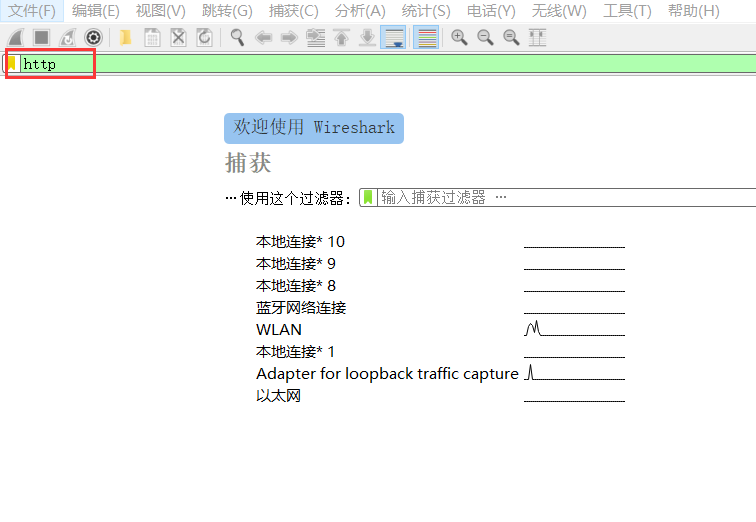
The five experiments can be roughly divided into the following steps（details may be different）:

1. Start up web browser and clear cache



2. Start up the Wireshark packet sniffer, but don’t begin packet capture. Enter “http” in the display-filter-specification window.

