Lab assignment 1: Getting familiar with Wireshark software

(Assigned Sept. 8th, Due date: Sept. 15th midnight via WebCourse)

In this simple assignment, you will install Wireshark software on your own desktop/laptop computer and get to know the basic procedure on how to use it to check network traffic.

Please go to: http://www.wireshark.org/ to download the software.

I want you to follow what I have demonstrated in class to capture the HTTP traffic when you check our college website: http://www.cecs.ucf.edu/.

Answer the following questions:

1. What is the IP address of your computer and the IP address of the website you connected? Did the web server keep the connection open? Did the server run HTTP 1.0 or 1.1?

2. How long did it take from when the HTTP GET message was sent to our college's webserver until the HTTP OK reply was received? (notes: there could be many http get and http ok packets during the packet capturing. Make sure you obtain the right pair of GET and OK messages.)

3. Save the HTTP GET message and the HTTP OK message. For the first HTTP GET message, right-click mouse on the selected packet. On the pop-up window, select "Copy"=>"Summary (Text)", which will save this HTTP GET message into a plaintext in the clipboard (then you can paste it into a text file to save it). Do this also for the corresponding HTTP OK message. Then copy the summary text content of both packets into the end of your lab report.

In addition, get a screenshot image (or two images) to show the above HTTP GET message and the HTTP OK message. Put this/these images in your report.

After finishing your lab report, submit it through Webcourse@UCF.

Hint: If you tried to connect to the website a few hours before you run Wireshark, you may not be able to capture the "HTTP OK" packet since the local browser has the content cached already. In this case, you can try to run Wireshark first and then use another browser to connect to the website for packet capture.