Shammah Thao

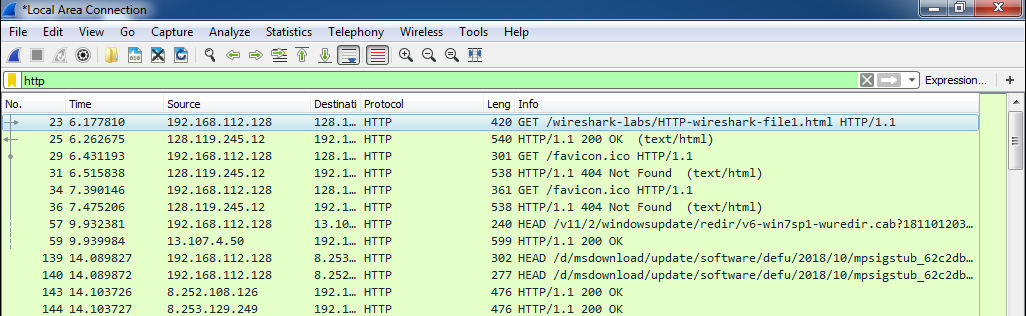
3/2/20

CPE 138

Wireshark Lab #2

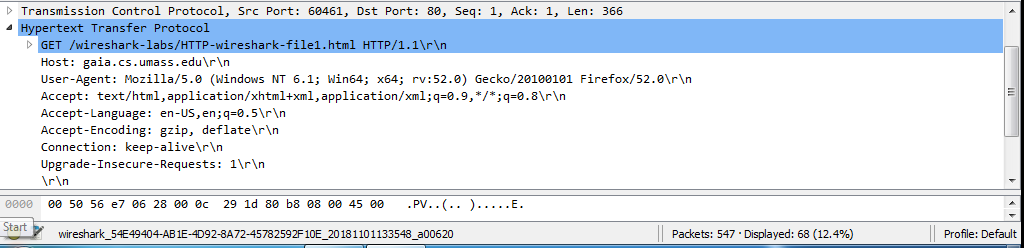
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running HTTP version 1.1. The version of HTTP is the server running is 1.1.



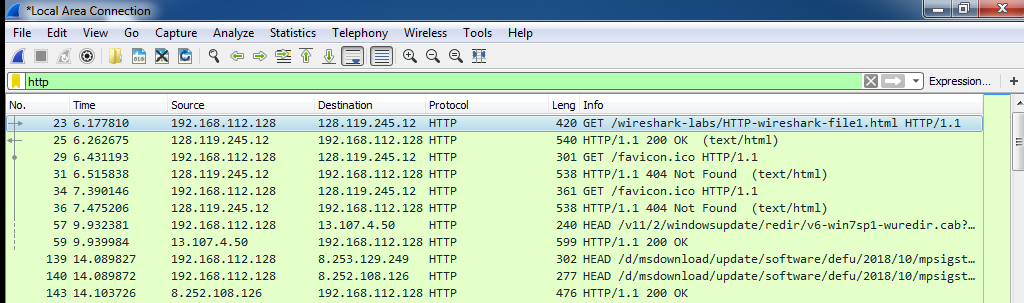
2. What languages (if any) does your browser indicate that it can accept to the server?

The language that my browser indicate that it can accept to the server en-US.



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

The IP address of my computer is 192.168.122.128 and the gaia.cs.umass.edu server is 128.119.245.12.

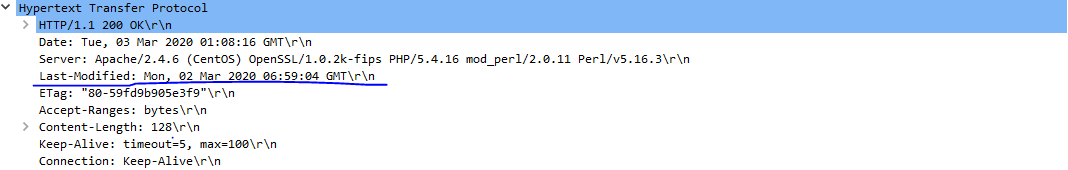


4. What is the status code returned from the server to your browser?

The status code returned from the server to my browser is 200.

