Objective:

In this lab you learn how to use Wireshark to capture network traffic and then examine the traffic.

Background:

We will be using a set of labs that introduce Wireshark as a network traffic analysis tool. These labs supplement the networks textbook: *Computer Networking: A Top-Down Approach, 7th ed.*, by Kurose and Ross.

Here is their introduction to the labs (available at [http://www-net.cs.umass.edu/wireshark-labs/](http://www-net.cs.umass.edu/wireshark-labs/)):

“One's understanding of network protocols can often be greatly deepened by "seeing protocols in action" and by "playing around with protocols" - observing the sequence of messages exchanges between two protocol entities, delving down into the details of protocol operation, and causing protocols to perform certain actions and then observing these actions and their consequences. This can be done in simulated scenarios or in a "real" network environment such as the Internet. The Java applets in the textbook Web site take the first approach. In these Wireshark labs, we'll take the latter approach. You'll be running various network applications in different scenarios using a computer on your desk, at home, or in a lab. You'll observe the network protocols in your computer "in action," interacting and exchanging messages with protocol entities executing elsewhere in the Internet. Thus, you and your computer will be an integral part of these "live" labs. You'll observe, and you'll learn, by doing."

“The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer passively copies ("sniffs") messages being sent from and received by your computer; it will also display the contents of the various protocol fields of these captured messages. For these labs, we'll use the Wireshark packet sniffer. Wireshark is a free/shareware packet sniffer (a follow-on to the earlier Ethereal packet sniffer) that runs on Windows, Linux/Unix, and Mac computers. The Wireshark labs below will allow you to explore many of the Internet most important protocols.”

Instructions:

1. Complete [Wireshark Lab: Getting Started](#). At the end of the lab you will be asked to hand in 4 items. I have modified the first item by asking for some additional information.

2. Complete [Wireshark Lab: HTTP](#). This second lab has 5 sections with questions to be answered in each section. There are a total of 19 questions to be answered.

Hand in:

Hand in the answers to the questions in each of these first two labs.
Help Policy:

Help Policy in Effect for This Assignment: Group Project with Limited Collaboration

In particular, you may discuss the assignment and concepts related to the assignment with the following persons, in addition to an instructor in this course: any member of your group; any St. Bonaventure Computer Science instructor; and any student enrolled in CS 254.

You may use the following materials produced by other students: materials produced by members of your group.