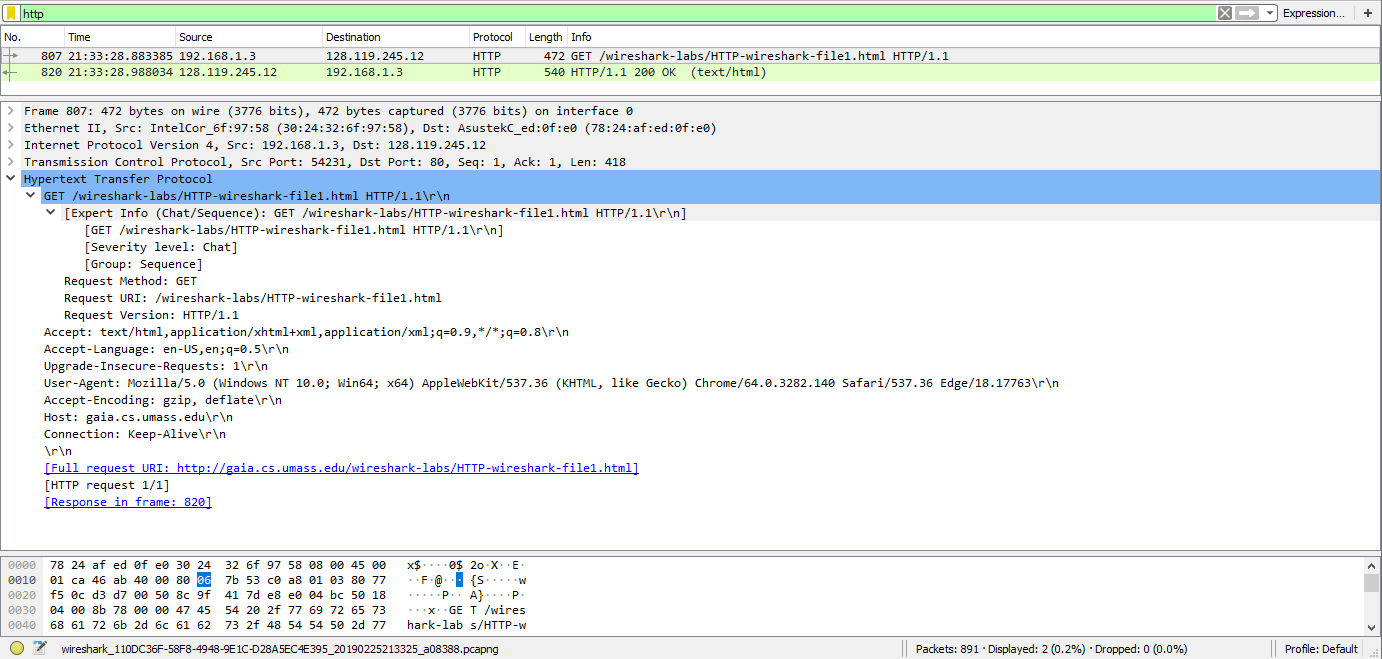
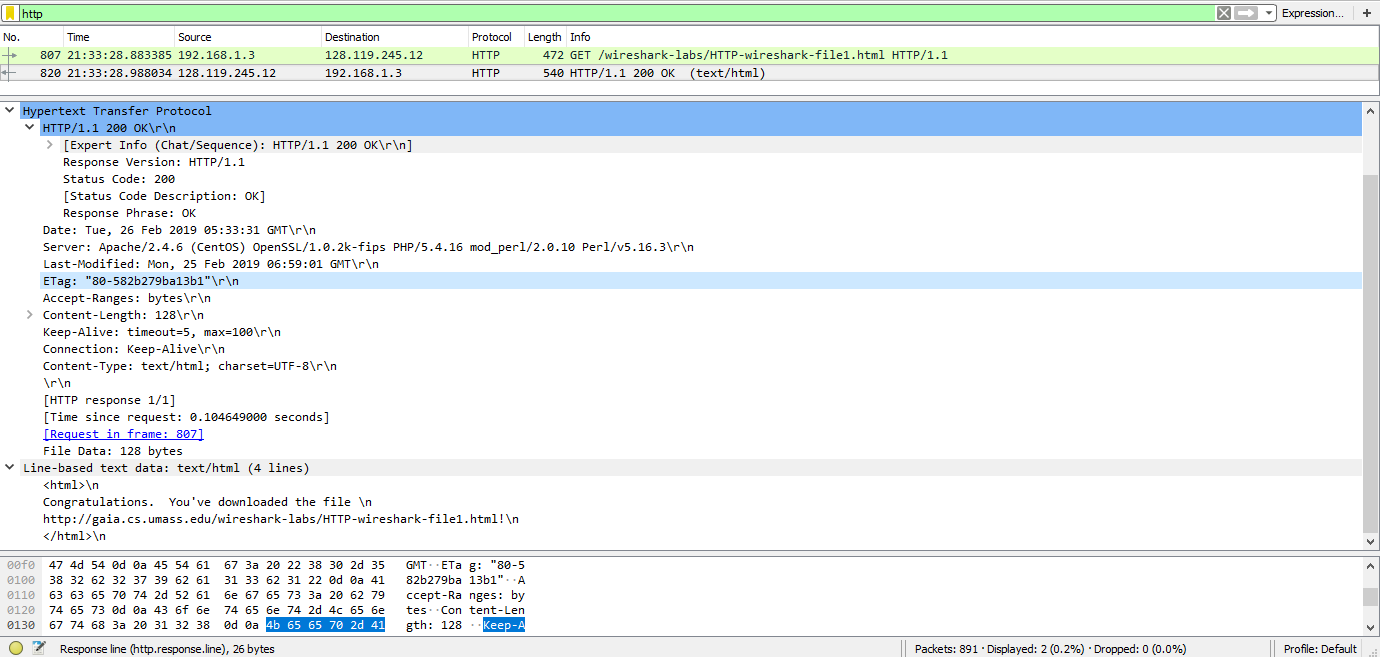
**Lab 2-Wireshark –HTTP**