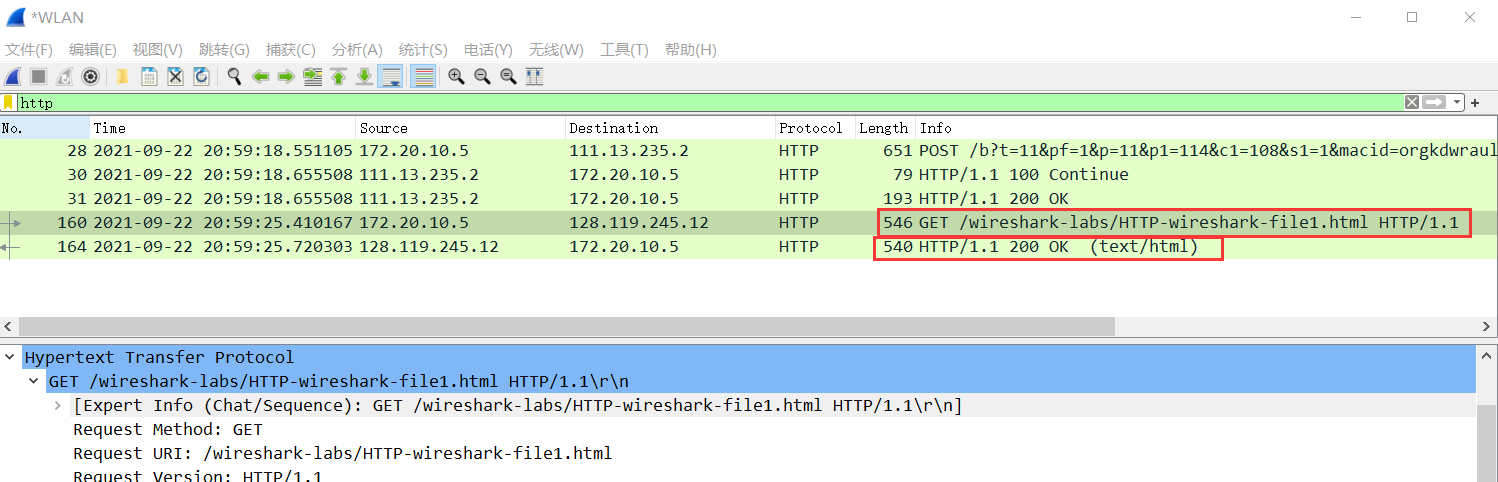


3. Enter the website.

4. Stop Wireshark packet capture

**一、The Basic HTTP GET/response interaction**

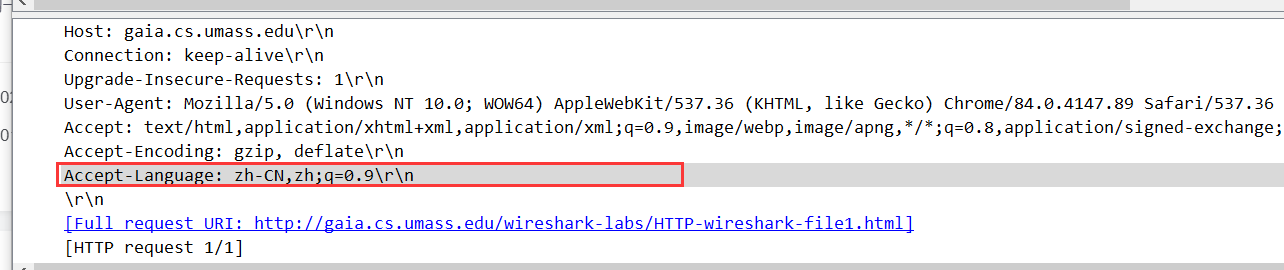
**1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?**



Both are running HTTP version 1.1

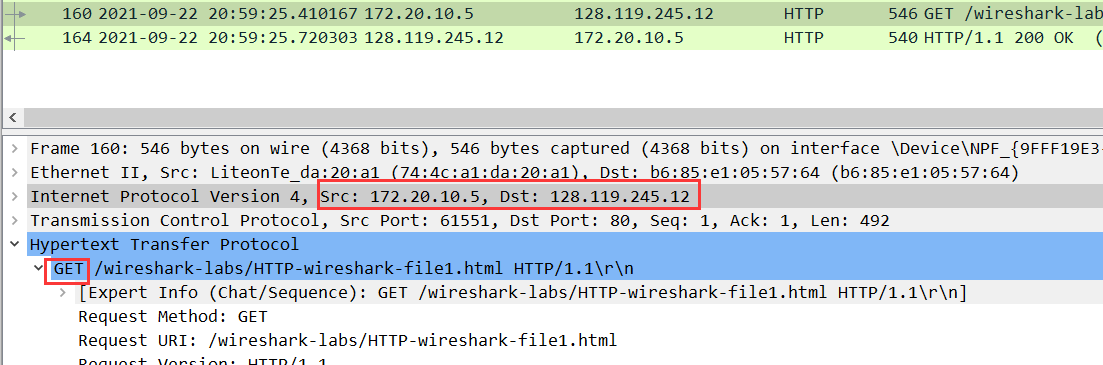
**2. What languages (if any) does your browser indicate that it can accept to the**

**server?**



Accept-Language:zh-CN,zh

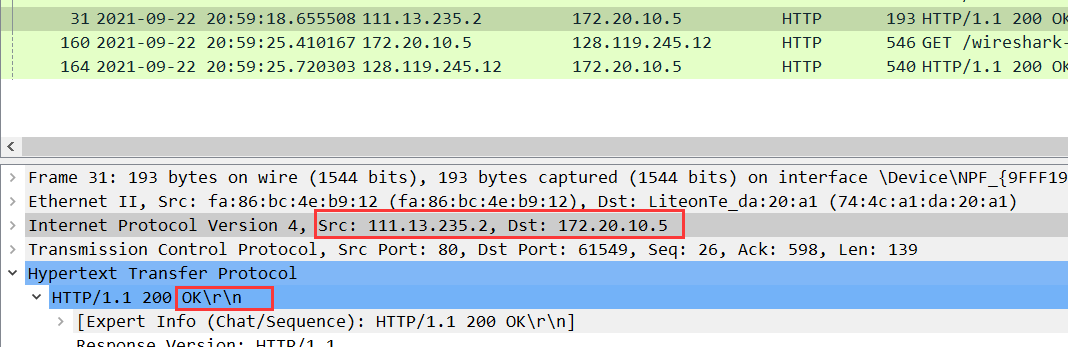
**3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?**



Get:

IP address of my computer(Src):172.20.10.5

IP address of the gaia.cs.umass.edu server(Dst):128.119.245.12

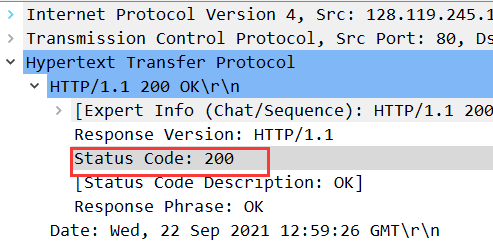


OK:

