Práctica 5 Wireshark

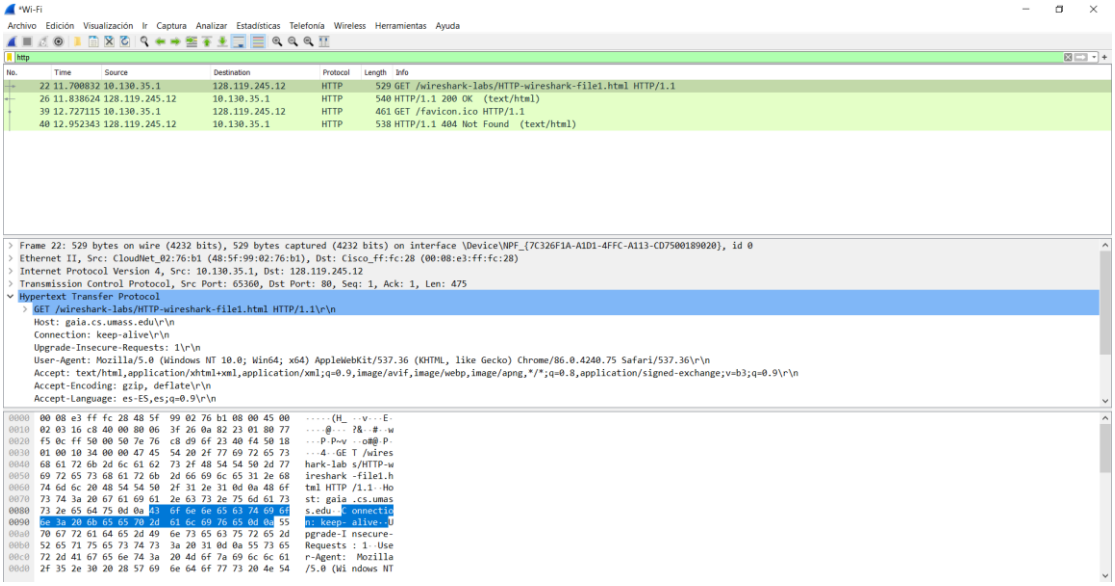
Guillermo Marcos García

The Basic HTTP GET/response interaction

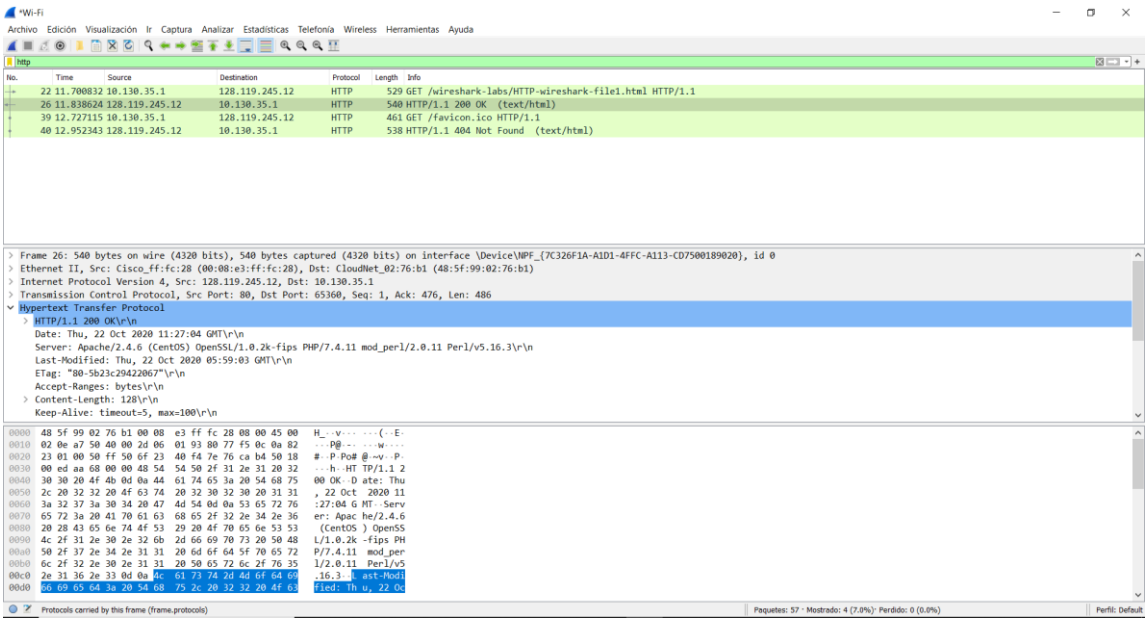
Questions

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 1.1

