|  |  |
| --- | --- |
| Wireshark Lab:  HTTP v8.0  Supplement to *Computer Networking: A Top-Down Approach, 8th ed.,* J.F. Kurose and K.W. Ross  *“Tell me and I forget. Show me and I remember. Involve me and I understand.”* Chinese proverb  © 2005-2020, J.F Kurose and K.W. Ross, All Rights Reserved | *A picture containing outdoor, water, bridge, building  Description automatically generated* |

FILL IN THE ANSWERS TO THE QUESTIONS 1 TO 10 AND 11-14 IF YOU HAVE TIME. ALSO HAND UP A PDF FILE WITH THE HTTP FRAMES YOU CAPTURED HIGHLIGHTING THE RELEVANT INFORMATION FOR EACH ANSWER.

1. The Basic HTTP GET/response interaction

By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the message you’ve found the information that answers the following questions. When you hand in your assignment, annotate the output so that it’s clear where in the output you’re getting the information for your answer (e.g., for our classes, we ask that students markup paper copies with a pen, or annotate electronic copies with text in a colored font).

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

It is running version 1.1

1. What languages (if any) does your browser indicate that it can accept to the server?

It accepts English-US and English

1. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

My computer = 128.119.245.12

Gaia.cs.umass.edu server = 10.100.106.170

1. What is the status code returned from the server to your browser?

304 not modified

1. When was the HTML file that you are retrieving last modified at the server?

Tuesday 8th of Feb 2022 06:59:01

1. How many bytes of content are being returned to your browser?

650 Bytes

In your answer to question 5 above, you might have been surprised to find that the document you just retrieved was last modified within a minute before you downloaded the document. That’s because (for this particular file), the gaia.cs.umass.edu server is setting the file’s last-modified time to be the current time, and is doing so once per minute. Thus, if you wait a minute between accesses, the file will appear to have been recently modified, and hence your browser will download a “new” copy of the document.

2. The HTTP CONDITIONAL GET/response interaction

Answer the following questions:

1. 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?

Yes

1. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes as it says http.request\_number

1. 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?

No it is not modified

1. 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.

N/A as not modified

3. Retrieving Long Documents

Answer the following questions:

1. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

My browser sent 1 HTTP GET message

121

1. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

10

1. What is the status code and phrase in the response?

200

1. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

15.3, (10,11, 13)