CSCI 2150 – Computer Organization
Serial Protocol/Wireshark Lab

Purpose

The purpose of this lab is to allow you to examine the raw data captured from an Ethernet port. It should reinforce the information presented during the serial protocols lecture by allowing you to examine the components that make up an Ethernet frame, an IP packet, and a TCP packet.

Starting Wireshark

For this lab, we will be using a user interface for the Ethereal packet capture and dissection library called Wireshark. It is Open Source Software released under the GNU General Public License. For more information regarding this software, visit http://www.wireshark.org.

Each of the laboratory PCs in Nicks 491 has an installation of Wireshark. You can get to it through the Start menu from the Wireshark folder. Upon startup, you will be presented with a blank Wireshark window like that shown below.

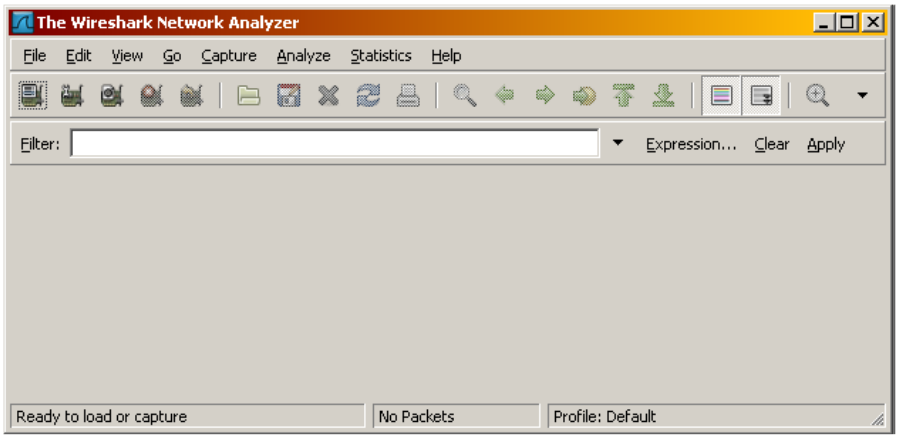

Figure A: Empty Wireshark Window

The icons along the top beneath the menu items allow quick access to most of the features of Wireshark. The first ten from left to right are:

- List available capture interfaces
- Show capture options
- Start a new live capture
- Stop running live capture
- Restart running live capture
- Open a capture file
- Save this capture file as
- Close this capture file
- Reload this capture file
- Print packets

We will only be using one of these options, "Open a capture file." The other options, however, are worth discussing.

The first icon, "List available capture interfaces," will be the typical starting point for capturing Ethernet packets that are visible from your network interface card. When clicked, it will give you a list of the available network adaptors on your machine. This includes both the installed physical adaptors

and virtual adaptors, their IP addresses, and any packet activity that is associated with each of these adaptors.

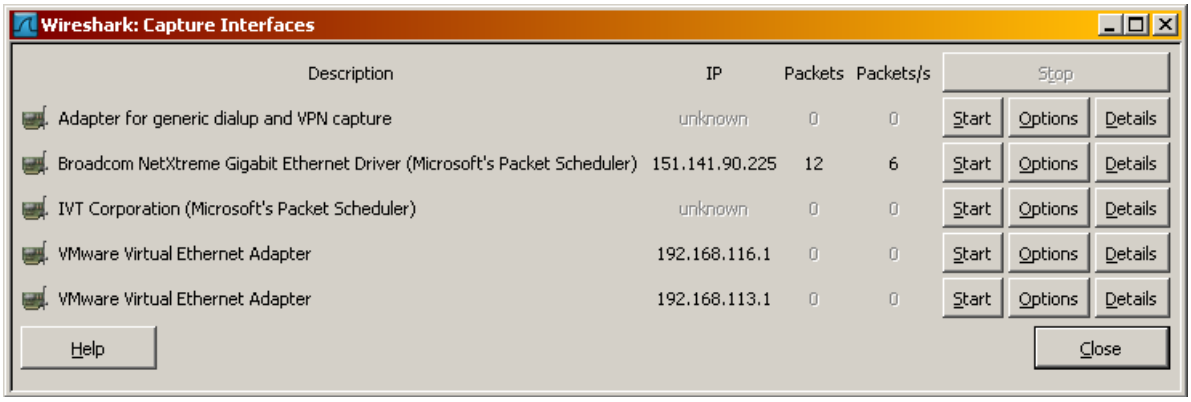

Figure B: Wireshark Adaptor List

The rightmost of the three buttons listed along with each adaptor is titled "Details" and is meant to give you access to any information regarding that adaptor. The enormous amount of information provided here includes driver, MAC address, NIC vendor, statistics, link status, and link speed.

