CS315: Lab Assignment 3

B Siddharth Prabhu

200010003@iitdh.ac.in

17 January 2023

1 Answers for Task 1: The Basic HTTP GET/response interaction

The following screenshot depicts the observed output records. Below it, some questions regarding the same are answered.

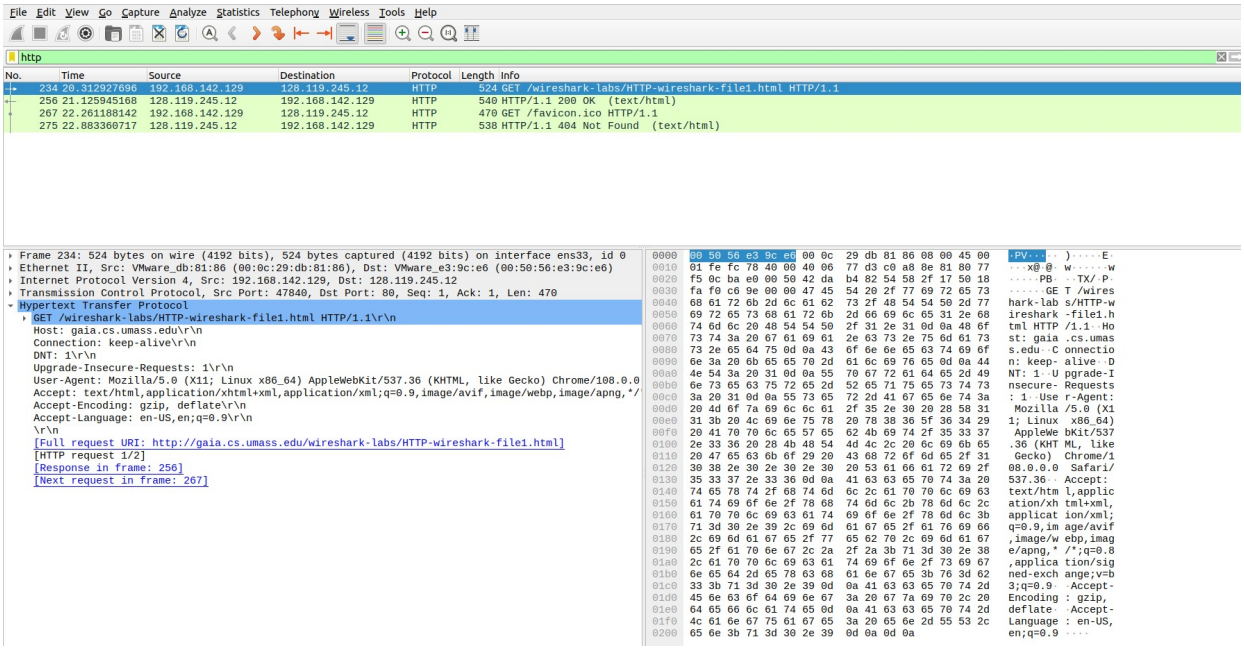

Figure 1: Screenshot of records obtained

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

- The browser is running HTTP version 1.1. This is observable in the record with ID 234.
- The server is running HTTP version 1.1. This is observable in the record with ID 256.

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

In the screenshot, within the description of HTTP, we find the accepted languages in the `Accept-Language` attribute. It is **en-US**, which is American English. This could be due to browser settings.

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

- The IP address of my computer (the VM) is **192.168.142.129**. The reason for this is that I'm running the browser (and Wireshark) on an Ubuntu VM with Network settings set to NAT (Network Address Translation). IP addresses beginning with 192.168 are for private networks, and in this case the private network is formed by the VM and the host system, via a network adapter. Hence, to communicate with the internet, this would take 1 hop more, than if this was run on the host.
- The IP address of the gaia.cs.umass.edu server is **128.119.245.12**.

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

As observed in the below screenshot, the status code returned from the server to the browser is **200** (which means status OK). This can be found in the header part of the HTTP Response packet.

