Lab 3: HTTP Wireshark Lab (Week 4)

Due: Sep 27th 11:59 PM.

Important: ONLY use the Wireshark traces provided to answer the question. Do NOT capture your own trace to answer the question.

What to Submit: Only the answers to the 10 questions

Where to Submit: Blackboard only.

Material: Watch the instructor video on HTTP Wireshark lab.

1. The Basic HTTP GET/response interaction. Use **http_trace1** to answer Question 1 - 4. This trace was captured using the following steps. Do NOT capture your own trace to answer the questions.

    a. Start up your web browser.
    b. Start up the Wireshark packet sniffer, as described in the Introductory lab (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. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
    c. Wait a bit more than one minute and then begin Wireshark packet capture.
    d. Enter the following to your browser
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
    Your browser should display the very simple, one-line HTML file.
    e. Stop Wireshark packet capture.

    Q1: Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
    Q2: What is the status code returned from the server to your browser?
    Q3: When was the HTML file that you are retrieving last modified at the server?
    Q4: How many bytes of content are being returned to your browser?

2. The HTTP CONDITIONAL GET/response interaction. Use **http_trace2** to answer Question 5 – 8. This trace was captured using the following steps. Do NOT capture your own trace to answer the questions.

    Recall that 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.

    a. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
    b. Start up the Wireshark packet sniffer

c. Enter the following URL into your browser
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
Your browser should display a very simple five-line HTML file.
d. Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)
e. 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.

Q5: 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?
Q6: Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Q7: 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?
Q8: 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. HTML Documents with Embedded Objects. Use **http_trace3** to answer Question 9 – 10. This trace was captured using the following steps. Do NOT capture your own trace to answer the questions.

Here we 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).

a. Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
b. Start up the Wireshark packet sniffer
c. Enter the following URL into your browser
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
Your browser should 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. Our publisher's logo is retrieved from the gaia.cs.umass.edu web site. The image of the cover for our 5th edition (one of our favorite covers) is stored at the caite.cs.umass.edu server. (These are two different web servers inside cs.umass.edu).
d. Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

Q9: How many HTTP GET request messages did your browser send?
Q10: Was the connection persistent or non-persistent? How do you know?