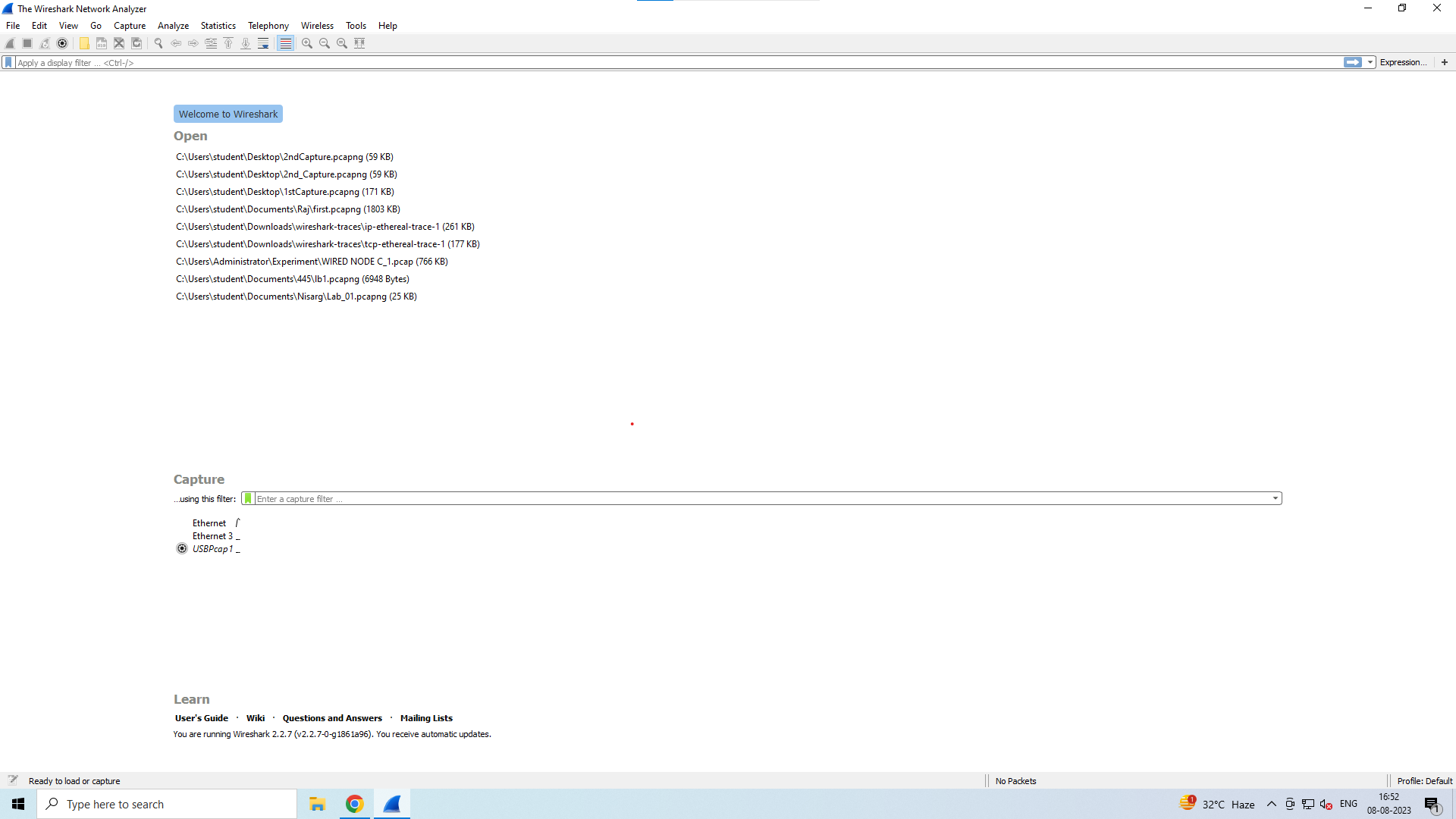
|  |  |
| --- | --- |
|  | LAB 1: Introduction to wireshark and analyzing HTTP. |
|  |  |
|  | Akshar Panchani ID- 202101522  IT304 Computer Networks  8/8/23 |