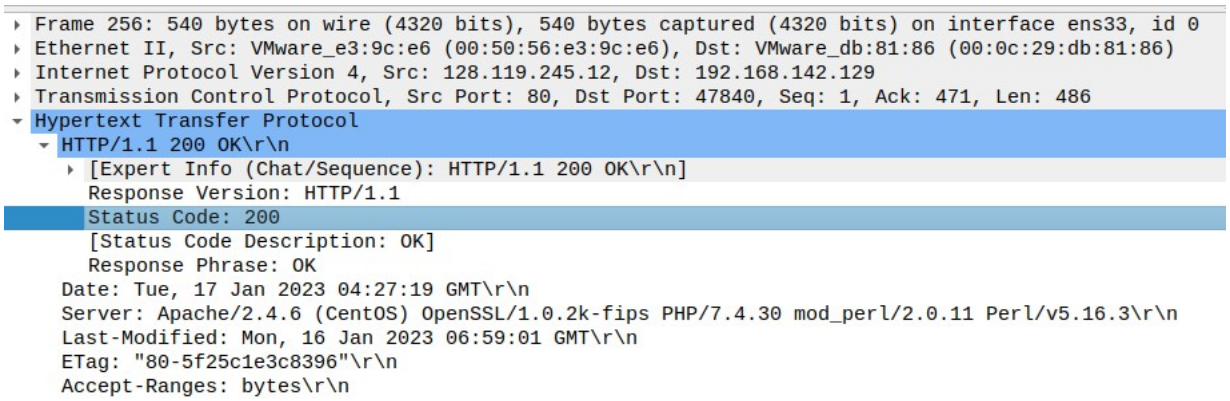

Figure 2: Screenshot of status code in response

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

As visible in the above figure, the `Last-Modified` field reads: **Mon, 16 Jan 2023 06:59:01 GMT**. This is possible due to the packet being modified along the way. Sometimes, the Last-Modified field comes to be a date in 2016, and this may occur if the file is not modified at all along the way.

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

As observed in the below screenshot, **128 bytes** of content are being returned to the browser.

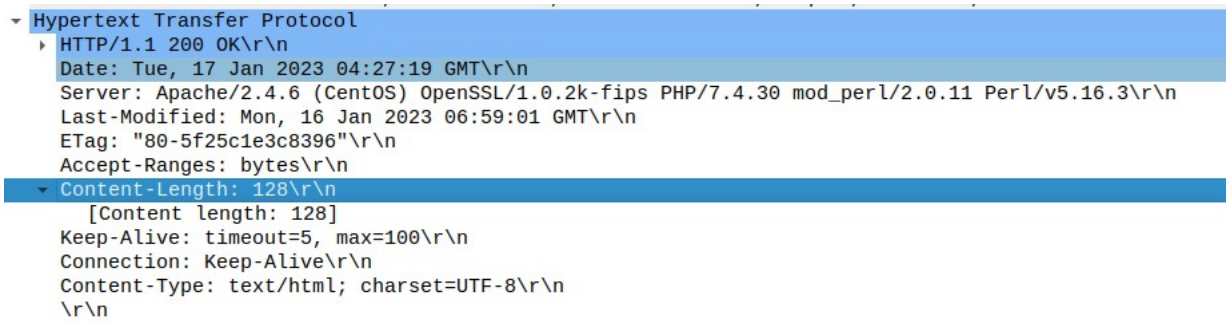

Figure 3: Screenshot of content bytes in response

(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. The raw data seems to exactly match up with what is shown in the packet-listing window.

2 Answers for Task 2: The HTTP CONDITIONAL GET/response interaction

The following screenshot depicts the observed output records on loading and refreshing the page. Below it, some questions regarding the same are answered.