To get an idea of what it looks like to capture this data, select one of the physical adaptors that is showing traffic, i.e., the number of packets is increasing, and click the "Start" button associated with that adaptor. The blank screen should have divided itself into three windows and now be filled with data.

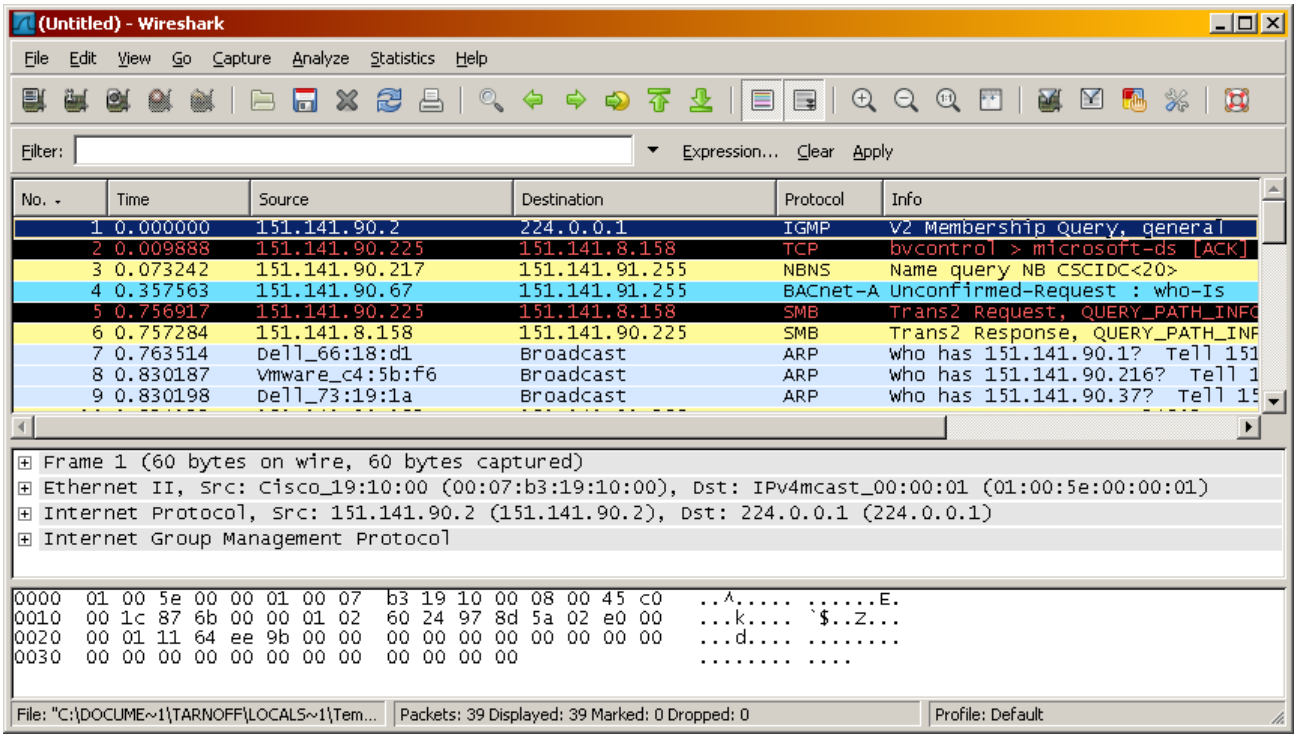

Figure C: Wireshark Window with Captured Data

If you do not see a number of messages loading to the screen, it may be that your adaptor setting is set to only see messages addressed to it. Click on the second icon, "Show capture options", and in the window that loads, click on the box, "Capture packets in promiscuous mode." This will allow Wireshark to capture all messages seen by this adaptor, not just the ones addressed to it.

After a significant number of messages appear, the capture can be stopped in order to examine a specific message.

Retrieving a Captured Session

In order to maintain consistency across all of the lab users, we will be using a captured session. ***Note: If you do not use the assigned capture session, your lab sheet will have incorrect data resulting in a loss of points.*** The following procedure will allow you to examine the correct captured file.

