CNT4704 (Fall 2015)

Lab assignment 1: Getting familiar with Wireshark software

(Assigned Sept. 2th, Due date: Sept. 9th 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 one of my simple webpage at:

http://www.cs.ucf.edu/~czou/research.htm

Then 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. Find out the pairs of "HTTP GET" messages and their corresponding "HTTP OK" messages for your browser to retrieve all objects from this webpage. How many HTTP GET messages are used to retrieve this webpage? What are the byte size of images files contained in this webpage?
Hint: 1. There could be many http get and http ok packets during the packet capturing if your other webpage tabs are active. Make sure you obtain the right pair of GET and OK messages.
2. If your browser has visited the webpage shortly before, you may not get "HTTP OK" response but "HTTP/1.1 304 Not Modified\r\n". In this case, you can either clear your browser's cache, or use a different browser to visit the webpage.

3. Save all those HTTP GET messages and the HTTP OK messages for the webpage. 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 for each pair of GET and OK messages into the end of your lab report.

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

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