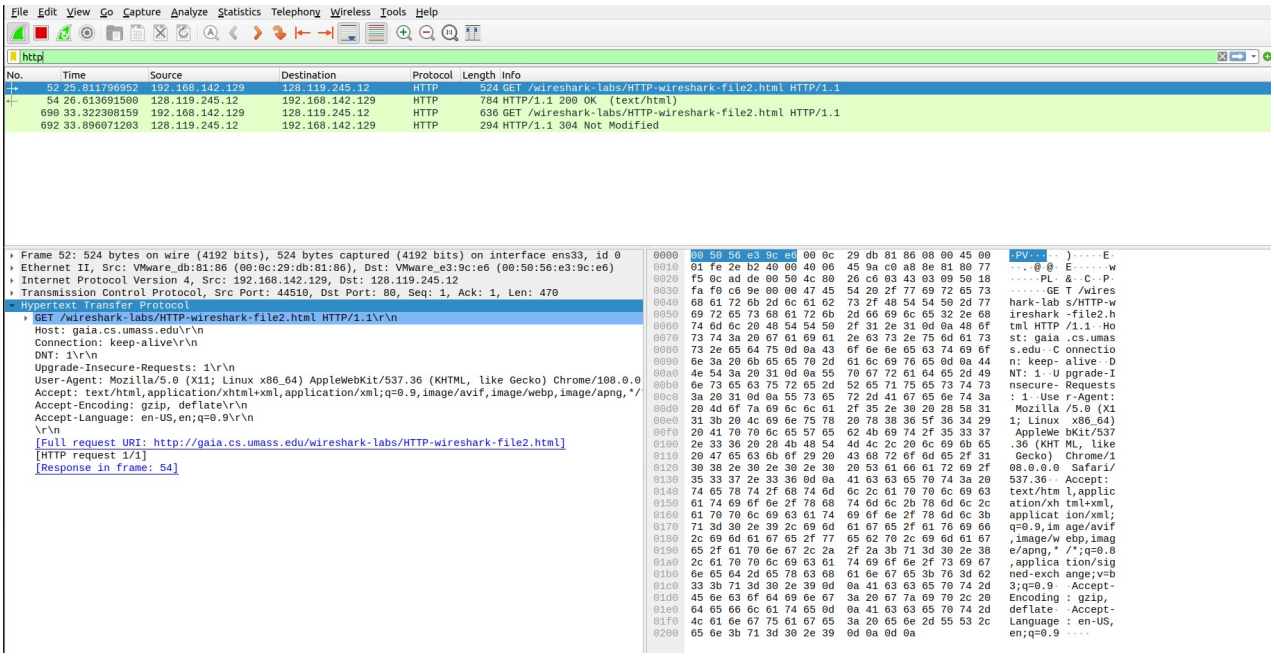

Figure 4: Screenshot of records obtained

(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?

No. `IF-MODIFIED-SINCE:` line is not present in the contents of the first HTTP GET request from the browser to the server, as seen in the below screenshot.

Figure 5: Lack of IF-MODIFIED-SINCE field

(2) 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 returned the contents of the file. We observe the section titled "Line-Based Text Data", which shows what the server sent back to the browser (which is exactly what the website displays). The contents of this section are shown in the below screenshot.

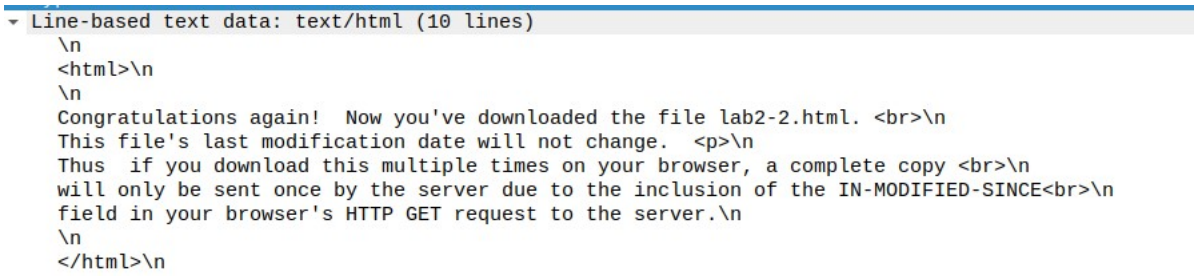

Figure 6: Contents returned by server

(3) 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. `IF-MODIFIED-SINCE:` line is present in the contents of the second HTTP GET request from the browser to the server, as seen in the below screenshot. It is followed by the time when the page was last accessed/modified by the browser.