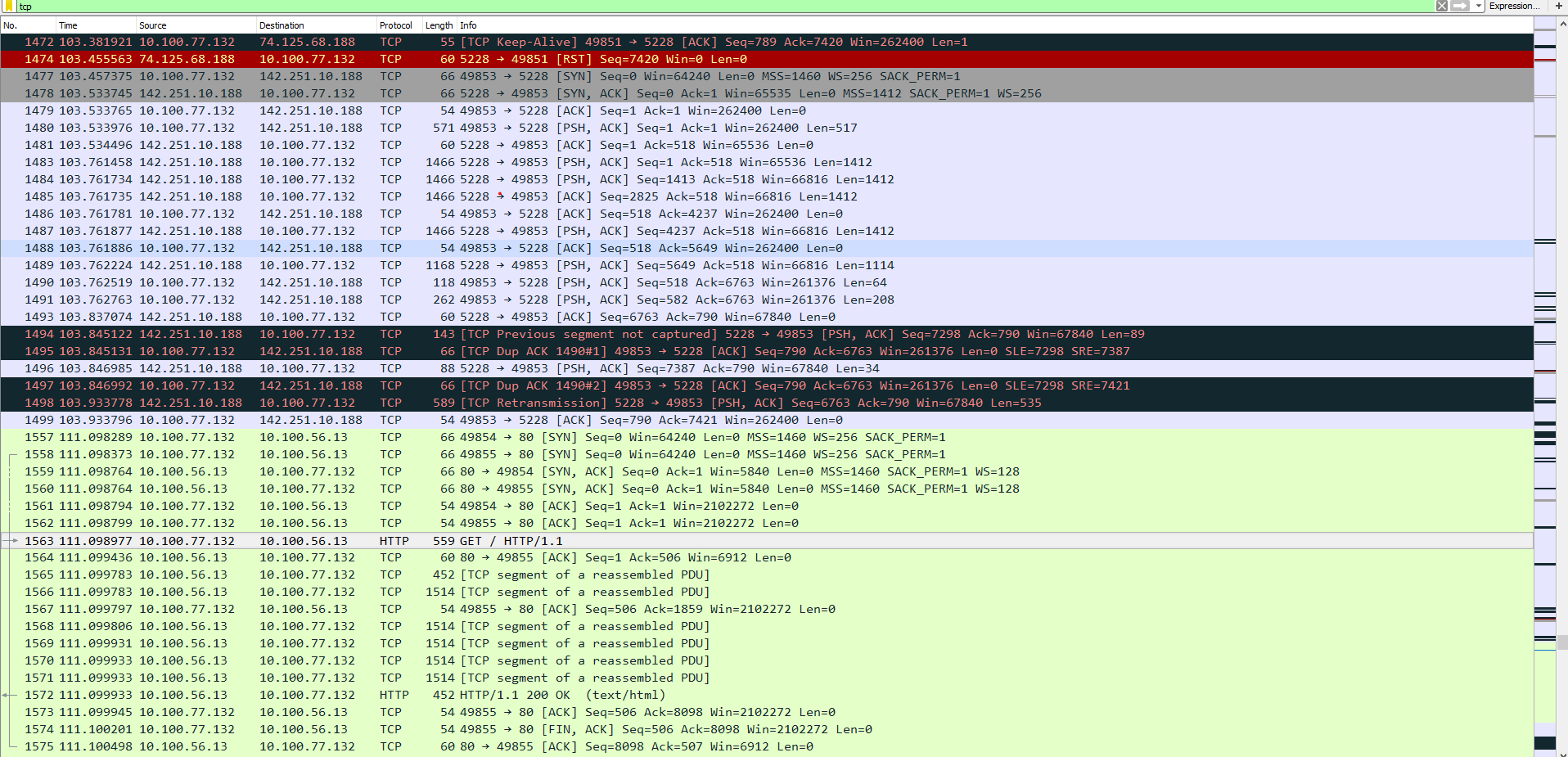
**Exercise:**

**2.9:**

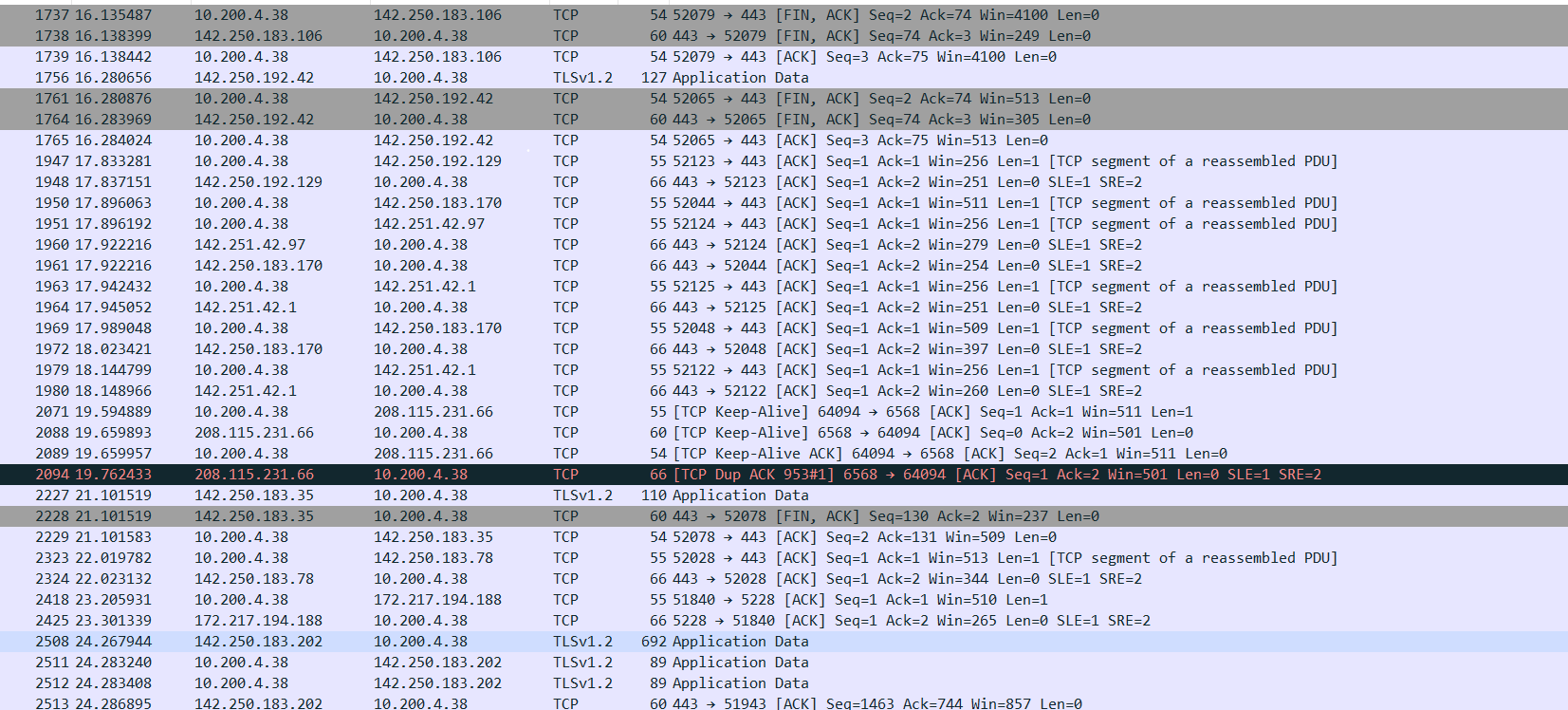
1. what are the interfaces shown on your default screen?



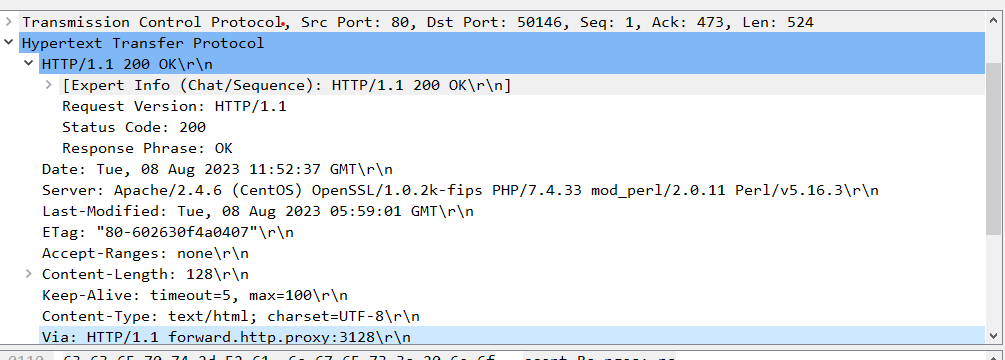
2. Begin packet capturing by selecting an interface that is being used to send and receive packets. AND 3. Filter out all the TCP packets and capture the screen.



