Lab Exercise 2: Sniffing UDP and TCP Traffic with Wireshark (20 pts.)

What You Need

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

Purpose

In this project, you will examine common UDP and TCP traffic with Wireshark. Almost all network traffic relies on these two layer 4 protocols, and you must understand them thoroughly to be an effective networking professional.

Sniff all Traffic with Wireshark

Start Wireshark and begin sniffing all traffic, as you did in the previous project.

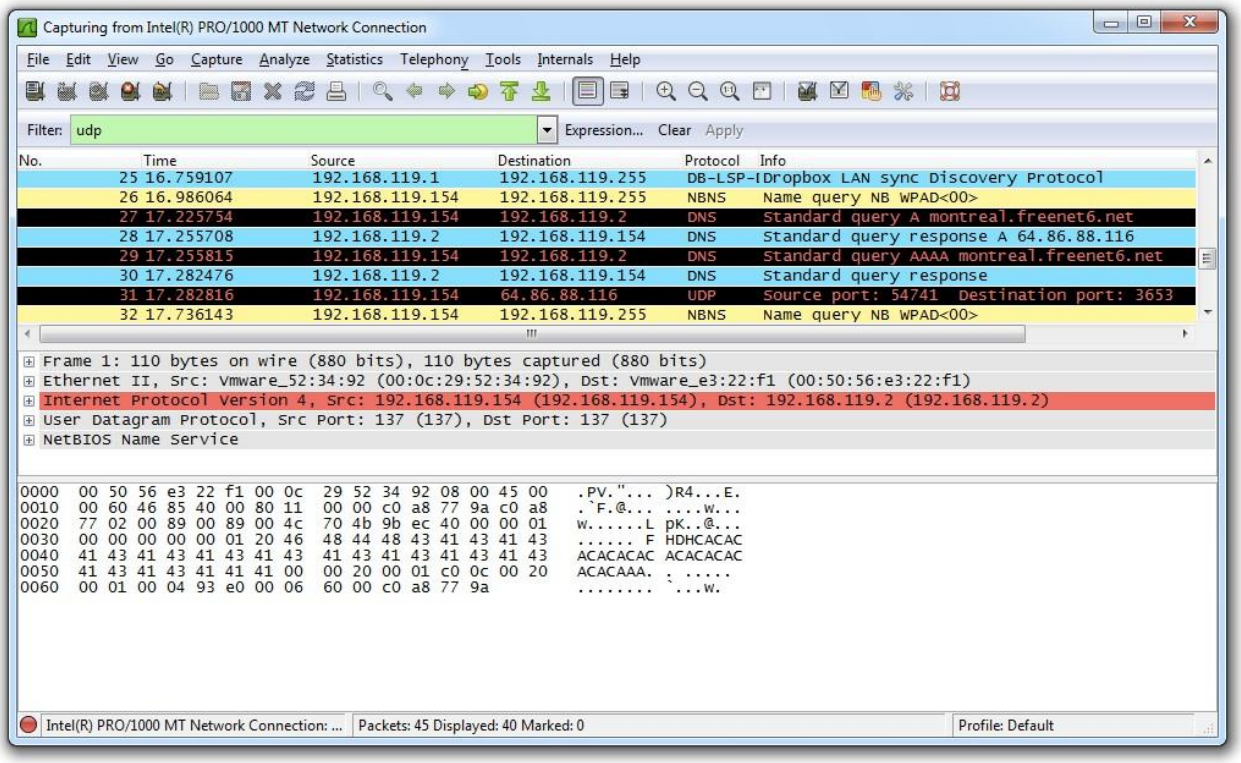
Examining UDP Traffic With WireShark

At the upper left of the Wireshark window, in the "Filter" bar, type

```
udp
```

Press the Enter key on the keyboard.

Packets scroll by, as shown below. These are background processes like Windows file-sharing and Dropbox running.



Performing a DNS Lookup

Click **Start**. In the Search box, type **CMD** and then press the Enter key.