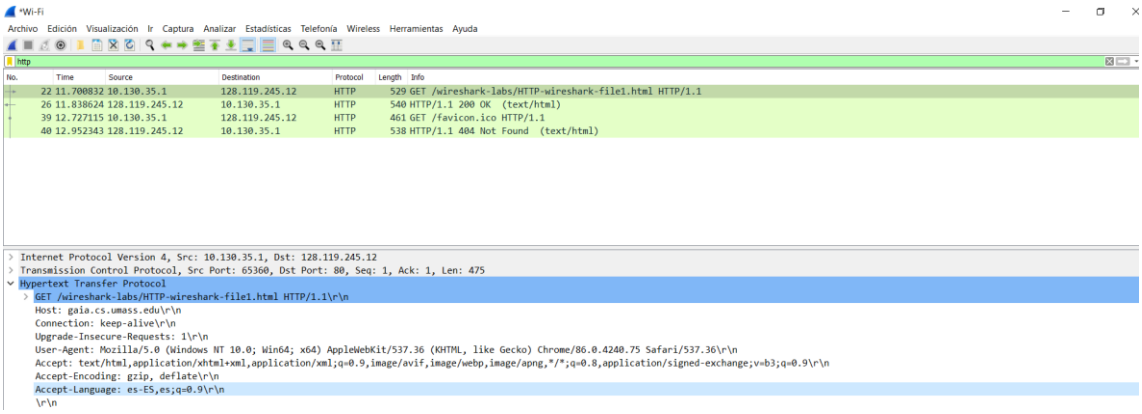


   The server also is running HTTP 1.1



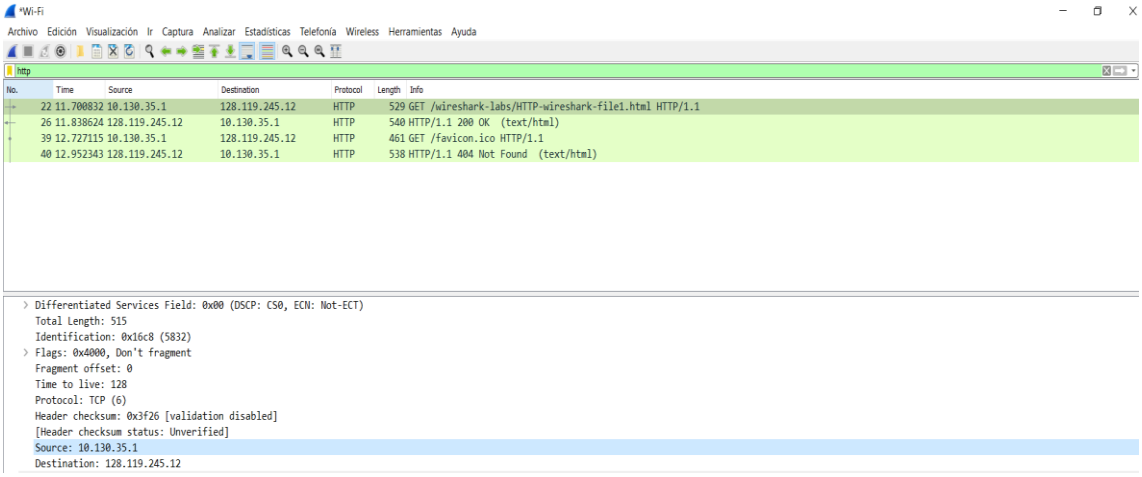
2. What languages (if any) does your browser indicate that it can accept to the server?