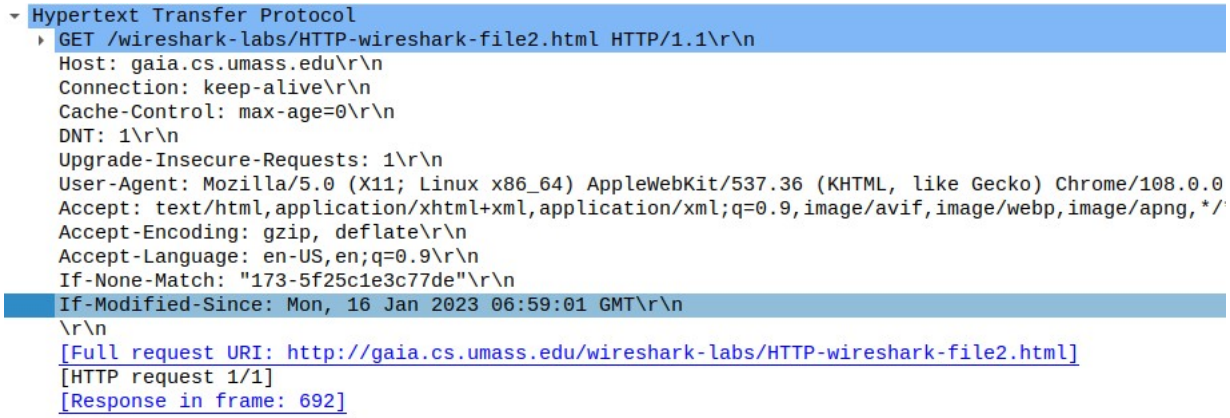

Figure 7: Presence of IF-MODIFIED-SINCE field

(4) 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 the second HTTP GET are **304** and **Not Modified** respectively. The same can be observed in the screenshot present at the top of the next page.
- Also, there is no section titled "Line-Based Text Data" here, so the server **doesn't explicitly return** the file contents in this case.

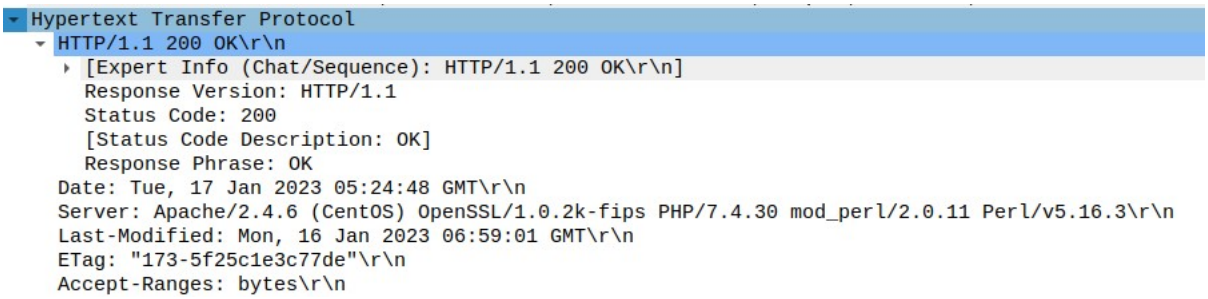

Figure 8: Status Code and Phrase from second HTTP GET

3 Answers for Task 3: Retrieving Long Documents

The following screenshot depicts the observed output records on retrieving a long document. Below it, some questions regarding the same are answered.