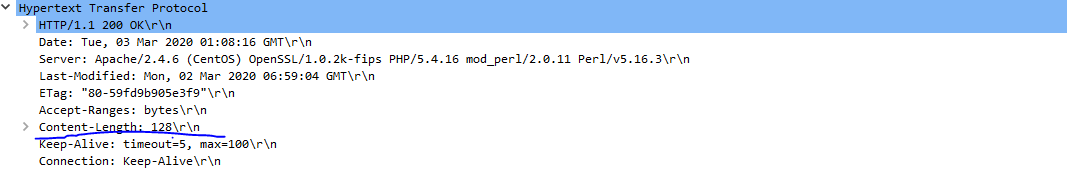
5. When was the HTML file that you are retrieving last modified at the server?

The HTML file that I was retrieving was last modified at the server on Tuesday, 03 March 2020 6:59 GMT.



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

128 bytes of content are being returned to my browser.

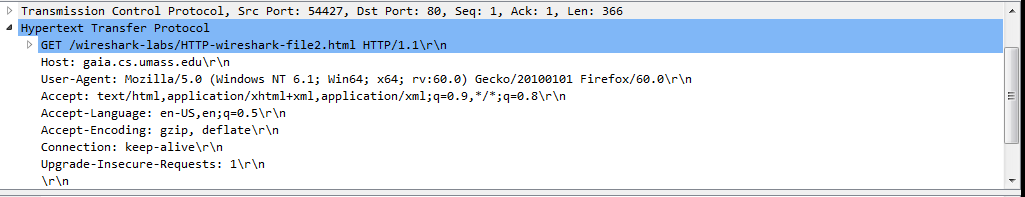


7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No I don’t see any.

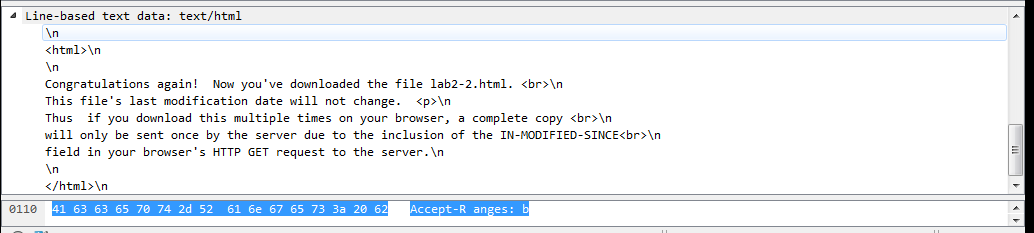
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

I do not see an IF-MODIFIED-SINCE line in the HTTP GET.



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

Yes the server explicitly return the contents of the file. I can tell because the content is shown in the section “Line-based test data: text/html.



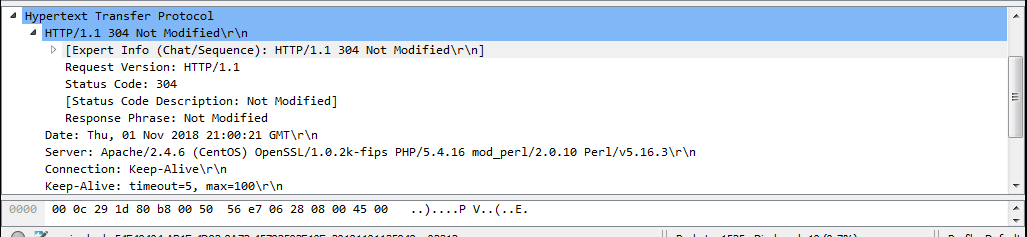
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

I do see an “IF-MODIFIED-SINCE:” line in the HTTP GET. The information that follows the the “IF-MODIFIED-SINCE:” header is Mon, 02 March 2020 6:59 GMT.



