CPE 400/ECG 600 Wireshark Project
Due by 4:00pm Monday, Mar. 5

1. Download Wireshark from http://www.wireshark.org/download.html and install it.
2. Learn how to use Wireshark following the quick start tutorial.
3. Analyze a trace of IP datagrams sent and received by an execution of the traceroute program. Download *pingplotter* from http://www.pingplotter.com/download.html and install it. In the following, you will capture the IP packets generated by running traceroute.

   Do the following steps:
   - Start up Wireshark and begin packet capture *(Capture->Start)* and then press *OK* on the Wireshark Packet Capture Options screen.
   - Start up *pingplotter* and enter "www.google.com" in the "Address to Trace Window." Enter 3 in the "# of times to Trace" field. Select the menu item *Edit->Advanced Options->Packet Options* and enter a value of 56 in the *Packet Size* field and then press OK. Then press the Trace button.

     Next, send a set of datagrams with a longer length, by selecting *Edit->Advanced Options->Packet Options* and enter a value of 2000 in the *Packet Size* field and then press OK. Then press the Resume button.

     Finally, send a set of datagrams with a longer length, by selecting *Edit->Advanced Options->Packet Options* and enter a value of 3500 in the *Packet Size* field and then press OK. Then press the Resume button.
   - Stop Wireshark capturing.
   - Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. **Print out** the screen shot of this window with detailed information visible. Answer the following questions.

   1) What is the IP address of your computer?
   2) Within the IP packet header, what is the value in the upper layer protocol field?
   3) How many bytes are in the IP header? How many bytes are in the payload *of the IP datagram*? Explain how you determined the number of payload bytes.
   4) Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

   - Next sort the traced packets according to IP source address by clicking on the *Source* column header while keeping the no. field of in increasing order. Move through the ICMP messages sent by your computer and answer the following questions.

   5) Which fields in the IP datagram *always* change from one datagram to the next within this series of ICMP messages sent by your computer? Why?
   6) Which fields stay constant?
   7) Describe the pattern you see in the values in the Identification field of the IP datagram.

- Next find the series of ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router and answer the following questions.

8) What are the values in the Identification field and the TTL field?
9) Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?
10) Find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 2000. Has that message been fragmented across more than one IP datagram?
11) **Print out** the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?
12) Now find the first ICMP Echo Request message that was sent by your computer after you changed the *Packet Size* in *pingplotter* to be 3500. How many fragments were created from the original datagram?
13) What fields are changed in the IP header among the fragments?

4. Analyze the traces of HTTP GET/response interaction.
   Do the following steps:
   - Start up your web browser, and make sure your browser's cache is cleared.
   - Start up the Wireshark packet sniffer. Enter *ip.addr==xx.xx.xx.xx* (your host IP address) in the filter window, so that only the messages including your host IP address will be displayed later in the packet-listing window.
   - Enter the following URL into your browser http://www.ee.unlv.edu/~meiyang/cpe400/wireshark_test.htm.
   - Select the refresh button on your browser.
   - Stop Wireshark capturing.
     Print out the first HTTP GET message sent from your computer. Answer the following questions.

1) What is the IP address of your computer? Of the www.ee.unlv.edu server?
2) What version of HTTP is your browser running? What version of HTTP is the server running?
3) What languages (if any) does your browser indicate that it can accept from the server?
4) How many data-containing TCP segments are used to carry the single HTTP response? How many bytes of content are returned to your browser?
5) What is the total length of the third reply message? What is the total length of the TCP datagram? What is the data link protocol used? What fields are included in the data link protocol?
6) By inspecting the raw data in the packet content window, can you find the text "This is a test html for wireshark." in any of the reply message? **Print** the message if you find any.
7) Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header? Does this line exist in the first HTTP GET message?
8) What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file?