A Command Prompt window opens, as shown below. Type this command, followed by the Enter key:

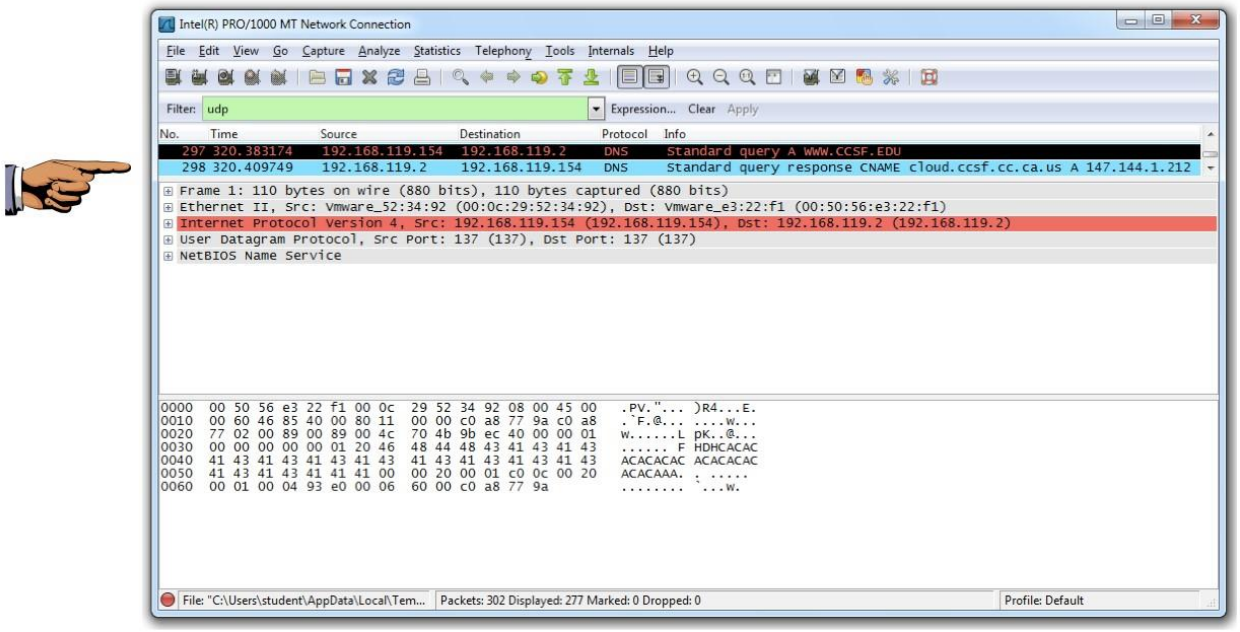
NSLOOKUP WWW.CCSF.EDU

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

for these two DNS packets, as shown below:

- **DNS Standard query A WWW.CCSF.EDU**
- **DNS Standard query response**

You may have to scroll up to find them.



These packets show a request to find the numerical IP address for the domain name WWW.CCSF.EDU and the response, delivering that request.

Saving the Screen Image

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

- **DNS Standard query A WWW.CCSF.EDU**
- **DNS Standard query response**

as shown above.