- Download the sample capture file from http://csciwww.etsu.edu/tarnoff/labs2150/network/SampleCaptureSession.cap. There is a link to this capture session in the Comments section for the "Serial Protocol Analyzer" lab on the CSCI 2150 Labs Page.
- Double clicking on this file or allowing Netscape to open the file using Wireshark will open a second session of Wireshark. If you do this, please close the first session.
- If you saved the capture session to the disk, open it by clicking on the Wireshark icon that looks like a folder (the "Open a capture file" icon) and selecting the downloaded file.

Once you have successfully opened the captured data file, the captured packets will appear in the Wireshark windows just as they did when you performed the live capture.

Evaluating a Frame

The three windows in the Wireshark main display screen present the details and data of the captured packets. The top window, the Packet List view, presents a list of all of the packets received during the capture session. The middle window is the Tree Details view. You will use this view to examine the components of the received packets. The bottom window, the Hex and ASCII Details view, shows the octets of the captured packed that has been selected in the Packet List view.

From the Packet List view, select a TCP packet. ***IMPORTANT: For the purpose of this lab, select message number 2.*** Once a packet has been selected, a user can examine not only the Ethernet packet information, but also the TCP and IP packet information from the protocol stack. In Figure D, packet number 9 has been selected from a different capture session.

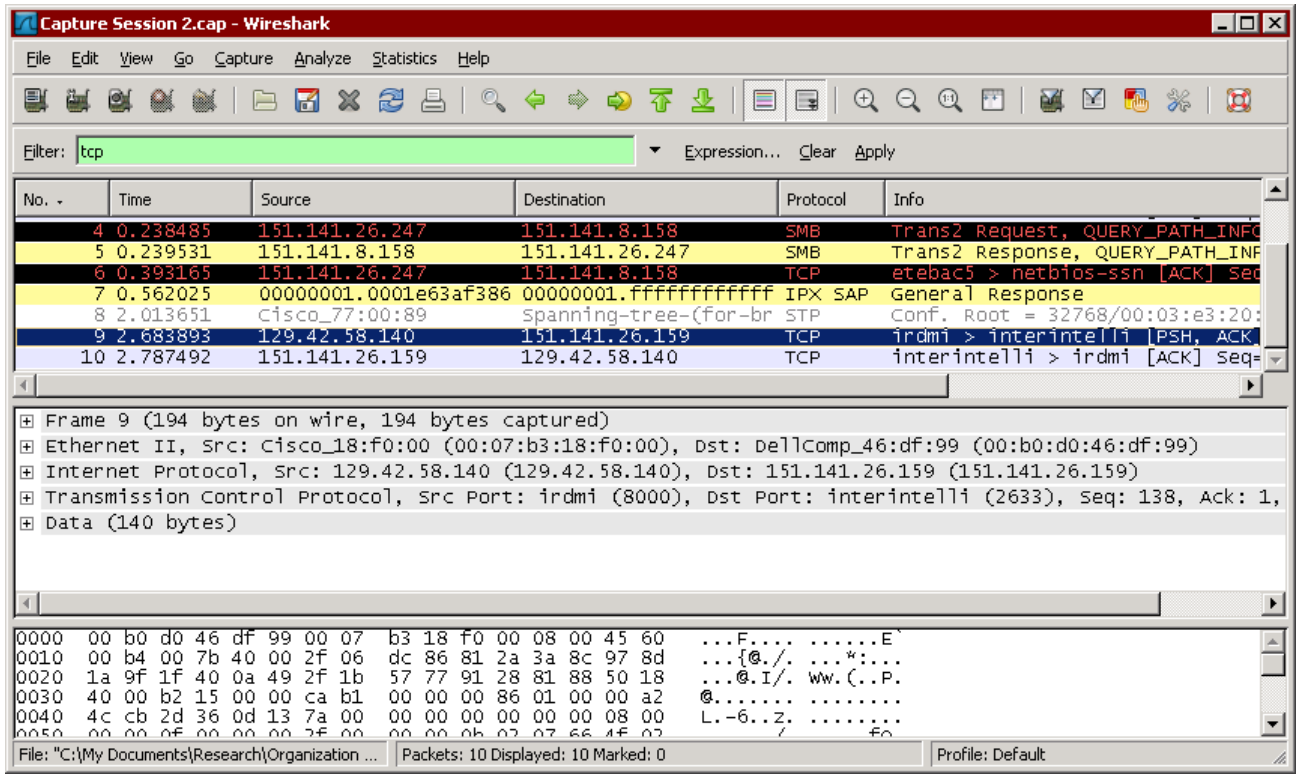

Figure D: The Three Wireshark Views with Message Selected

The middle window, the Tree Details view, now presents the parsed information from each of the protocols present in the packet. Clicking on the plus-sign next to any one of the message elements will expand the tree to reveal the details of that frame or packet. Figure E presents only this view with the Ethernet details expanded..

