Baptiste Saliba

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. I found it in the line:  
`GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n`

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

My browser accepts the English language (US version). I found this info in the line:

`Accept-Language: en-US,en;q=0.9,fr;q=0.8\r\n`

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

My computer’s IP address is 128.226.30.148 and gaia.cs.umass.edu is 128.119.245.12. This was found in the lines:

`Source: 128.226.30.148`

`Destination: 128.119.245.12`

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

The return code can be found in response frame which is linked at the end of the GET message:  
`http.response\_in: 9708`  
In that response we can find the status code:  
`Status Code: 200`

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

This information can also be found in the response body:

`Last-Modified: Tue, 11 Feb 2020 06:59:01 GMT\r\n`

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

The returned content length is 128 bytes. This can be found in the response body in line:

`Content-Length: 128\r\n`

**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 wasn’t able to find any headers that weren’t in the packet-listing window.

**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 did not. It doesn’t have the “IF-MODIFIED-SINCE” header.

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

Yes, in the section:

`Line-based text data: text/html (10 lines)`

You can see the response body.

**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, the line is:

`If-Modified-Since: Tue, 11 Feb 2020 06:59:01 GMT\r\n`

The time listed in this line is the time at which this webpage was last cached.

**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 response code was   
`HTTP/1.1 304 Not Modified\r\n`

This means that the cached copy has not been modified since the last request, meaning that the cached copy can be used and doesn’t require a new copy with the info in the response body.

**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 browser only sent one GET request message. The packet number of the GET message was 435.  
Frame 435: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface en0, id 0

**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 that contains the status code is 441.

4 Reassembled TCP Segments (4861 bytes): #437(1448), #438(1448), #439(1448), #441(517)

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

`HTTP/1.1 200 OK\r\n`

**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 segments to carry the single http request.

`4 Reassembled TCP Segments (4861 bytes): #437(1448), #438(1448), #439(1448), #441(517)`

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

The browser made 3 requests:

1. `Requested URI: /wireshark-labs/HTTP-wireshark-file4.html`
2. `Requested URI: /pearson.png`
3. `Requested URI: /~kurose/cover\_5th\_ed.jpg`

**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 images were downloaded serially. You can tell because the GET request for /~kurose/cover\_5th\_ed.jpg was only sent after the GET and response for /pearson.png had already been sent and received respectively.

/pearson.png GET -> `[Time since reference or first frame: 5.051203000 seconds]`

/pearson.png response -> `[Time since reference or first frame: 5.072161000 seconds]`

/~kurose/cover\_5th\_ed.jpg GET -> `[Time since reference or first frame: 5.085501000 seconds]`

/~kurose/cover\_5th\_ed.jpg response -> `[Time since reference or first frame: 5.373579000 seconds]`

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

`HTTP/1.1 401 Unauthorized\r\n

Status Code: 401`

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

These two new fields are sent:

`Cache-Control: max-age=0\r\n`

`Authorization: Basic YnNhbGliYTE6c29jY2VyMTY=\r\n`