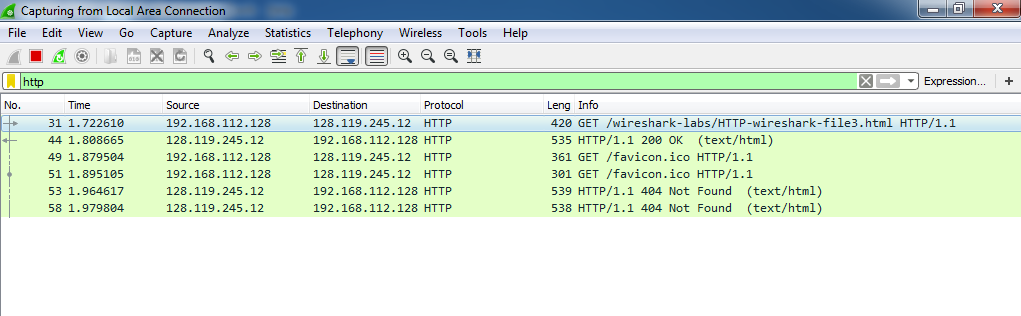
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

The HTTP status code and phrase returned from the server in response to this second HTTP GET is 304 and Not Modified. The server did not explicitly return the contents of the file because the second HTTP GET request sent by the browser included the “IF-MODIFIED-SINCE:” header (as the file has already been cached) and since the file on the server has not been modified since the time specified by the “IF-MODIFIED-SINCE:” header, the server simply responds that it has not been modified instead of returning the contents of the file again.



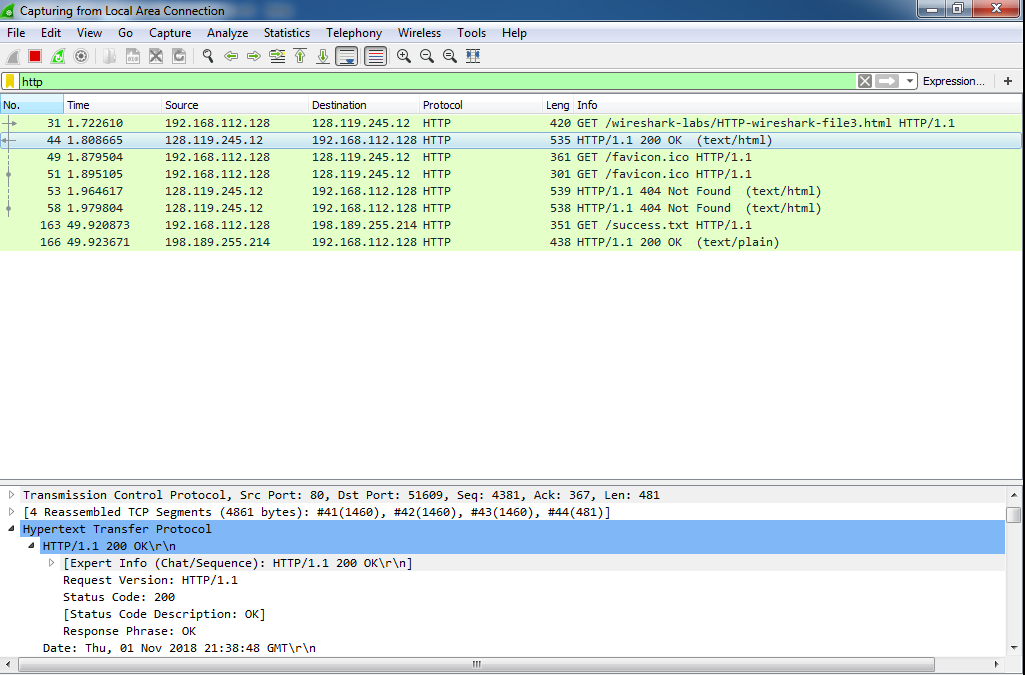
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

The HTTP GET request messages that my browser send was 1. The packet number in the trace that contains the GET message for the Bill or Rights is 31.



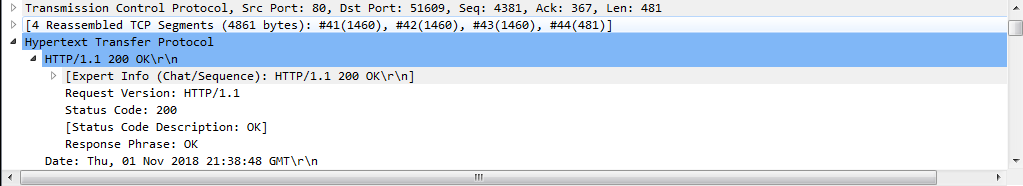
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? Answer: packet 10.