4. Filter out all the TCP data packets which has packet length more than 30 bytes.



**4.2:**



From the above screenshot we extract this answers.

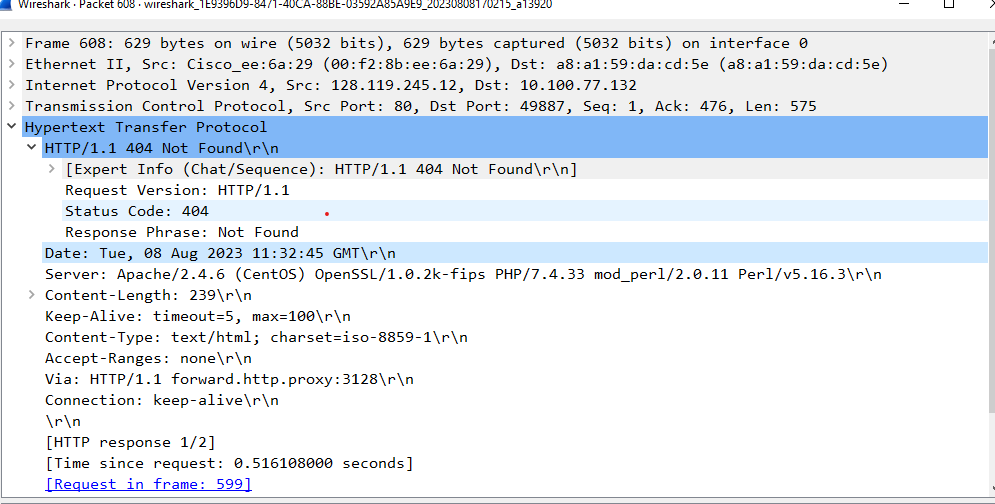
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

HTTP Version 1.1 is the version for both server and browser.