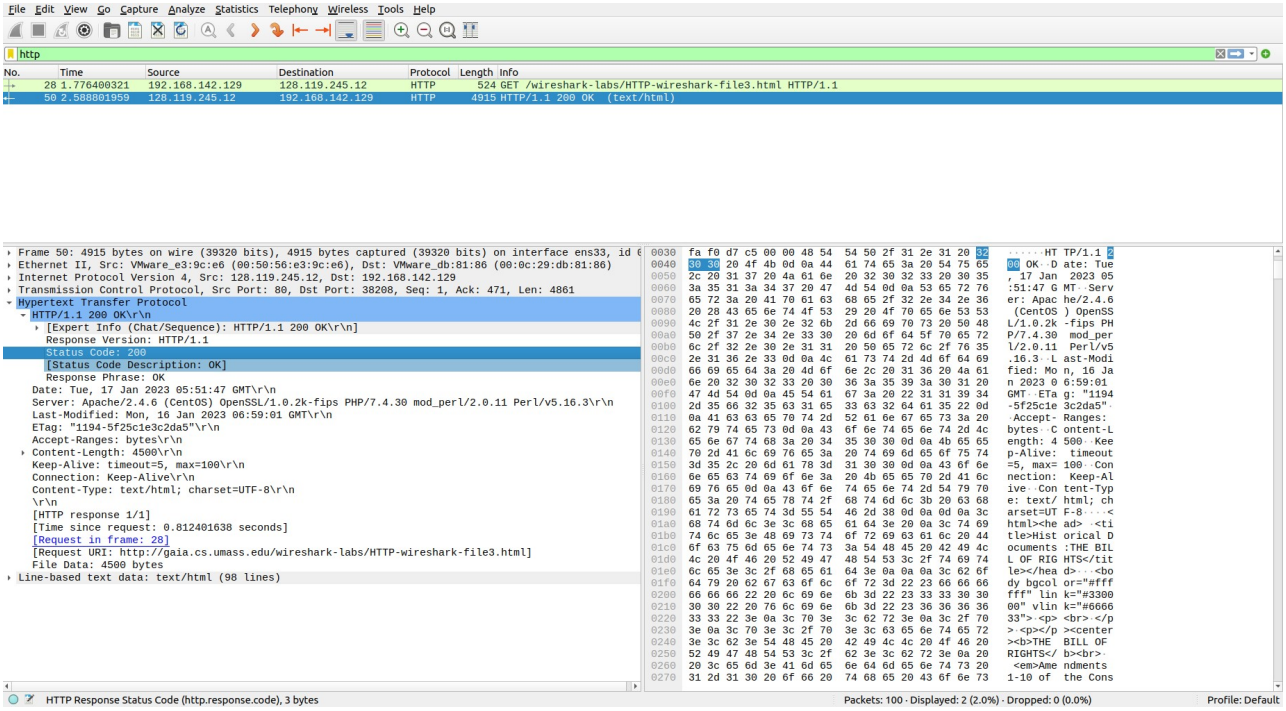

Figure 9: Screenshot of records obtained

(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?

- The browser sent **ONE** HTTP GET request message, as visible in the above screenshot.
- The packet number **28** in the trace contains the GET message for the Bill of Rights.

(2) Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

The packet number **50** in the trace contains the status code and phrase associated with the response to the HTTP GET request

(3) What is the status code and phrase in the response?

As visible in the second image on the previous page, the HTTP status code and phrase in the response are **200** and **OK** respectively.

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

As visible in the below screenshot, there are 2 TCP segments needed to carry the single HTTP response. The number of such segments seems to vary in each packet capturing (even after clearing cache). This would be based on congestion of the network.

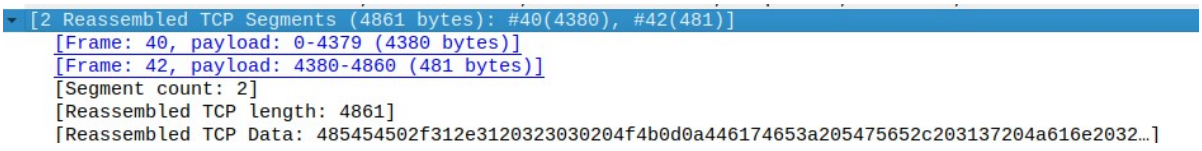

Figure 10: Screenshot of TCP segments

4 Answers for Task 4: HTML Documents with Embedded Objects

The following screenshot depicts the observed output records on retrieving HTML documents with embedded objects. Below it, some questions regarding the same are answered.

