CS420 Computer Communication and Networks

Assignment 3
Assigned: 9/22/2015
Due: 9/29/2015 11:59 PM

Read the Wireshark Introduction document available on WesternOnline, and carry out the activities described in the document. In this lab, we'll explore several aspects of the HTTP protocol: the basic GET/response interaction, HTTP message formats, retrieving large HTML files, and retrieving HTML files with embedded objects.

1. The Basic HTTP GET/response interaction

1. Start up your web browser.
2. Start up the Wireshark packet sniffer (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.
3. Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
4. Enter the following to your browser http://www.wiu.edu/users/sjp111/cs420/HTTP-wireshark-file1.html. Your browser should display the very simple, one-line HTML file.
5. Stop Wireshark packet capture.

Questions:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
2. What is the IP address of your computer? Of the www.wiu.edu server?
3. What is the physical address of your computer? Of the www.wiu.edu server?
4. Inspect the HTTP header of the request packet and briefly describe the fields in it.
5. How many bytes of content are being returned to your browser in the HTTP response (not including the HTTP header)?

2. The HTTP CONDITIONAL GET/response interaction

Before performing the steps below, make sure your browser's cache is empty. (To do this under Firefox, select *Tools->Options* and click on *clear all current history*, or for Internet Explorer, select *Tools->Internet Options->Delete* under Browsing History; these actions will remove cached files from your browser's cache.) Now do the following:

1. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
2. Start up the Wireshark packet sniffer
3. Enter the following URL into your browser http://www.wiu.edu/users/sjp111/cs420/HTTP-wireshark-file2.html.
4. Click the refresh button on your browser

5. 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.

Questions:

6. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
7. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
8. 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?
9. 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? Explain.

3. Retrieving Long Documents

In our examples thus far, the documents retrieved have been simple and short HTML files. Let's next see what happens when we download a long HTML file. Do the following:

1. Start up your web browser, and make sure your browser's cache is cleared, as discussed previously.
2. Start up the Wireshark packet sniffer.
3. Enter the following URL into your browser http://www.wiu.edu/users/sjp111/cs420/HTTP-wireshark-file3.html. Your browser should display the rather lengthy US Bill of Rights.
4. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

   In the packet-listing window, you should see your HTTP GET message, followed by a multiple-packet response to your HTTP GET request. This multiple-packet response deserves a bit of explanation. Recall that the HTTP response message consists of a status line, followed by header lines, followed by a blank line, followed by the entity body. In the case of our HTTP GET, the entity body in the response is the entire requested HTML file. In our case here, the HTML file is rather long, and at 4700 bytes, is too large to fit in one TCP packet. The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment.

Questions:

10. How many HTTP GET request messages were sent by your browser?
11. How many data-containing TCP segments were needed to carry the single HTTP response?

12. What is the status code and phrase associated with the response to the HTTP GET request?

4. HTML Documents with Embedded Objects

Now that we've seen how Wireshark displays the captured packet traffic for large HTML files, we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server(s).
Do the following:

1. Start up your web browser, and make sure your browser's cache is cleared, as discussed previously.
2. Start up the Wireshark packet sniffer.
3. Enter the following URL into your browser http://www.wiu.edu/users/sjp111/cs420/HTTP-wireshark-file4.html. Your browser hould display a short HTML file with two images. These two images are referenced in the base HTML file. That is, the images themselves are not contained in the HTML; instead the URLs for the images are contained in the downloaded HTML file. As discussed in the textbook, your browser will have to retrieve these logos from the indicated web sites.
4. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

Questions:

13. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?
14. Can you tell whether your browser downloaded the two images serially (i.e., one after the other), or whether they were downloaded from the two web sites in parallel? Explain.
15. How many TCP connections were opened for the transfer of the page with the images to your browser? How can you tell?

What to submit

Answer the questions in a MS Word document or PDF file, and submit your file on WesternOnline before the due date.