IP address of my computer(Dst):172.20.10.5

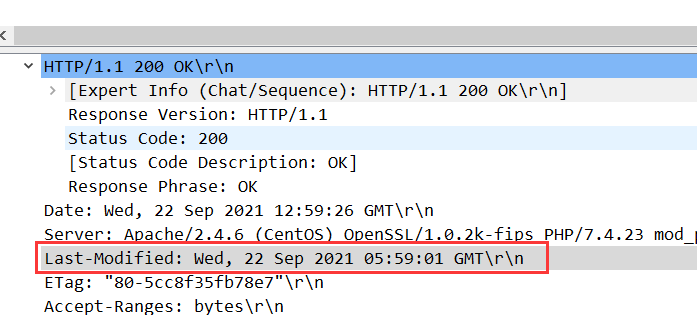
IP address of the gaia.cs.umass.edu server(Dst):111.13.235.2

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



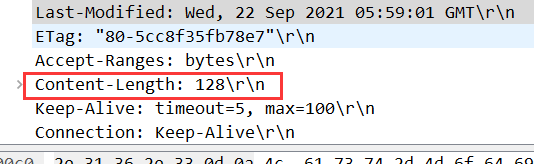
Status Code:200

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



Last-Modified:Wed,22 Seq 2021 05:59:01 GMT

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



Content-Length:128

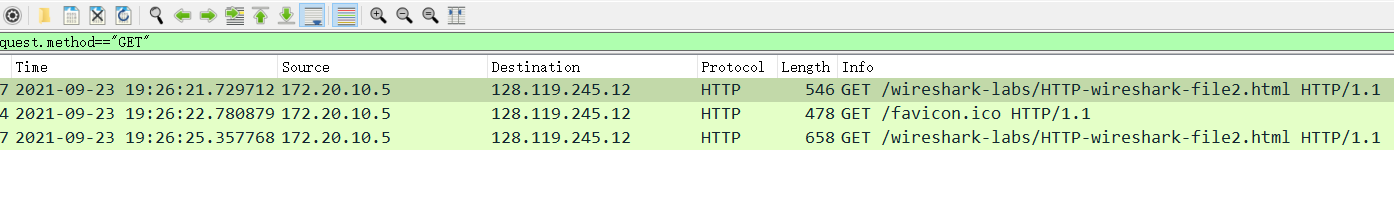
**7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.**

No,all of the headers displayed in the packet-listing window.

**二、The HTTP CONDITIONAL GET/response interaction**

**8. Inspect the contents of the first HTTP GET request from your browser to the**

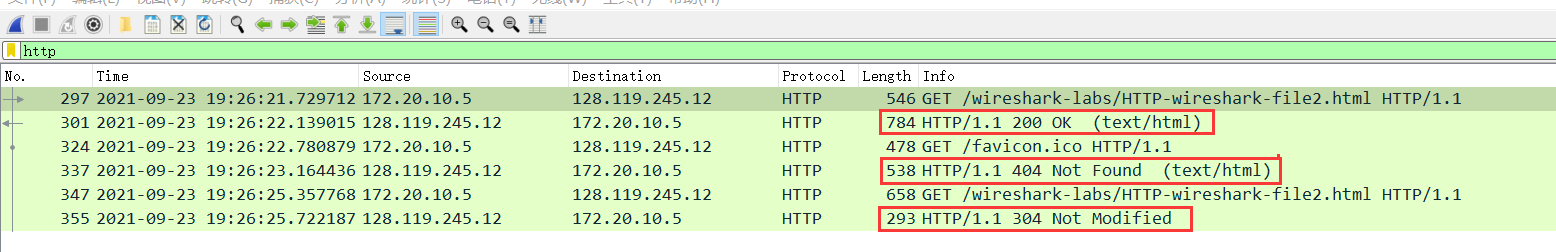
**server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?**



No.