**Goal:** To use Wireshark for the exploration of several important aspects in the HTTP protocol.

**Part 1: The Basic HTTP GET/response interaction**

These two snips are the GET and response.





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

My browser is runner HTTP Version 1.1 and the server is running the same version.

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



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



My PC IP address is the source and the server’s IP is the destination.

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



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



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

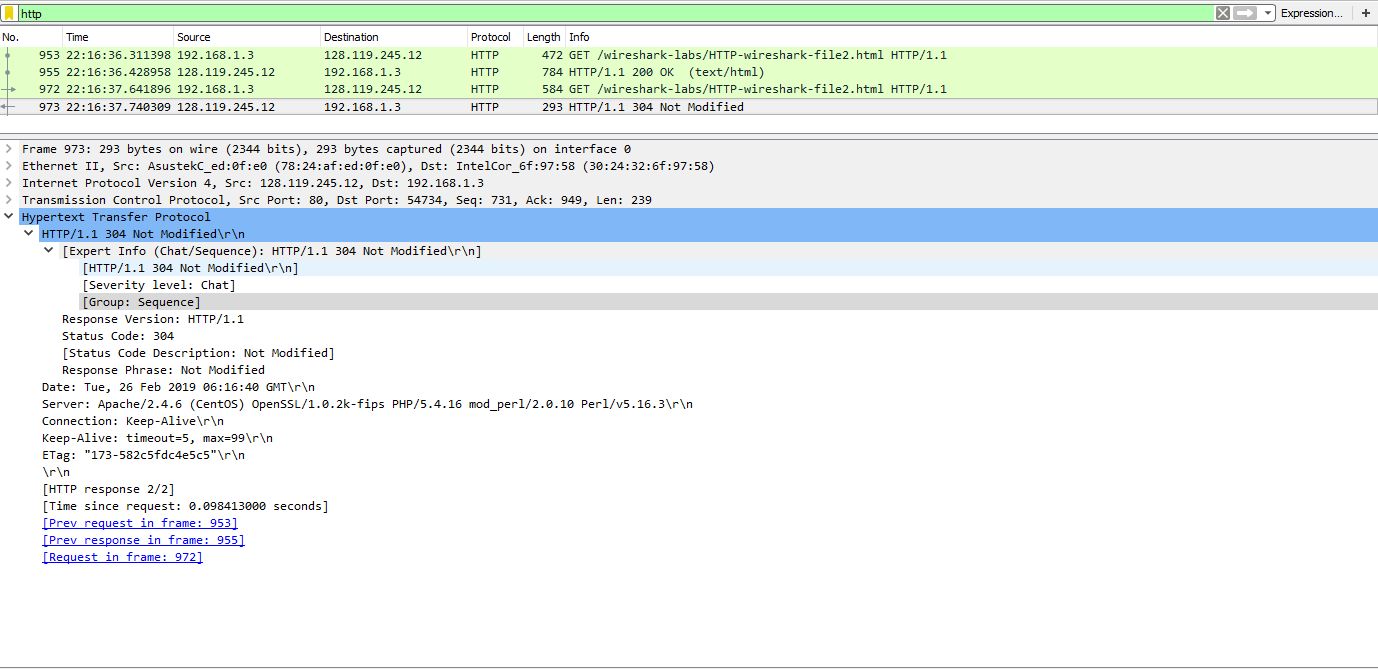


**7. By inspecting the raw data in the packet content window, do you see any headers**

**within the data that are not displayed in the packet-listing window? If so, name one.**

I don’t think I see any headers that aren’t displayed in the packet listing window.