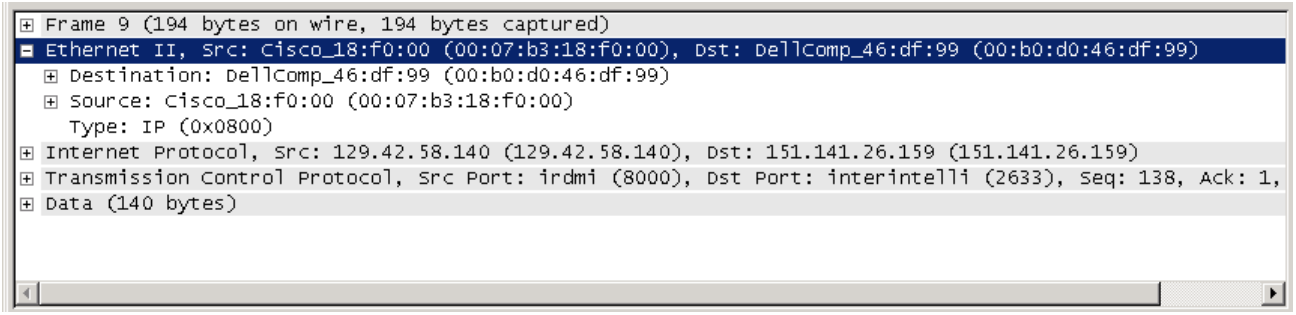

Figure E: Tree Details View with Ethernet Branch Expanded

By doing this, you can reveal the details of each level of the protocol stack.

Remember from the Ethernet frame discussion that the first three octets of the MAC address used by Ethernet identify the manufacturer. In the details revealed beneath the Ethernet identifier, it can be seen that the first three octets of the destination address in Figure E represents a Dell NIC while the first three octets of the source address represents a Cisco NIC.

The different views in Wireshark allow you to not only see the details of the different levels of the protocol stack – they also allow you to see the raw data. In Figure F below, you can see that by highlighting the Ethernet destination address in the Tree Details view, the corresponding raw data is highlighted in the bottom window, the Hex and ASCII Details view. This is true for any detail you highlight from the Tree Details view.