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

Language shown is :- en-US, en q=0.9

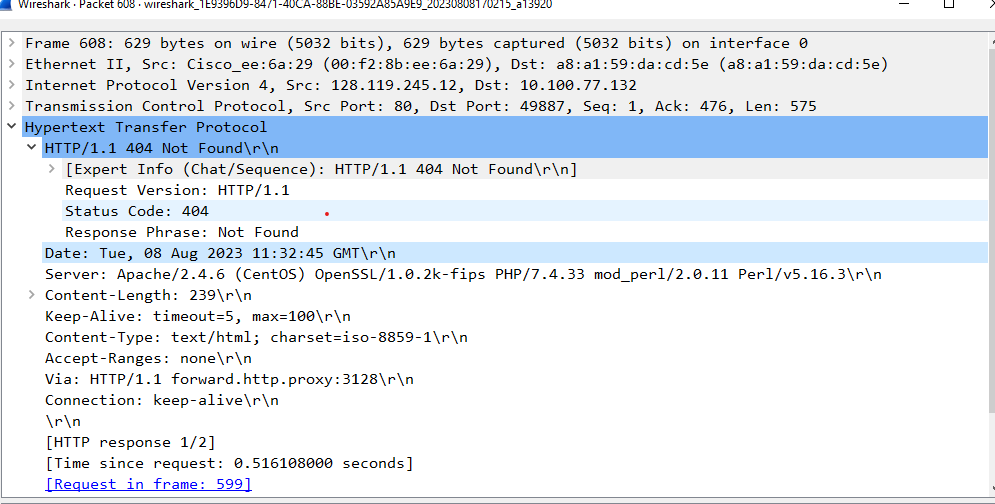
3. What is the IP address of your computer? and the gaia.cs.umass.edu server?



IP address of Computer (Src) 128.119.245.12 and the given server (dst)

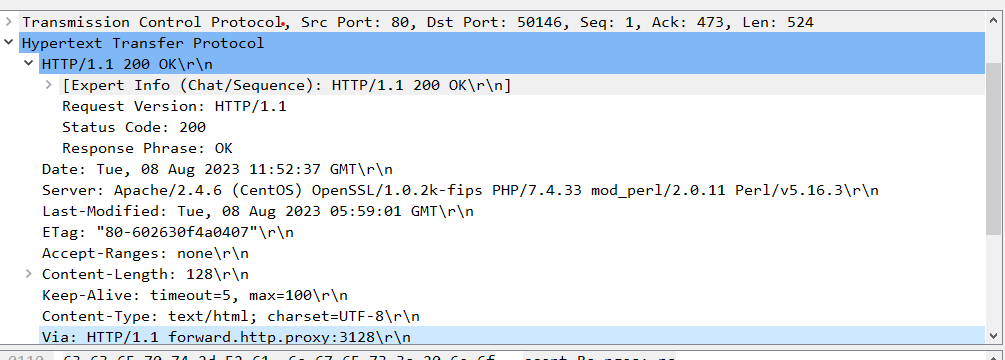
10.100.77.132

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



404 Not Found as it was reloaded twice.

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



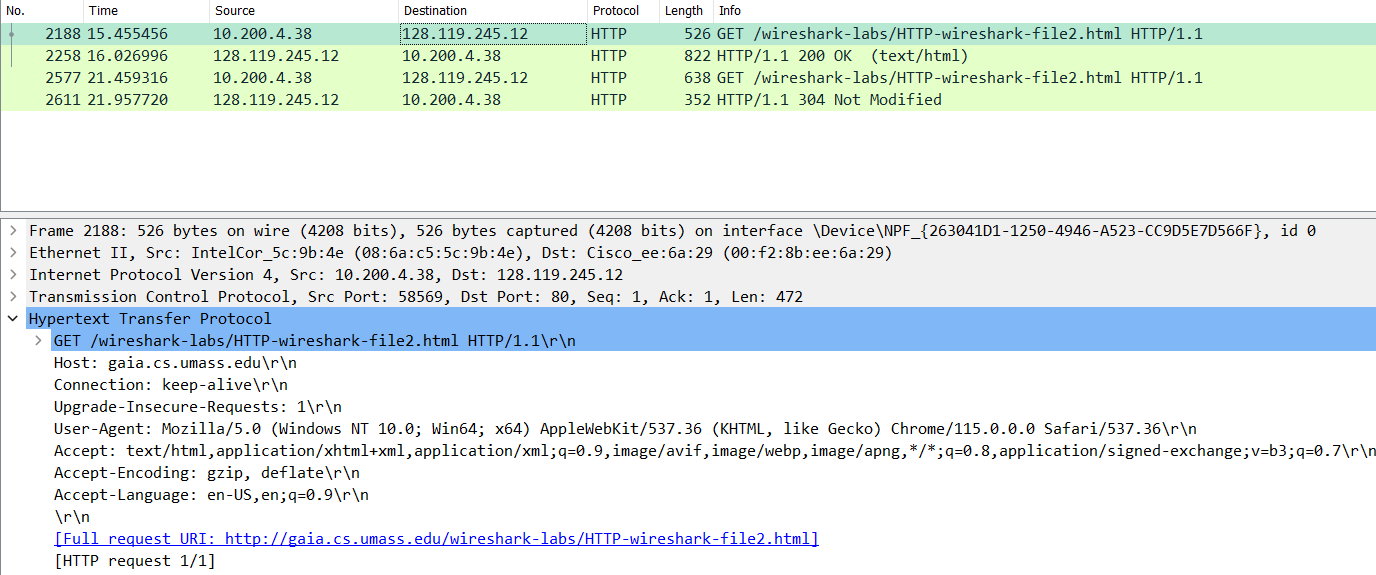
6. How many bytes of content are being returned to your browser?

