# CS 447: Networks and Data Communications

## Project #02

**Assigned Date** : Friday, October 24, 2014
**Due Date** : **Wednesday, October 29, 2014 @ 02:59:59 p.m.**

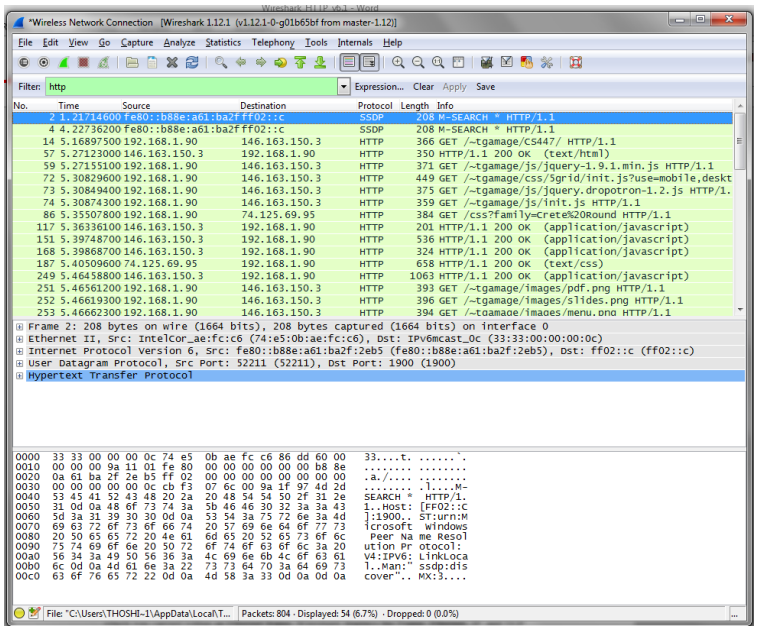
## Overview

The objective of this project assignment is to expose you to the `wireshark` packet sniffer/analyzer. As for that matter, there is no direct programming involved in this assignment, making this a much simpler assignment with a very short deadline. Having said that, you are highly encouraged to visit the wireshark wiki at http://wiki.wireshark.org/ to learn more about `Wireshark` and get a feel for its true power as a networking tool.

## Procedure

1. Install `Wireshark` on your local computer, if you haven't done already, by downloading the appropriate installer from https://www.wireshark.org/. (On Windows machines, you are also required install WinPcap, which should be prompted as an option during the default Windows Wireshark installation.)
2. Start Wireshark but do not start capturing. Enter `http` as the filter. Also select the appropriate network interface to capture traffic, if you machine has multiple interfaces.
3. Start your browser. Clear the browser cache. Enter the following URL at the address bar but don't hit `Enter` for now. http://www.cs.siue.edu/~tgamage/CS447/
4. Switch back to Wireshark and hit `Start` to begin capturing traffic.
5. Switch to the browser again and hit enter to visit the course home page.
6. Once the page is fully loaded, switch back over to Wireshark and stop the traffic capture.
7. Save your packet capture (*.pcapng)

At this point, your Wireshark window should look similar to the following.




## Deliverables

Your task is to reconstruct the TCP segment headers and the IP Datagram headers that corresponds to your packet capture. Consult the course textbook for details of TCP and IP header fields. You must attempt to fill in as much information as possible in as much detail as possible. For example, if you have evidence of IP fragmentation (which is highly likely), you must show that using separate datagrams corresponding to each fragment.

In addition, you are required to submit your saved packet capture as evidence of your work.

The due date of this assignment is **Wednesday, October 29, 2014 @ 02:59:59 p.m.**. A Moodle dropbox will be opened for your submission. A complete solution comprises of:

- A short report **in PDF format** that lists your reconstructed TCP segments headers and IP datagram headers. Provide an explanation of your observations. List the number of TCP segments and IP datagrams that was required for your HTTP data exchange.
- The RTT of the data exchange based on your traffic capture
- Your traffic capture evidence in .pcapng format

Similar to the last assignment, submit a compressed tarball that includes your PDF report and the captured traffic file. To create a compressed tarball of the directory source, use the following command: `tar -zcvf name111-pr1.tar.gz source/`. Obviously, change the name to your last name and 111 to the last three digits of your SIUE ID.