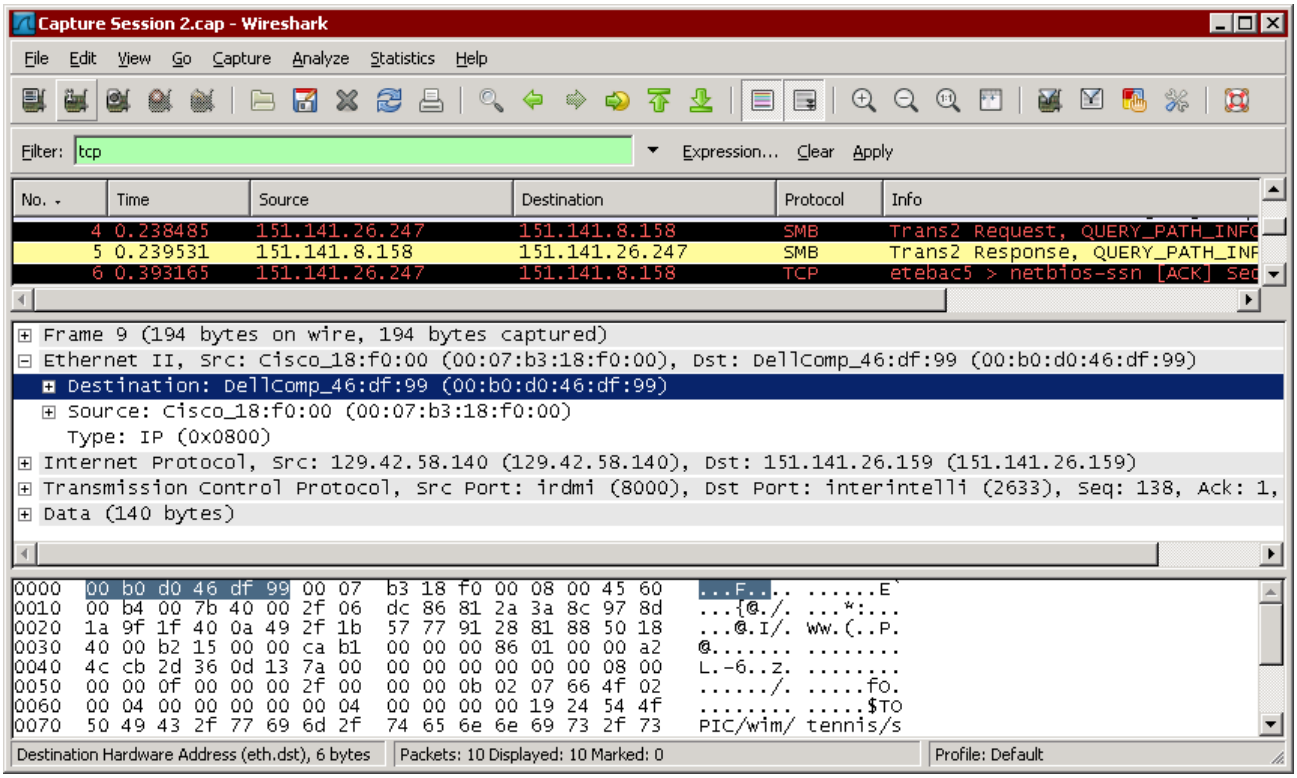

Figure F: Message with Raw Ethernet Destination Address Highlighted

Figure G shows how the properties of the IP header can be expanded.

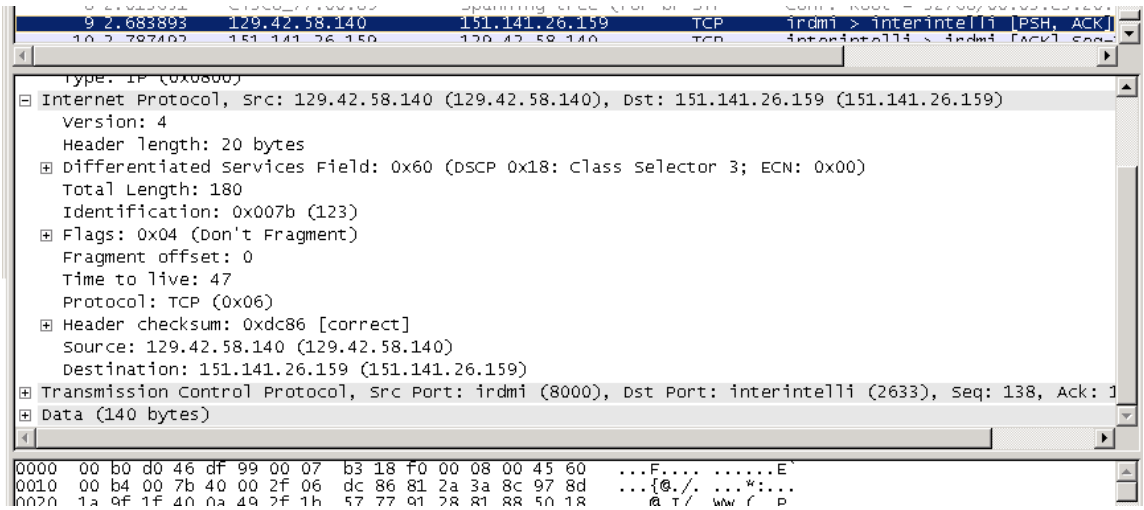

Figure G: Details of Internet Protocol Packet Revealed

From this expansion, the user can select details such as the header length, time to live, IP address, total length, and so on. If you select the total length,

Performing the Lab

Now let's do the lab. Using Wireshark's Tree Details view and Hex and ASCII Details view, dissect packet 2 determining the values for each element of the Ethernet frame, the IP packet, and the TCP packet. Record this information on your lab sheet. In addition, record the first 8 bytes of the data contained inside the TCP packet to your lab sheet. Before you leave, turn in your worksheet to the instructor.