It is 128 Bytes.

**5.2:**

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?

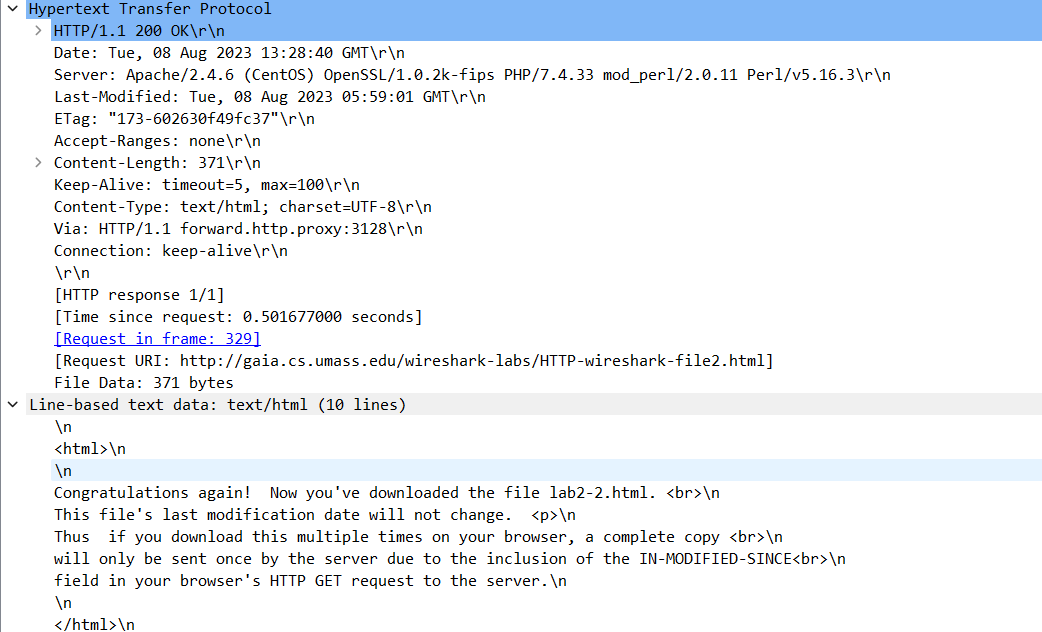
No it is not shown.



Yes as mentioned above.

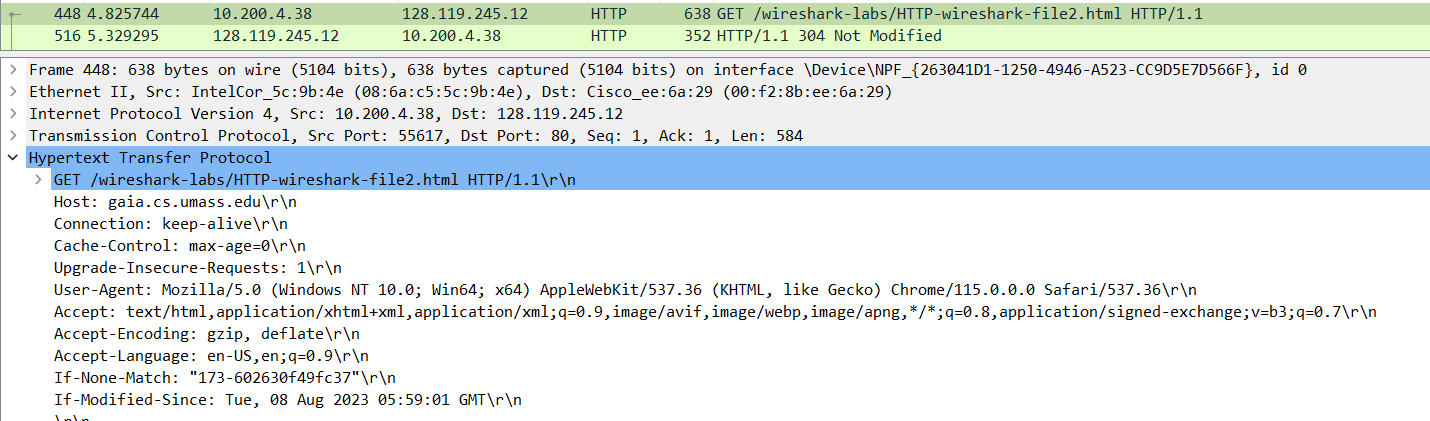
2. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Yes as it shows the content length with the line based content as shown