   The accepted language is es-Es

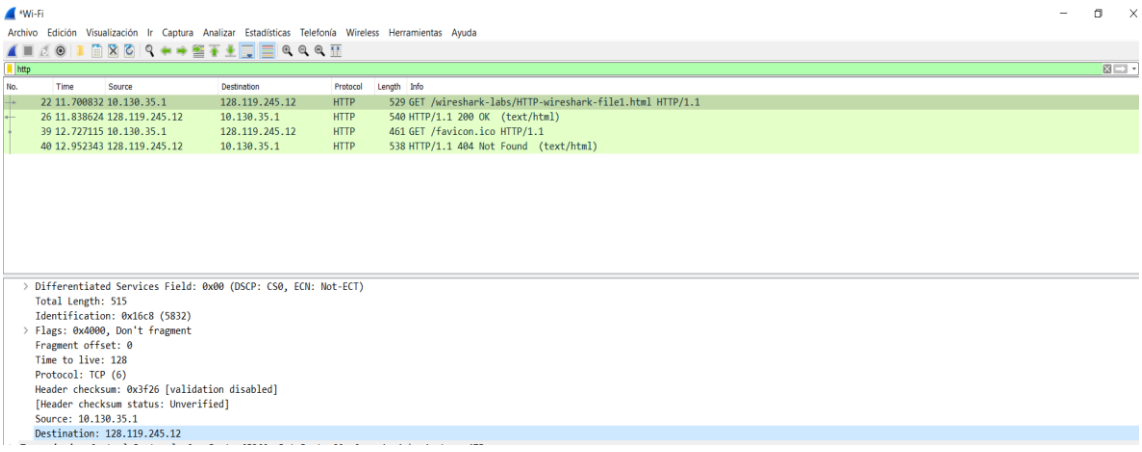


3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

   My IP address is 10.130.35.1

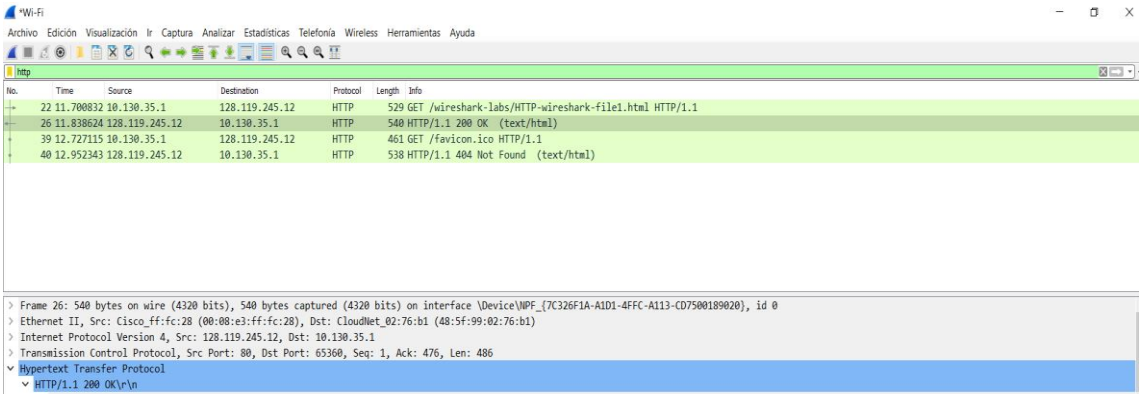


   The IP address of the server is 128.119.245.12



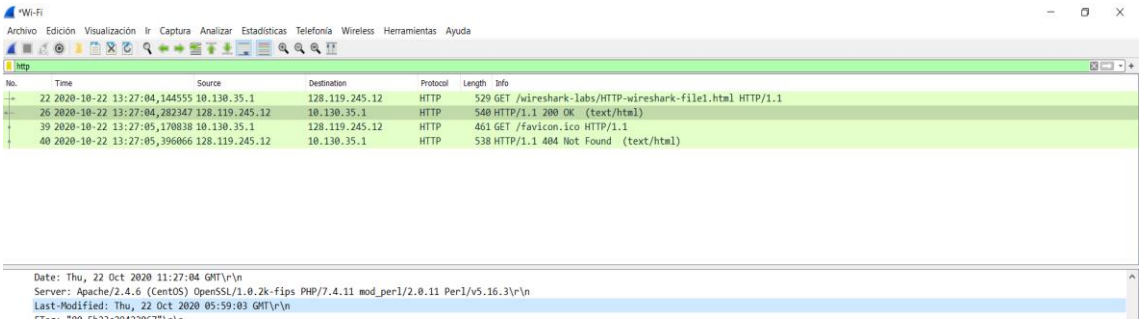
4. What is the status code returned from the server to your browser?

The status code returned is 200



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

The last time that the file was modified was Thursday 22 2020 at 05:59:03



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

The size of the file is 128 bytes.