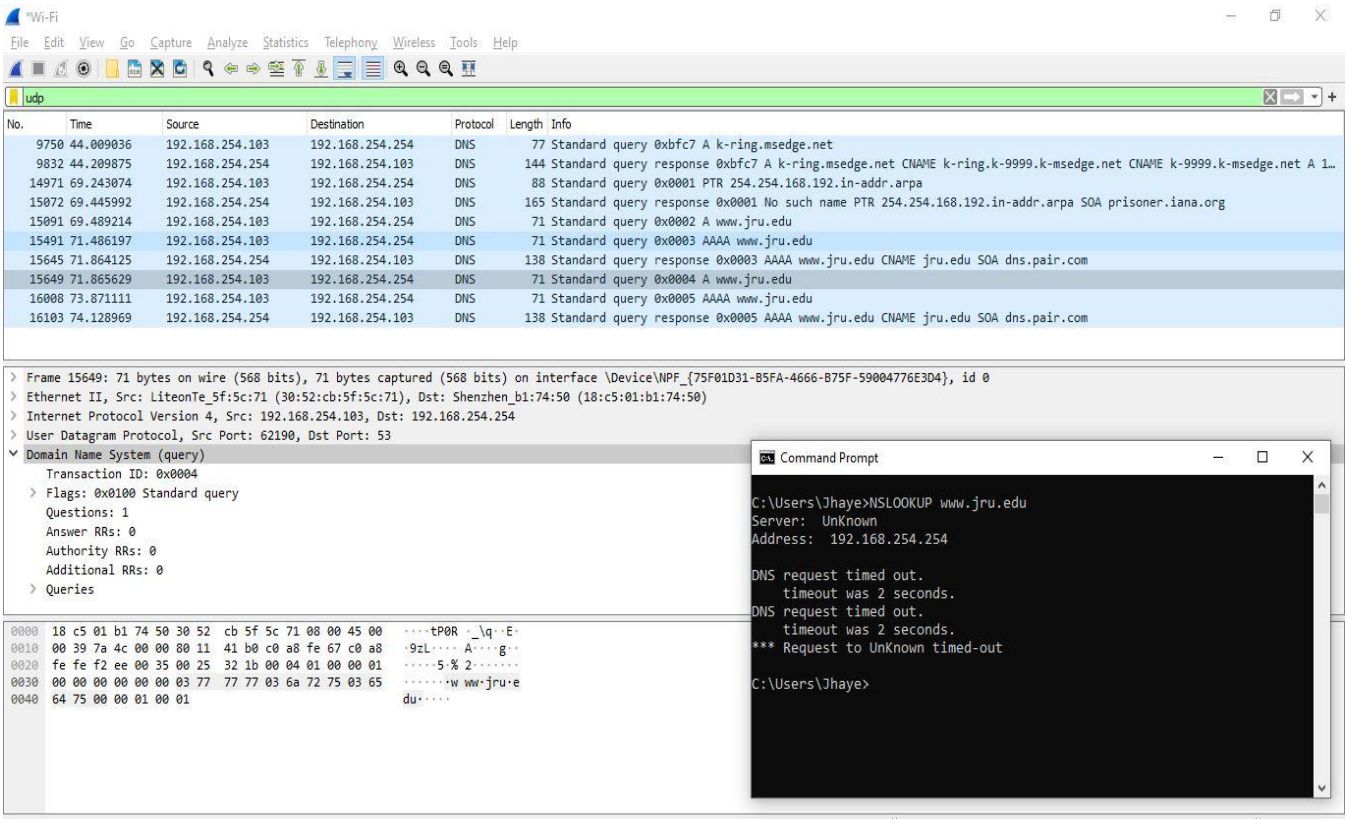
On your keyboard, press the PrntScrn key.

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 "**LabExer2_[YourName]**".



Capturing a TCP Handshake

In Wireshark, click **Capture**, **Start**. A box pops up asking if you want to save a capture file. Click "**Continue wuth g**".
At the upper left of the Wireshark window, in the "Filter" bar, delete the "udp" filter and type

`tcp.port==23`

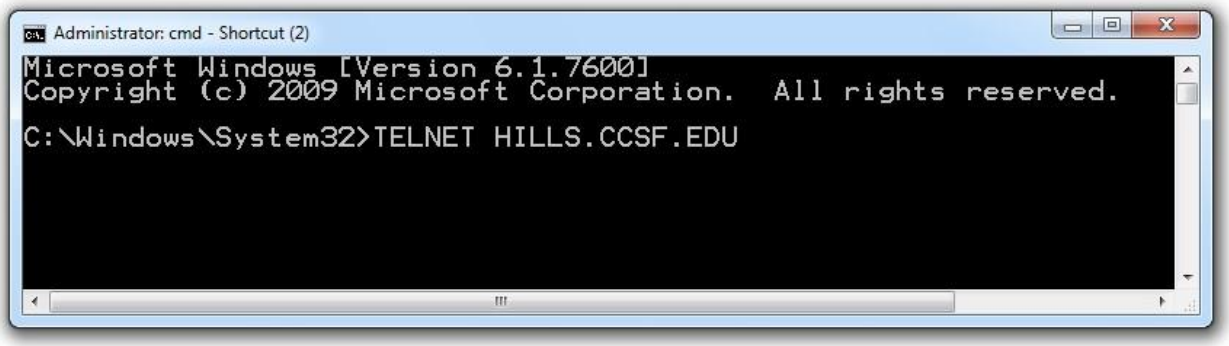
Press the Enter key on the keyboard.