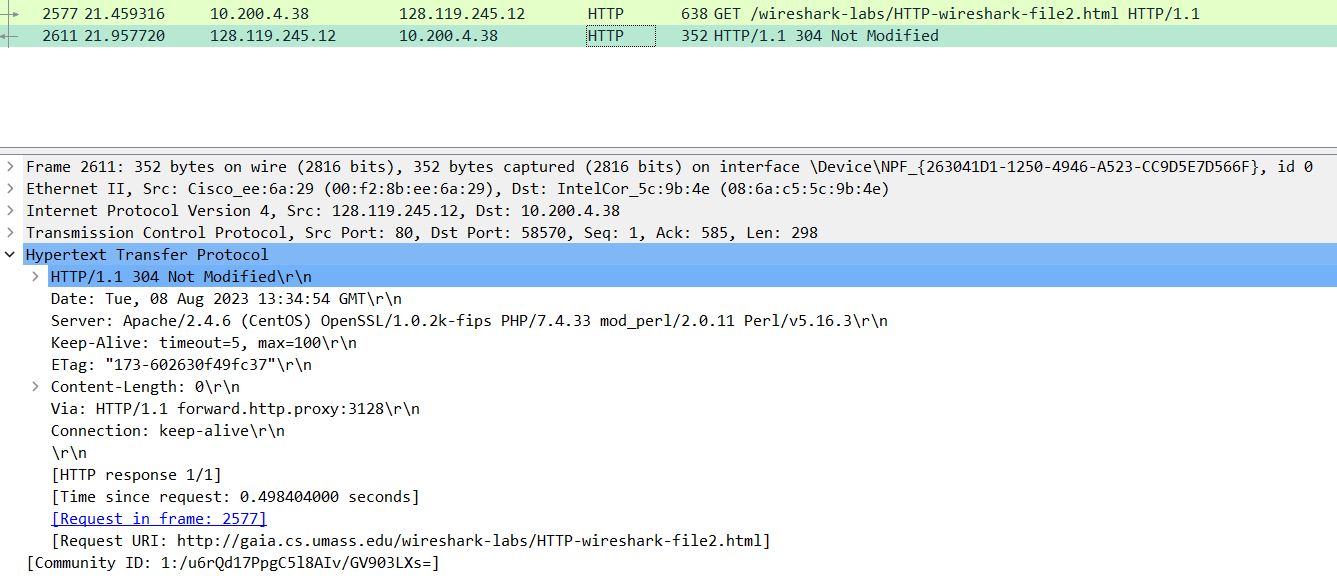
3. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an ”IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the ”IF-MODIFIED-SINCE:” header?

Yes it is shown as below.



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.

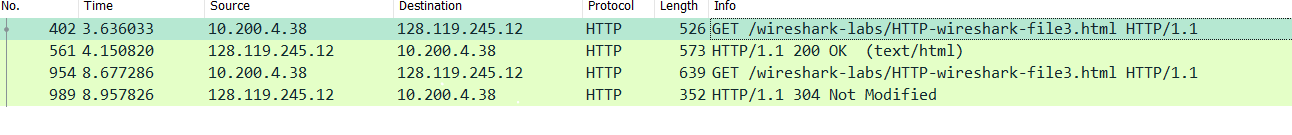
It is 304 Not modified and this time the line based data is not shown as it is the same.



**6.2:**

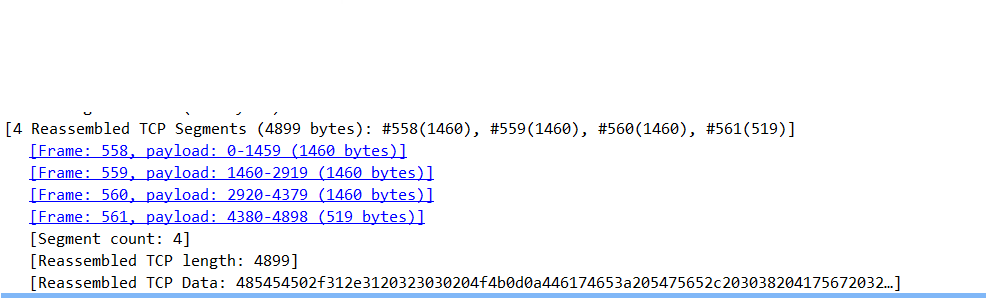
1. How many HTTP GET request messages were sent by your browser?

Only 1 GET request was send by the browser.



