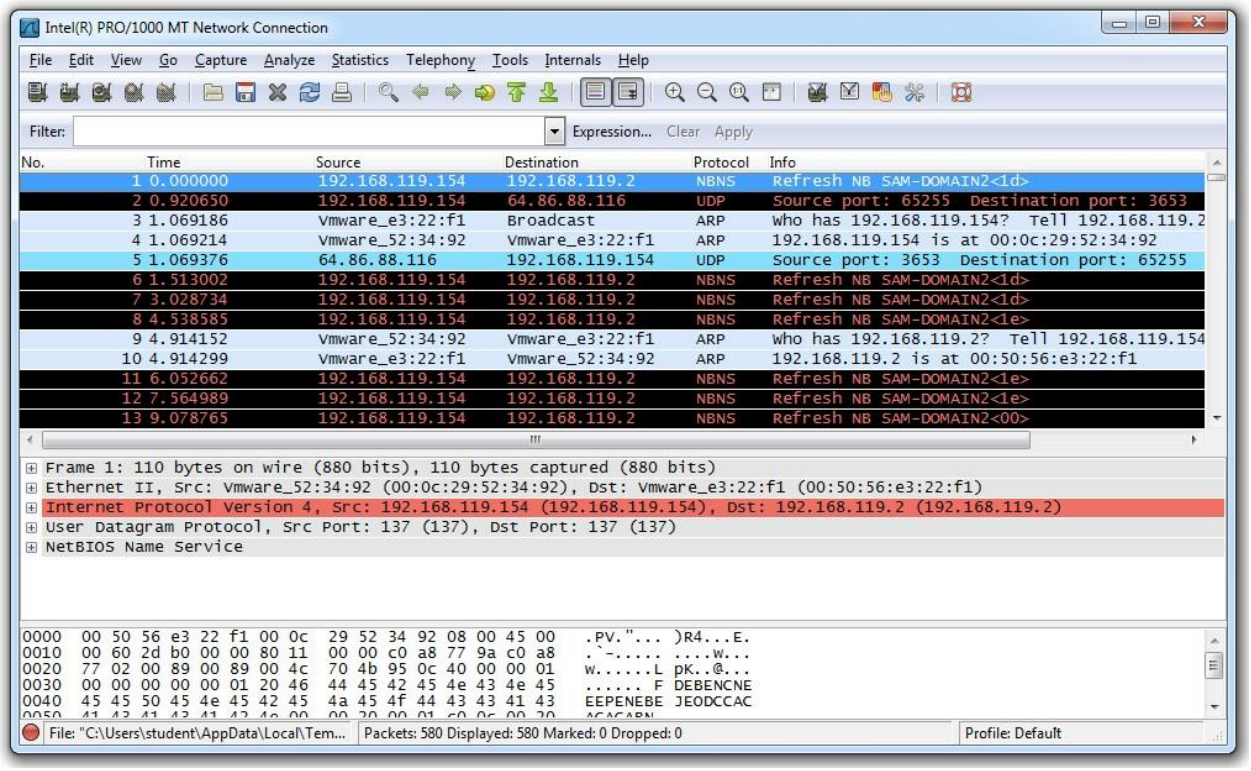


Click the **Start** button next to the interface that connects to the Internet.

You should see a lot of text scrolling by, as shown below on this page. Each line in the upper pane summarizes one frame (or packet).

Find these columns in the Wireshark window:

- **No** Frame Number
- **Time** Time in seconds that the frame was captured
- **Source** Source address of the frame
- **Destination** Destination address of the frame
- **Protocol** Protocol of the frame
- **Info** Other information



Notice that some lines show Broadcast in the Destination column. Broadcast traffic is common on networks as network devices alert one another of their presence. But it's usually not very interesting. To make Wireshark easier to use, you can Filter the traffic, to see only the interesting packets.

Capturing HTTP Traffic With WireShark

At the upper left of the Wireshark window, in the "Filter" bar, type **`http`**
Press the Enter key on the keyboard.

Wireshark now just sits there, with little or no visible traffic, because it is ignoring all the nonHTTP packets.

Loading the CCSF Web Page

In a Web browser, go to **www.ccsf.edu**

You should see a lot of text scroll by in the Wireshark window.

From the Wireshark menu bar, click **Capture**, **Stop**.

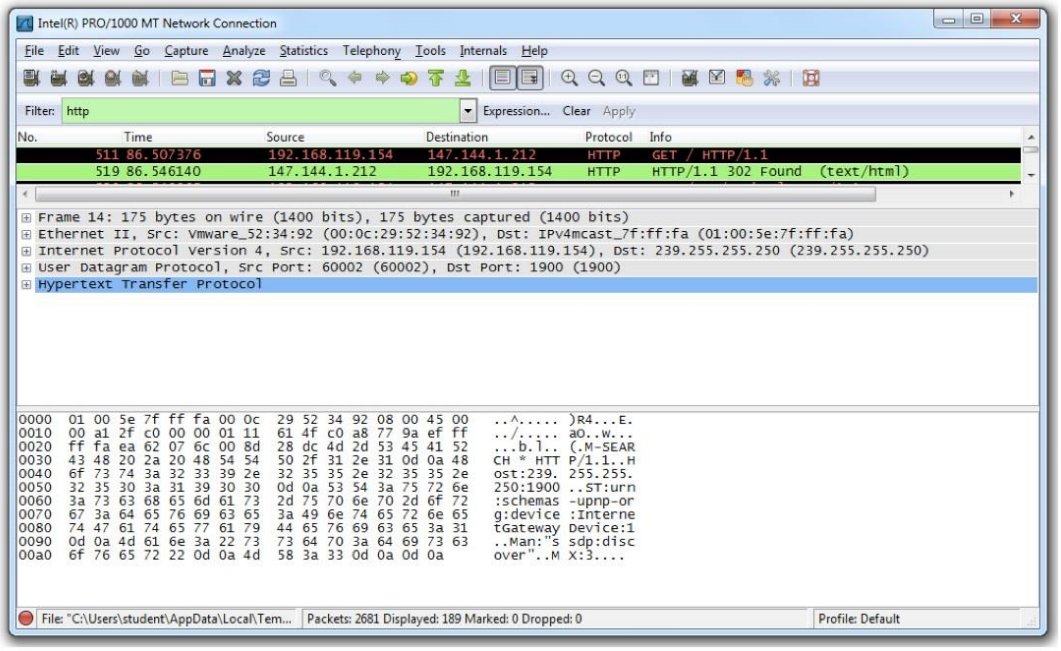
In the Wireshark window, scroll back to the top of the packet list.

Understanding HTTP GET Packets

The CCSF Web server has an IPv4 address of 147.144.1.212.

Find a packet with a Destination of 147.144.1.212 (the CCSF Web server), and "**GET / HTTP/1.1**" in the Info column. In the example below, it is packet number 511.

Find the response to that packet, with a Source of 147.144.1.212, and "**HTTP/1.1 302 Found (text/html)**" in the Info column. In the example below, it is packet number 519.



Saving the Screen Image

Resize the panes in Wireshark so that only these two packets are visible:

"**GET / HTTP/1.1**" and "**HTTP/1.1 302 Found (text/html)**", as shown above.

On your keyboard, press the PrntScrn key.

Click **Start**, type in **PAINT**, and open Paint.

Press **Ctrl+V** to paste in the image of your desktop.

YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT.

Save the image with a filename of "**LabExer1_[YOUR NAME]**".

Example: LabExer1_DonErickBonus **Turning**

In Your Project

Upload the Lab Exercise to Canvas.