Lab Exercise 2: Examining HTTP with Wireshark[1]

(Total: 15 points)

OBJECTIVE:

The aim of this lab is to use Wireshark to examine details of the Web protocol HTTP and learn the communication between Web browsers and Web servers.

LAB ACTIVITIES:

Please go through the following lab activities and answer the questions in your lab report as required.

1. As we discussed in the lectures, most Web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object. Before performing the steps below, make sure your browser's cache is empty.
2. Start Wireshark from Windows VM or your personal computer and launch a packet capture.
   a. Enter http://cs.unb.ca/~wsong/lab_http1.html into your browser and your browser should display a very simple HTML file[2];
   b. Click the reload button to refresh the webpage within **the same tab** of your browser;
   c. Stop Wireshark packet capture and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
3. Examine your trace captured above and answer the following questions:
   a. Inspect the contents of the first HTTP GET request **for the Webpage "lab_http1.html"** from your browser to the server. Do you see an "If-Modified-Since" line in the HTTP GET?
   b. Inspect the contents of the server response to the first HTTP GET request. Did the server explicitly return the contents of the file? How can you tell?
   c. Now inspect the contents of the next HTTP GET request **for the Webpage "lab_http1.html"** 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?
   d. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET for "lab_http1.html"? Did the server explicitly return the contents of the file? Explain.
4. Next, let's start a new capture with Wireshark.
   a. Enter http://cs.unb.ca/~wsong/lab_http2.html into your browser and your browser should display a webpage with three embedded images;
   b. Stop the capture and enter "http" to only display the HTTP messages.
5. Examine your trace captured above and answer the following questions:
   a. How many HTTP GET request messages did your browser send? Were these request messages sent toward the same or different Web servers? How can you tell?

[1] The lab materials are adapted from the textbooks "Computer Networking – A Top-Down Approach" by James Kurose and Keith Ross and the materials provided with them. They can only be used by students who registered for this course. Reproduction outside of this course use is prohibited.

[2] Note: This is the exact URL you should use. Make sure that you are not visiting the secured UNB website, i.e., the URL cannot begin with "https". Also, you cannot use VPN while capturing the trace.

b. Was persistent or non-persistent HTTP used between your browser and the Web server? How can you tell?

c. According to the order of the HTTP messages for the embedded images, do you find the browser waits for the response for an earlier request before it sends the HTTP GET request for another image?

LAB REPORT:

Go through the above lab activities and write a report **answering the questions listed in item 3 and item 5**.

- **Please follow the lab report template in Microsoft Word posted on D2L.** Once you are done, convert your Word document into **a single PDF file** and submit it to the corresponding dropbox on D2L by the due time.
- In your report, you need to attach a **screenshot** of the packet trace to indicate where you find the answer to each question. You can capture the display in Wireshark using a screen capture software and then annotate the output packet trace with color markups to show the information related to your answers.