**Part 2:** **The HTTP CONDITIONAL GET/response interaction**



**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?**

No.

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

Yes I think because there were no error messages or anything looking amiss.

**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?**

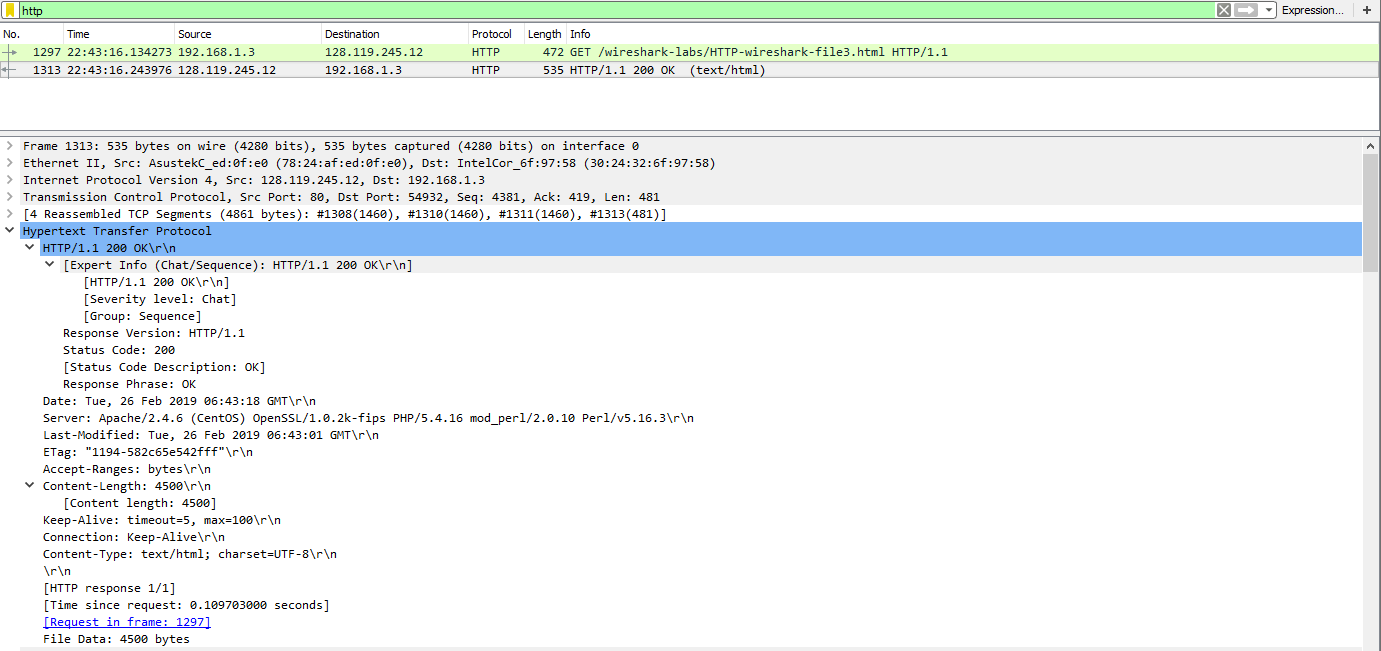
The “if-modified-since” did come up and the date and time is followed by it.

**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.**



Since the conditions looks similar to question 9, I would have to say yes again since nothing seemed wrong.

**Part 3: Retrieving Long Documents**



**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?**

It only sent 1 message with the first packet containing the GET message.

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

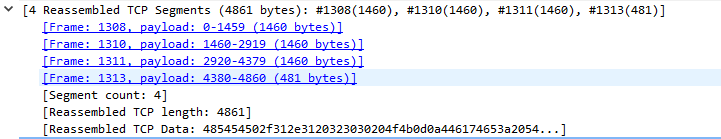
It is still the first packet.