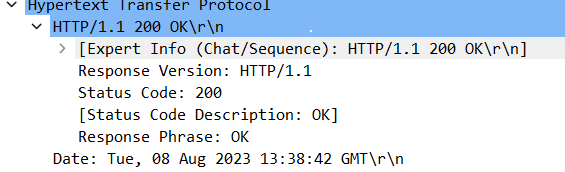
2. How many data-containing TCP segments were needed to carry the single HTTP response?

There were 4.



3. What is the status code and phrase associated with the response to the HTTP GET request?

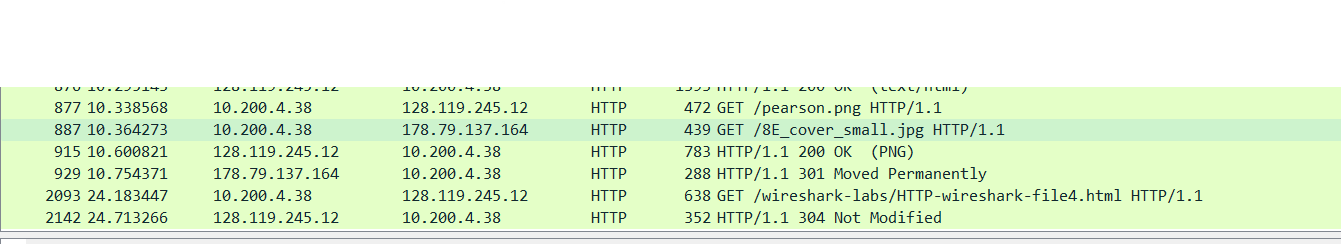
Status code is 200 and phrase is OK



**7.2:**

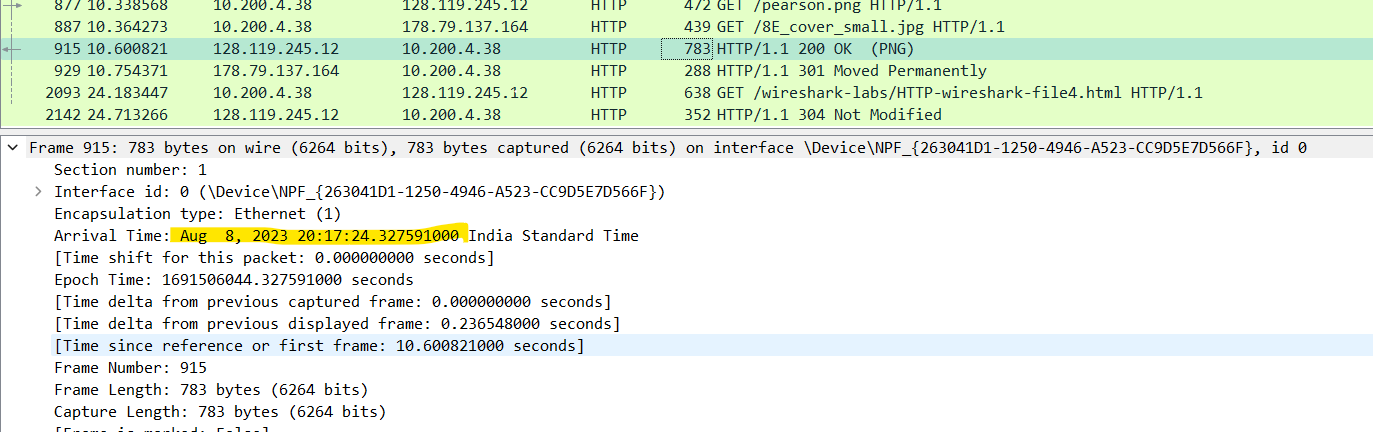
1. How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?

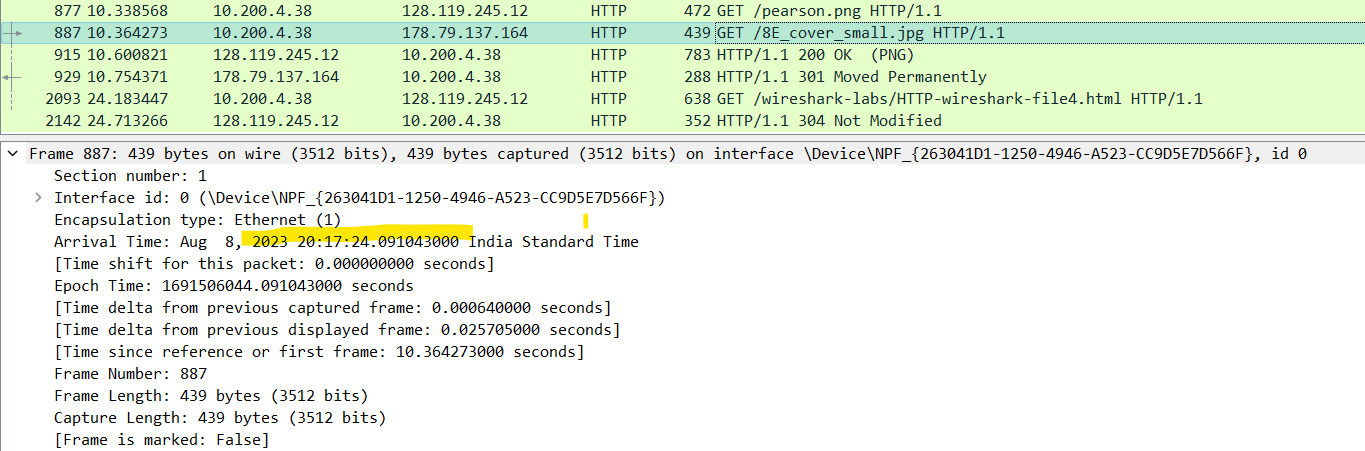
There were 3 GET request , 2 for the images (Pearson and BE cover small) and 1 webpage