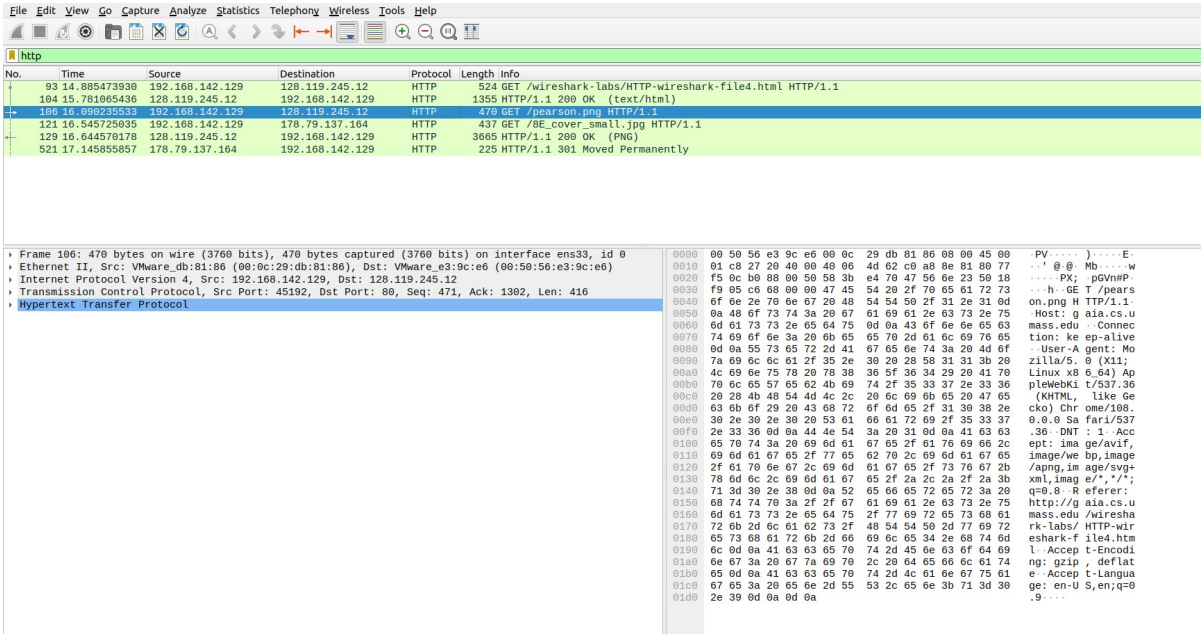

Figure 11: Screenshot of records obtained

(1) How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

In total, the browser sent **THREE** HTTP GET request messages. The first two GET requests were sent to IP address `128.119.245.12` , while the third one was sent to IP `178.79.137.164` . This is shown in the above screenshot.

(2) Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

It can be concluded that the browser downloaded the two images parallely. Here, both files have been requested, and then have returned in the same time period. Since the second image's GET request doesn't wait for the response of the first image to return, we could come to the conclusion that it is **parallel**. Had it been serial, the second image's GET request would have been sent after the arrival of the response of the first image. Evidence for all this is visible in the second image on the previous page.

5 Answers for Task 5: HTTP Authentication

The following screenshot depicts the observed output records on accessing a page that requires authentication. Below it, some questions regarding the same are answered.