**14. What is the status code and phrase in the response?**

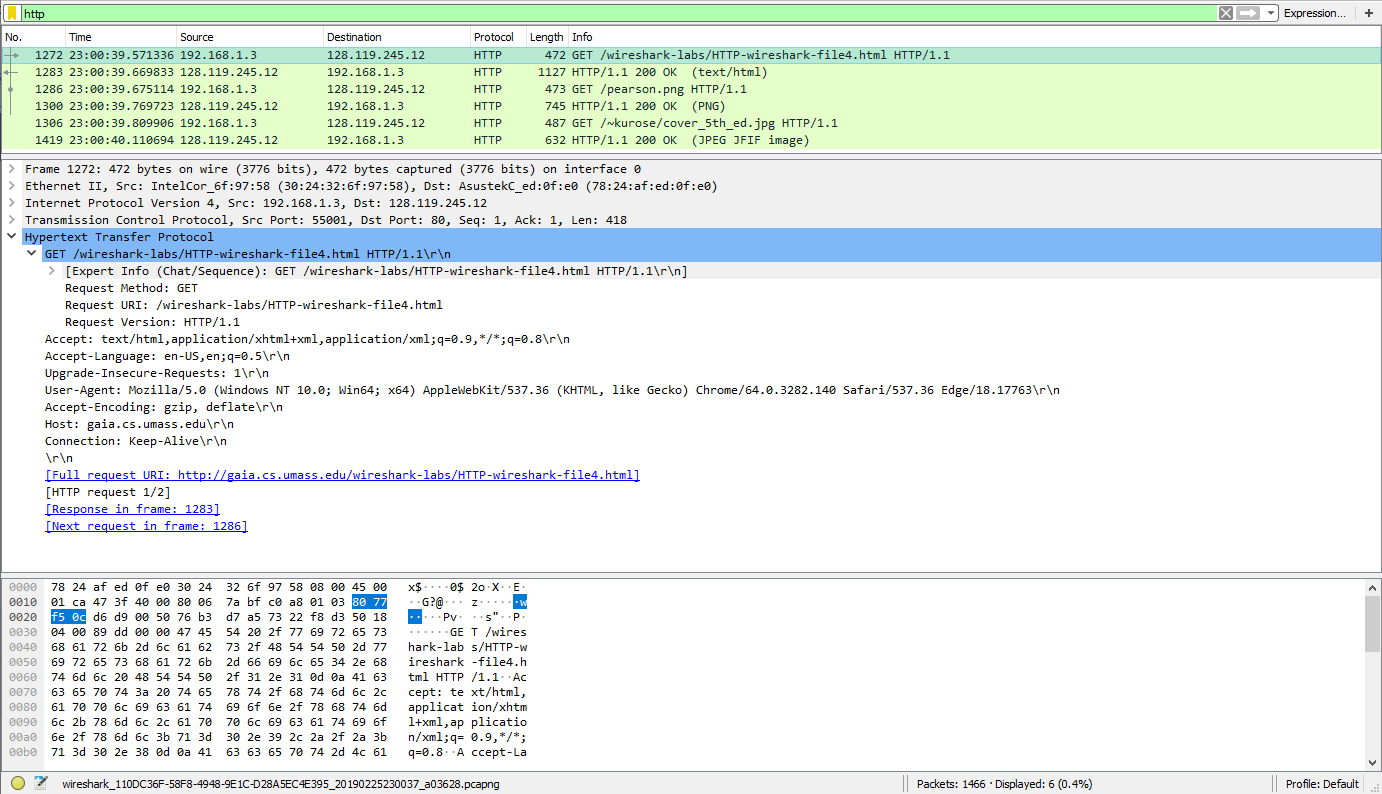


**15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?**

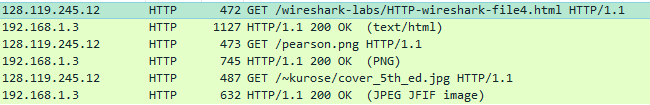
It took 4 TCP segments.



