CS514 Homework 2
Due: Monday February 3

The primary purpose of this homework assignment is to get you using Ethereal, which was introduced in lecture 3. To prove that you've used it, though, you must capture a trace and answer the following questions about it. The trace must be for an HTTP (web) document download. You may chose any website you wish, but it is preferred that you choose a popular commercial website with relatively rich format (pictures, etc.).

After you get a trace, save it as text (using 'print', and print to file), with the settings 'print detail' and 'expand all levels'. To show that you found the packets you are looking for, you will need to cut and paste from this saved trace.

You will hand in three documents. One contains the answers to the questions. This document should be in the same format as last week's homework assignment. The second is a text file containing the parts of the trace that gave you the answers. The third is a text file containing a separate trace of (one of) the TCP conversation(s) that was used to transfer the web page.

Note, the first document should be ***one page****. The second will be short,* ***a few pages*** *at most, because it will only contain a DNS query/answer and a TCP SYN and SYN ACK. The third document should be truncated to* ***two pages*** *(the entire trace would be much longer than two pages).*

1. The first thing your computer should have done is a DNS query for the IP address(es) of the web site. How many IP addresses were returned in the answer to the DNS query? Include the DNS query and answer in the trace (second document) you hand in.

   (Hint: to find the DNS queries and answers, sort the Ethereal output by 'protocol'.) If you do not find a DNS query, it means that your machine has cached a previous DNS answer and did not have to do a query. In this case, pick another web site so that you force a DNS query.

2. Find the TCP connection over which the main web page was transferred (there may be separate TCP connections that transferred images, advertisements, and so on). Answer the following questions about it:
   a. What is the IP address of the web server?
   b. What are the initial TCP sequence numbers in both directions?

   Include the two packets (SYN and SYN ACK) that contain this information in the (second document) trace.

3. Ethereal has a feature where it shows the contents of a TCP conversation in a separate window. (Right click on one of the packets of the TCP stream, and click 'follow TCP stream'.) Save this TCP conversation and hand it in as the third document trace.

4. How many separate HTTP GETs were used to transfer the web page? (Hint: sort the ethereal display by the ‘Info’ column and count the GETs.) (Note: you do not have to include anything in the second trace document for this question.)