This hides all the packets except TCP to or from port 23.

Making a Telnet Request

In the Command Prompt window, type this command, followed by the Enter key:

TELNET HILLS.CCSF.EDU



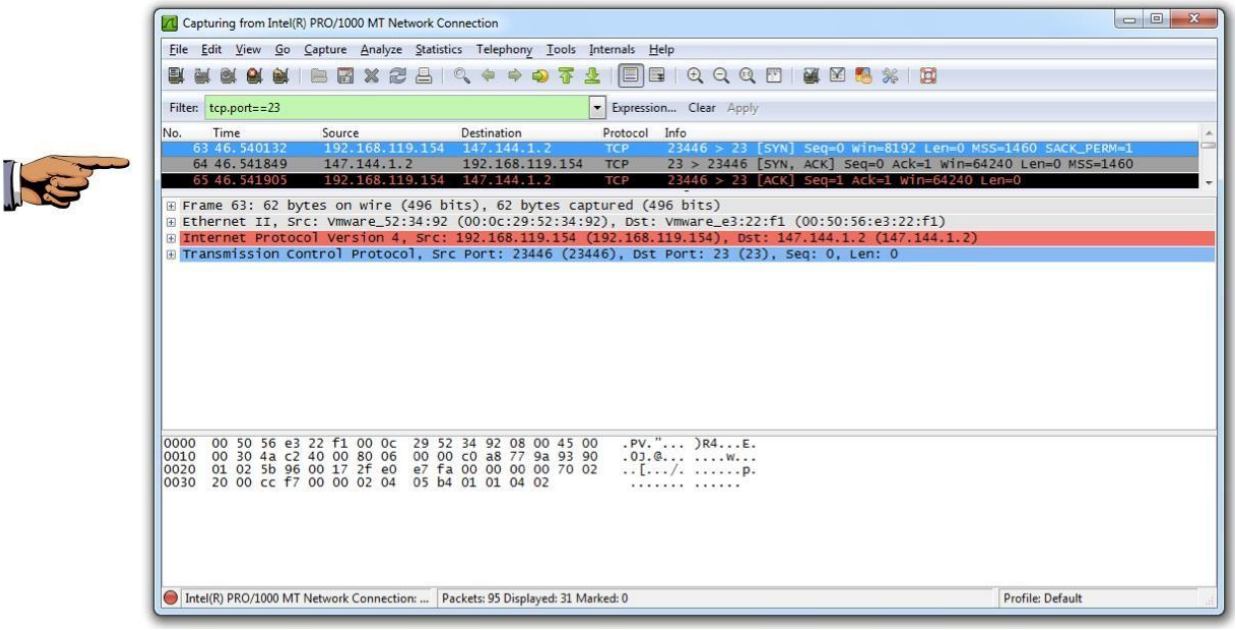
Troubleshooting

If telnet is not recognized, you need to install it:

Click **Start**, "**Control Panel**", **Programs**, "**Turn Windows features on or off**", and turn on the "**Telnet Client**".
You see a screen asking you to log in. Ignore that and switch to the Wireshark window.
You should see the three packets shown below, followed by other packets that aren't important right now.

Make sure you see these three packets in order, as described in the Info column:

- **[SYN]**
- **[SYN/ACK]**
- **[ACK]**



This is a TCP Handshake, opening a reliable channel of communication between two devices.

This particular one lets you use a very old command-line tool named Telnet, which should have been abandoned decades ago but, unfortunately, still remains in use.

Saving the Screen Image

Resize the panes in Wireshark so that only the three handshake packets are visible:

- **[SYN]**
- **[SYN/ACK]**
- **[ACK]**

as shown above.