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 it is the same content so I see the same in both sites.

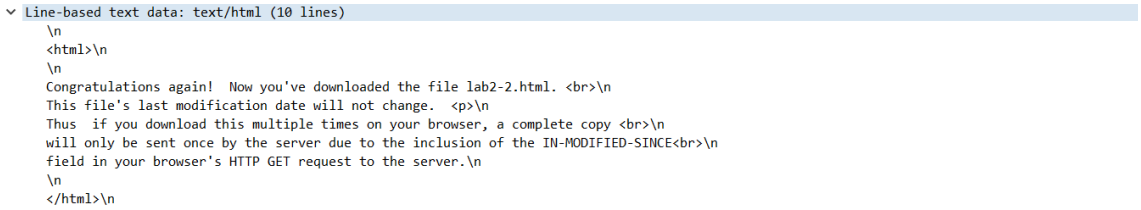
The HTTP CONDITIONAL GET/response interaction

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, it doesn´t appear.

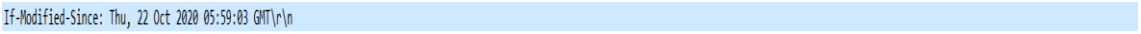
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

   Yes, the server returns the content of the file



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?

    Yes, now I can see 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.

    The status code is 304, it means that the file has not been modified . In this case we can’t see the content of the file because the server doesn´t send the file.

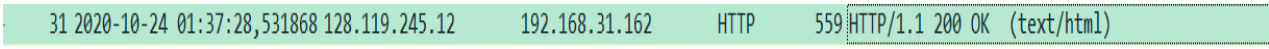
Retrieving Long Documents

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 sends one HTTP GET request message. The packet number 23

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

The packet number 31



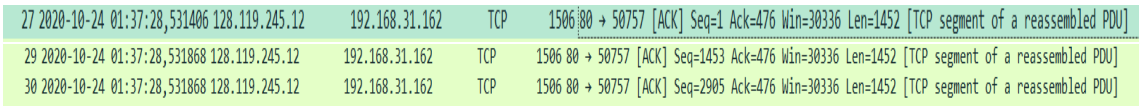
14. What is the status code and phrase in the response?

The status code is 200 and the phrase “OK”

```
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
```

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

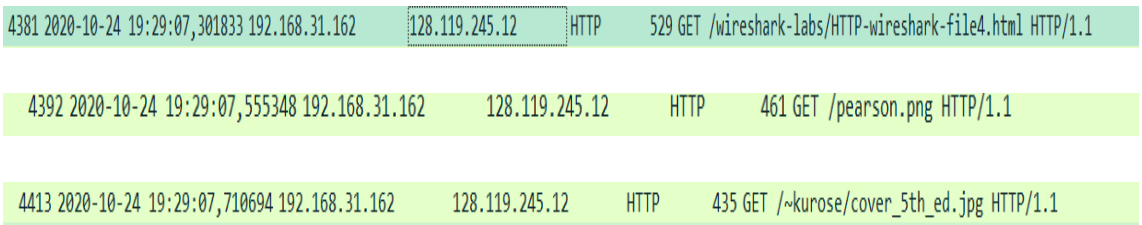
Three TCP packets, the number 27,29 and 30.



HTML Documents with Embedded Objects

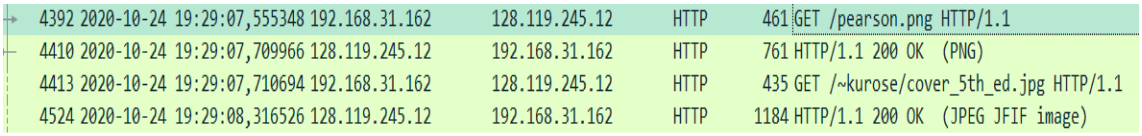
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

My browser send three GET requests to 128.119.245.12 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.

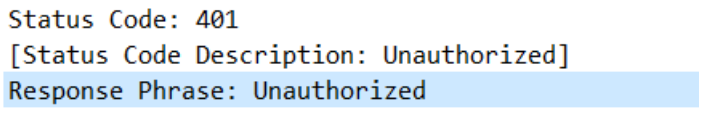
Serially



HTTP Authentication

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

In the response status code is 401 and the phrase "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?

It includes authorization to access the webpage.