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

It will be in series as both the timestamp are different from image so this is justified.

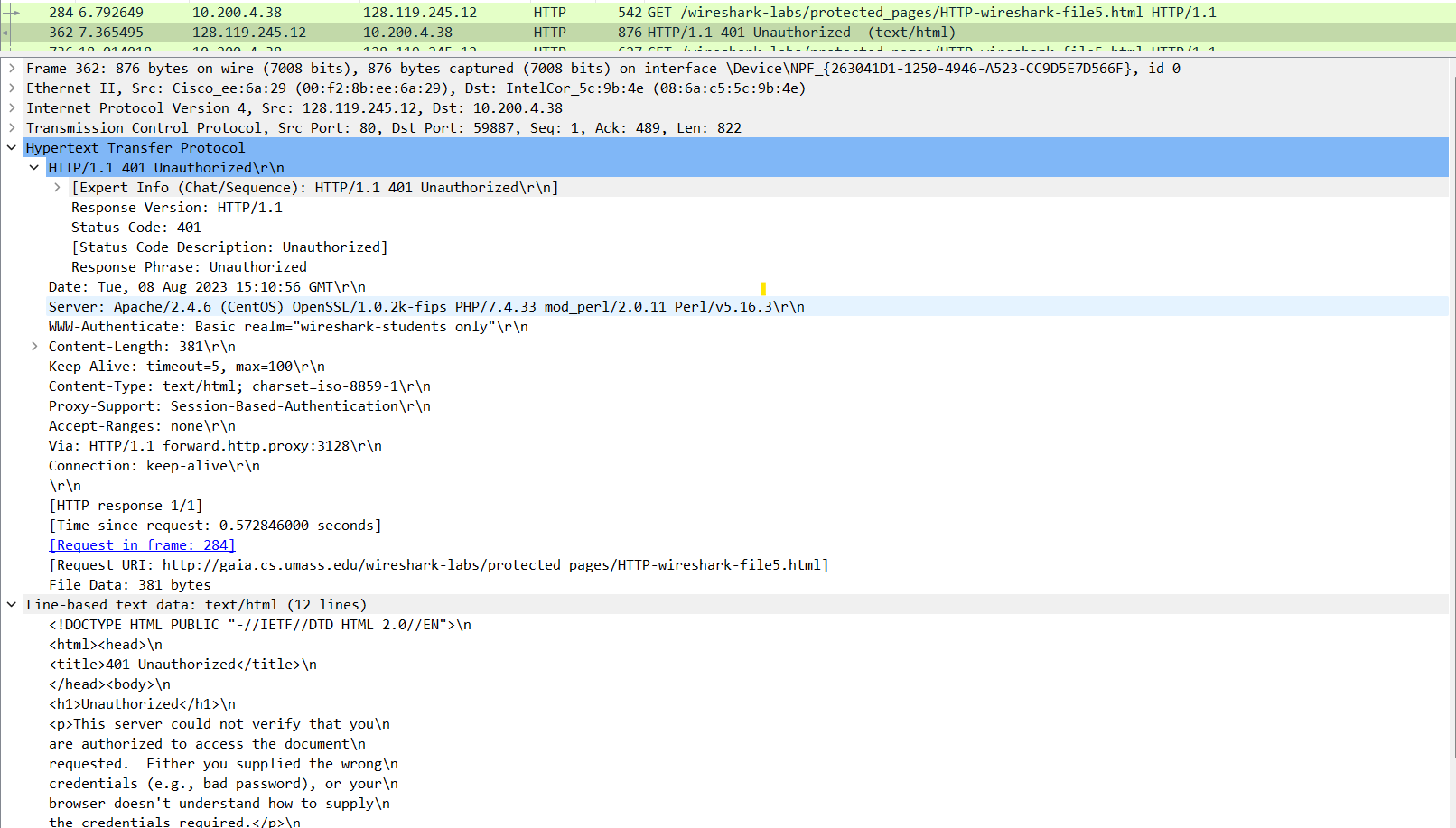




**8.2:**

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

It showed the unauthorized 401 error.



2. When your browsers sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The new message of Authorization is included in the field and this time it accepts the request and leads to the webpage with 200 status code and OK phrase.