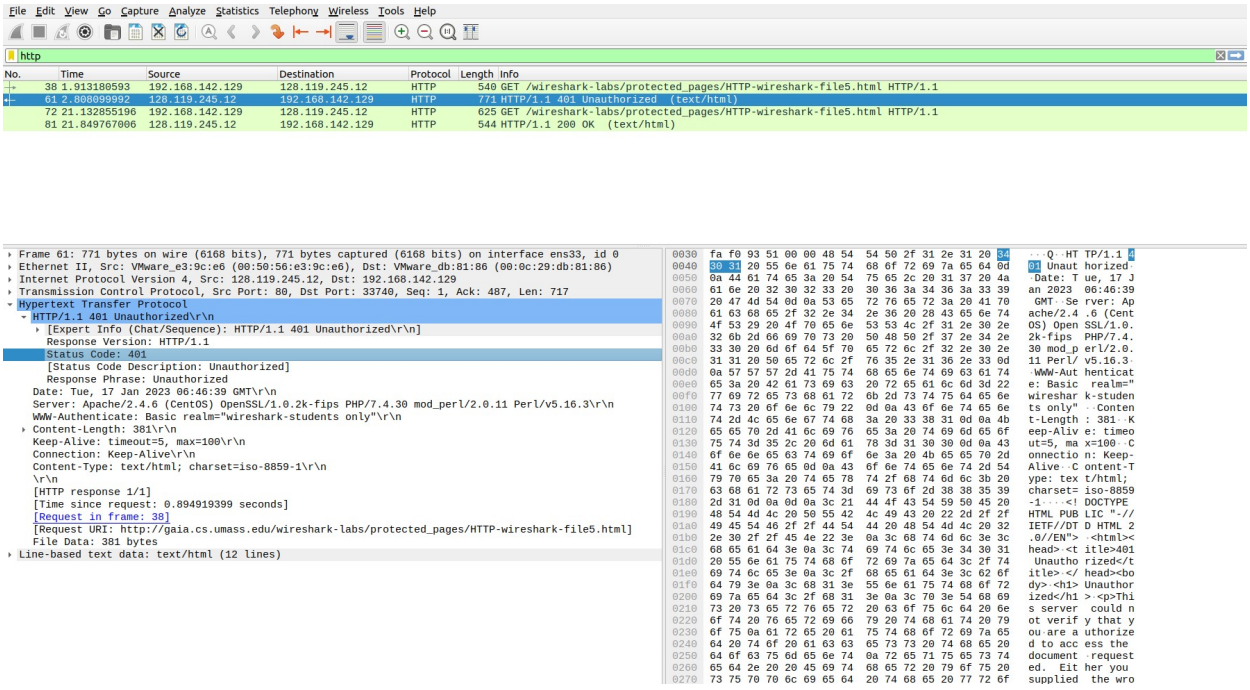

Figure 12: Screenshot of records obtained

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

As visible in the above screenshot, the HTTP status code and phrase returned from the server in response to the second HTTP GET are **401** and **Unauthorized** respectively.

(2) When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

As visible in the screenshot on the next page, a new field called "Authorization" is included when the browser sends the second HTTP GET message.

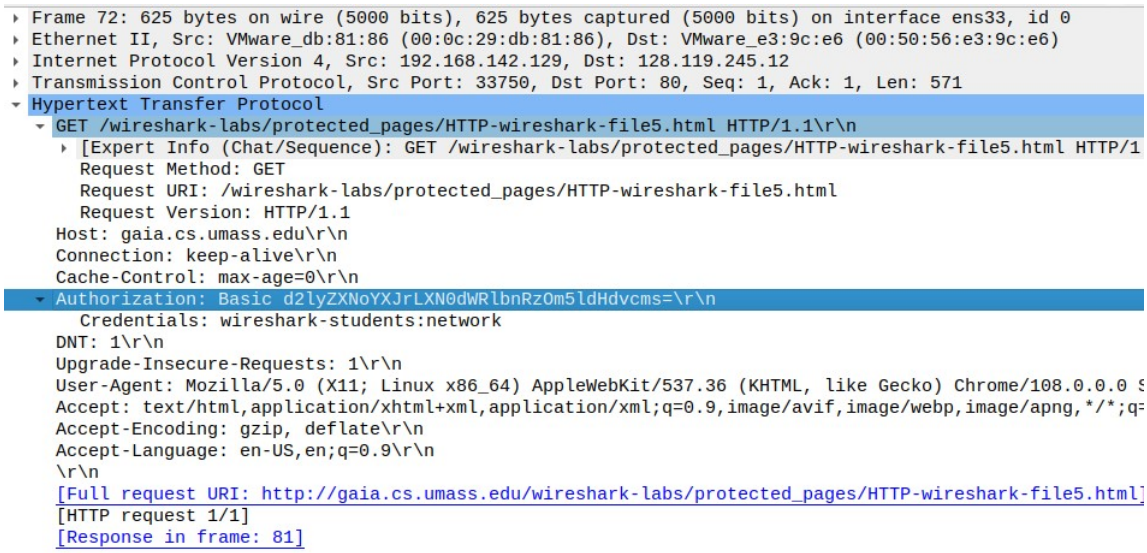

Figure 13: Presence of Authentication field