6397 Homework 1

Wireshark and Protocols

Final Version

In order to do this assignment, you have to download and install Wireshark (See http://www.wireshark.org/download.html). You will need a computer that you can connect to using ssh.

Part A. HTTP Protocol

- Start your browser.
- Start up the Wireshark without capturing packets.
- To begin packet capture, select (double click) the *Interfaces*. If you are on a desktop with a wired connection, choose Ethernet. If you are connected via a wifi, choose wifi.
- While Wireshark is running, visit COSC 6397 course website using your browser.
- Go to the lecture notes page (with the password), and retrieve the Gettysburg file: http://www2.cs.uh.edu/~acl/cs6397/Resource/Gettysburg.txt.
- Save the trace into a file.
- Exit Wireshark.

Use the filters to find all the packet exchanges between your machine and the server for this Gettysburg page. Please explain what is going on between the two machines. Take a screenshot of the Wireshark. This screen should show only the relevant HTTP exchanges.

Answer the question: from the data, can you see if a TCP connection is necessary for the HTTP connection? If yes, when does it terminate?

Part B. Secure Shell (SSH)

Similar to Part A capture all packets related to the SSH including the 3-way handshaking of the TCP. You should show and identify the followings:

- TCP handshaking.
- SSH protocol that establish the secured connection.
- Some data packets via SSH.
- TCP FIN.

We will discuss the SSH later. For this assignment, just identify the packets.