**Part 4. HTML Documents with Embedded Objects**



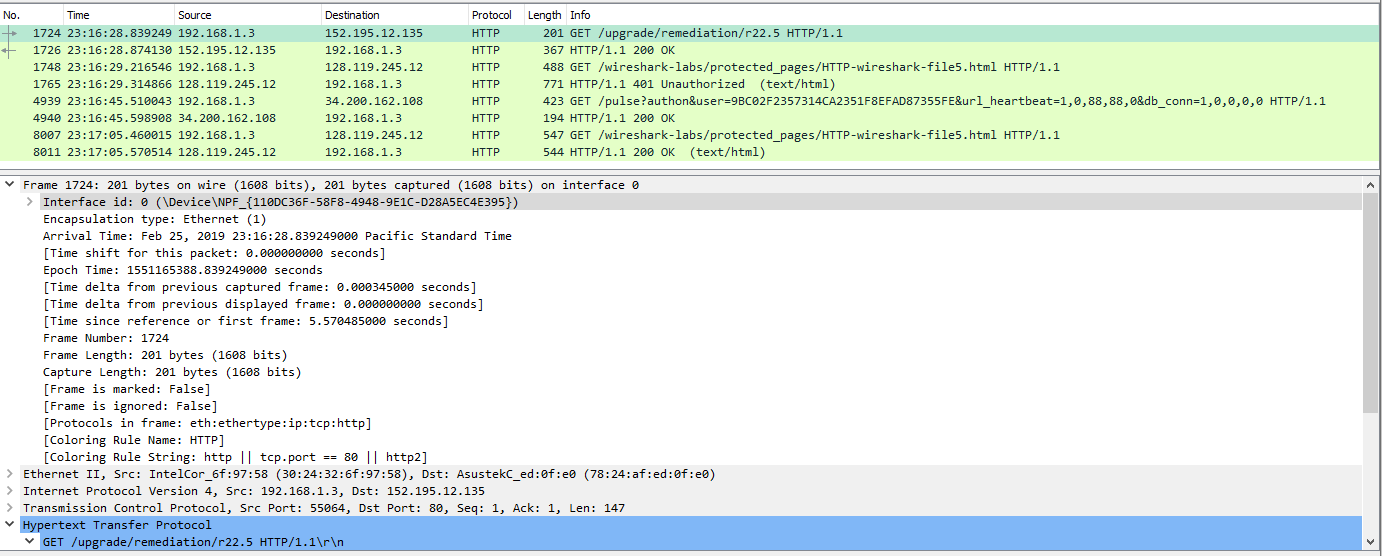
**16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?**

It sent 3 HTTP GET requests. They all have the same Internet address.

**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.**

From what I can see, it seems like it was done serially hence the multiple HTTP GET requests.

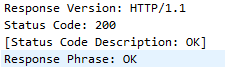
**Part 5: HTTP Authentication**



In the snip above, I am not too sure whether the first GET is a part of what I am suppose to get.

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

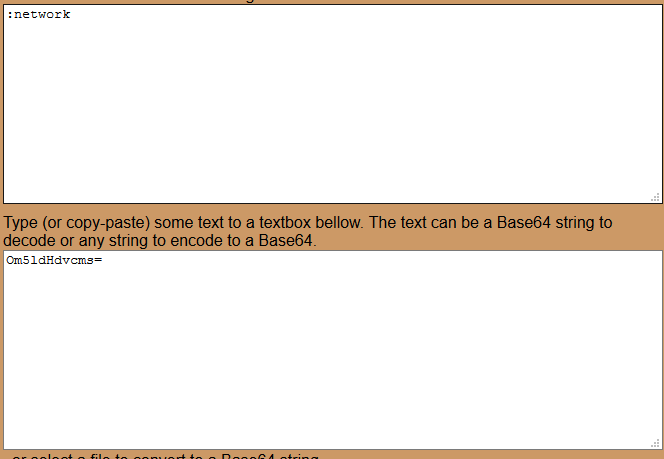
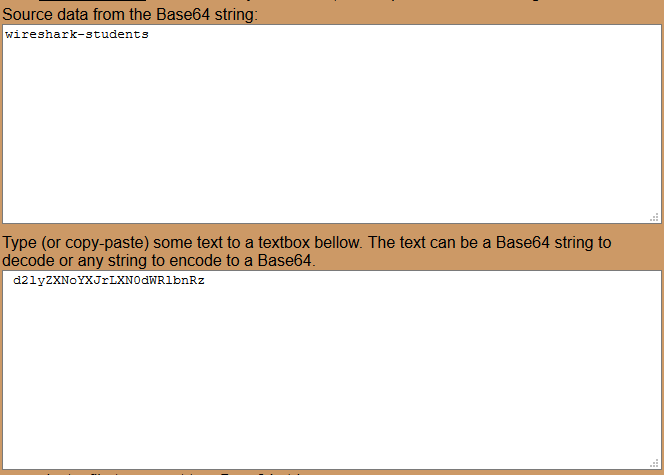
All the responses are the same.



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

It seems like it is the pop-up that prompts me to enter username and password and prevents me from seeing the content.

The password came up a little differently.



**Conclusion:**

In conclusion, it seems like there are still things that I don’t completely understand. This have been straightforward. One of the coolest things while at the same time concerning is being able to find out a person’s username and password information. Even though we get the username and password, we won’t know what it is as it just comes up as a mess of numbers and letters.