The packet number in the trace that contains the status code and phrase associated with the response to the HTTP GET request is 44



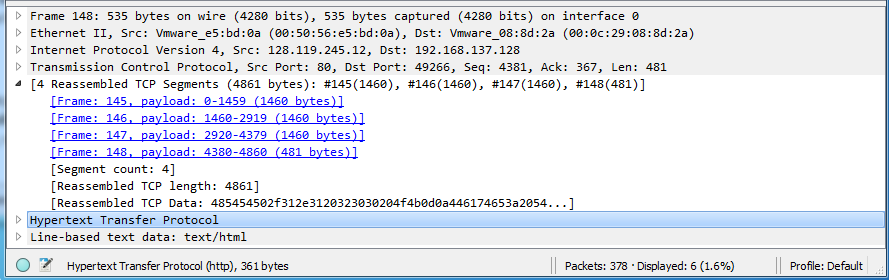
14. What is the status code and Phrase in the response?

The status code and phrase in the response is 200 and OK.



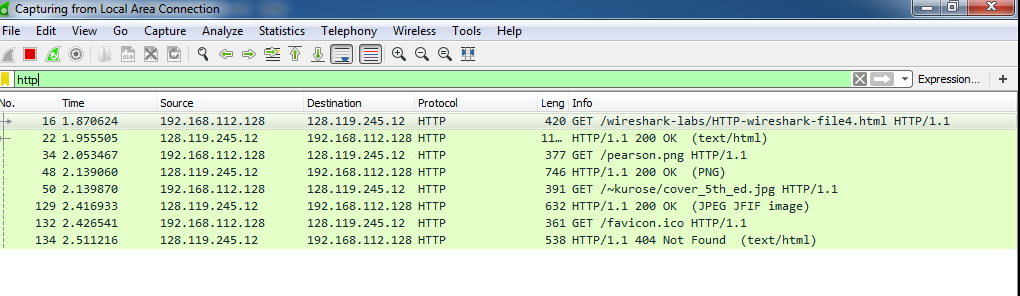
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Four data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.



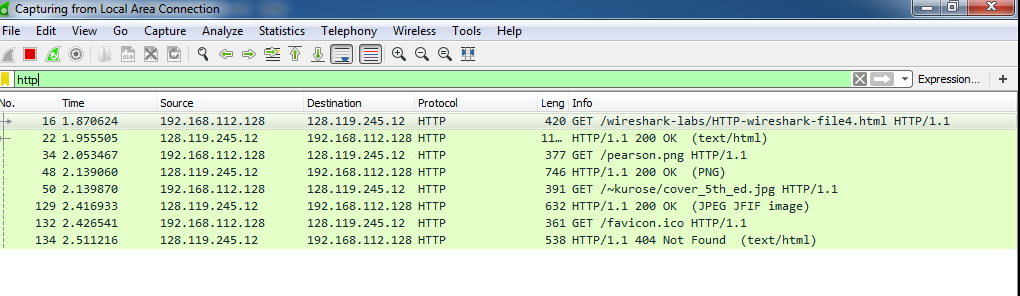
16. How many HTTP GET request messages did your browser send?

There are three HTTP GET request messages that my browser sent.



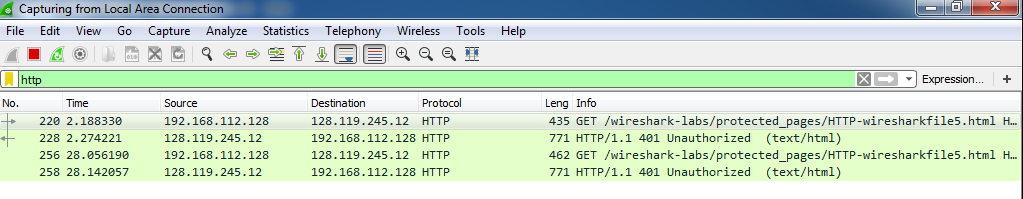
17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

The browser downloaded the two images serially. The times shown in the packet listing window indicates that the browser sent the HTTP GET request message for the second image after the HTTP response for the first image was received.



18. What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?

The server’s response in response to the initial HTTP GET message from your browser is 401 Unauthorized.



19. When your browser’s sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The new field that is included in the HTTP GET message is Authorization: Basic.