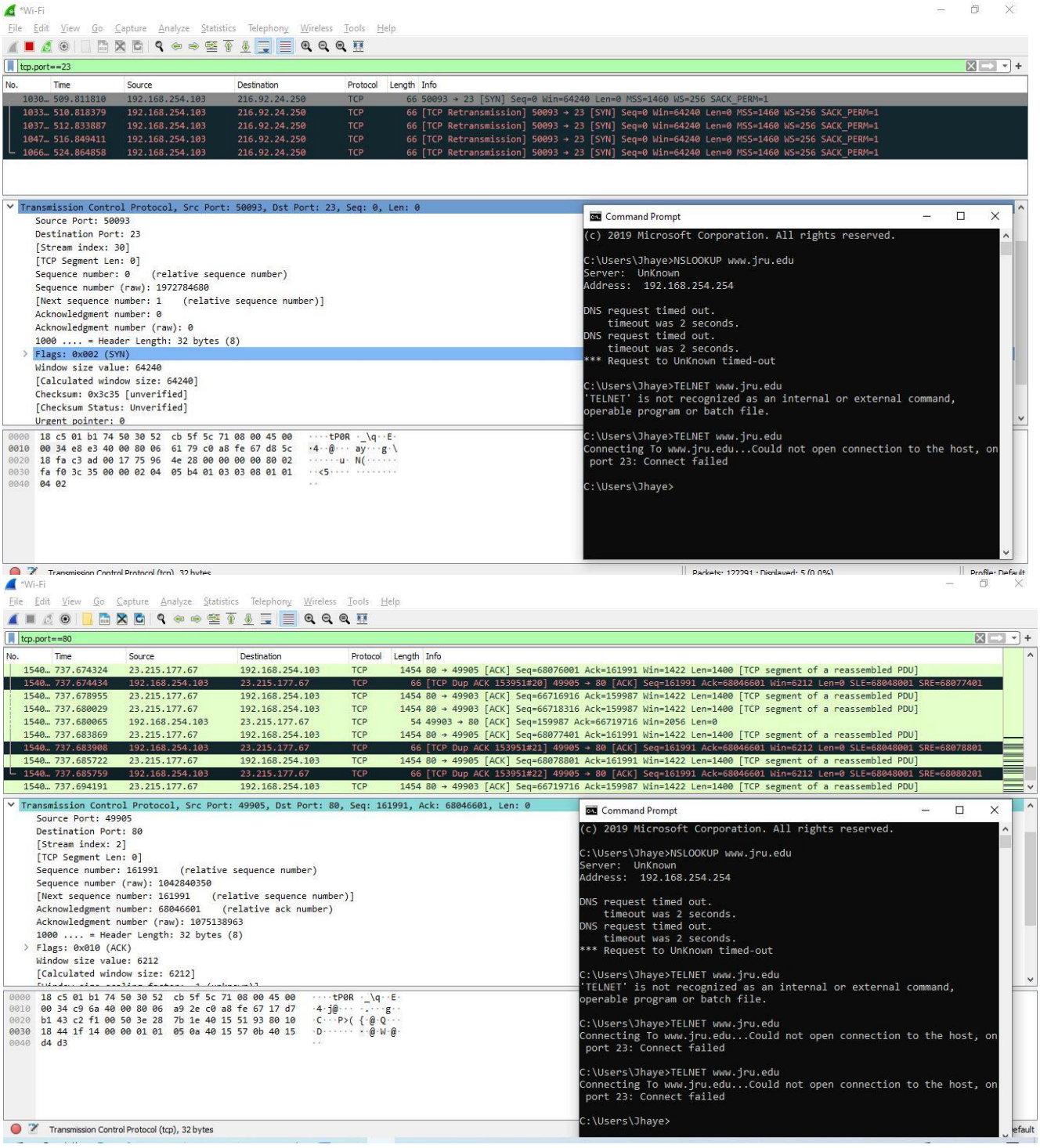
On your keyboard, press the PrntScrn key.

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 "**LabExer1B_[YourName]**".



Example: LabExer1B_DonErickBonus Turning

In Your Project

Upload the images to Canvas