**9. Inspect the contents of the server response. Did the server explicitly return the**

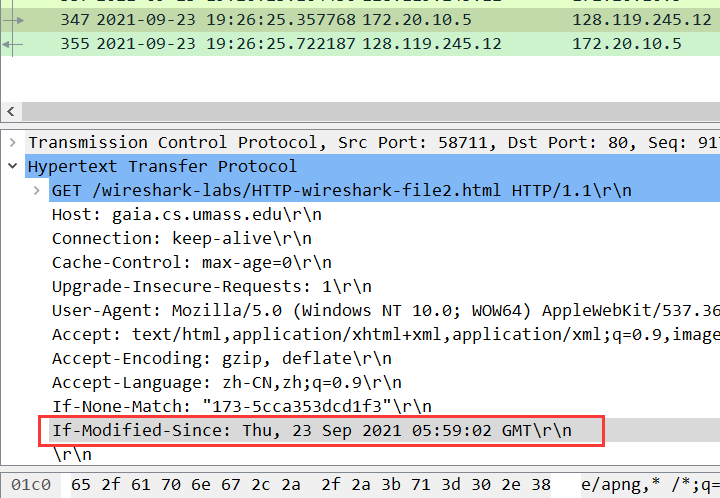
**contents of the file? How can you tell?**



When we first access the website, the server explicitly return the constents of the file,but the second access,the server didn’t return any contents of the file.

When we first access the website http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html,my browser’s cache is empty,so the server explicitly return the constents of the file.But when the second access,cause what we need is in the browser’s cache,so the server didn’t return any contents 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?**



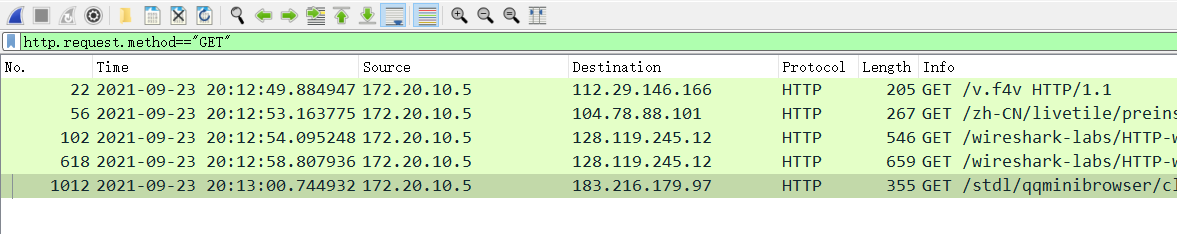
Information follows header is the server response last-modified time.

**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.**

304 Not Modified, the server did not explicitly return the contents of the file,cause the second time the cache had already instore the information.

**三、Retrieving Long Documents**

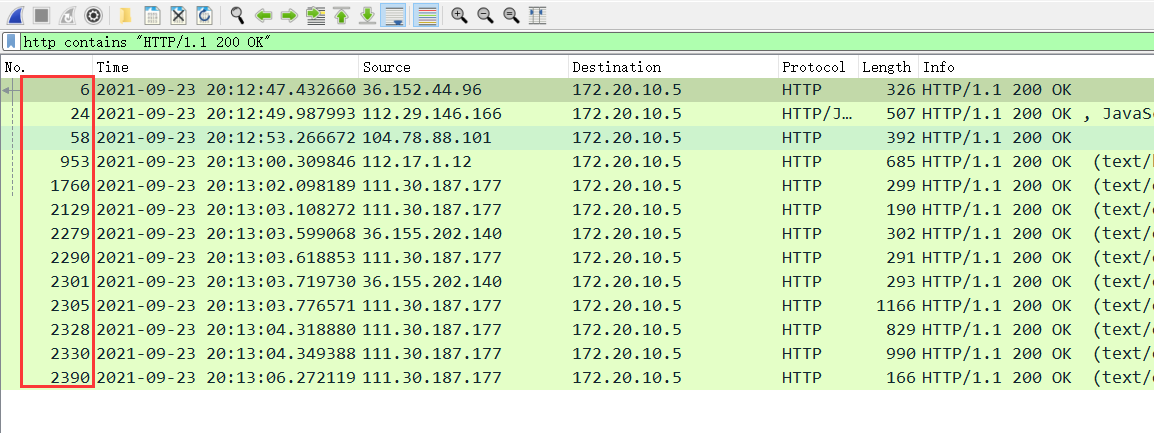
**12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?**



5 requests messages.

packet 22

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

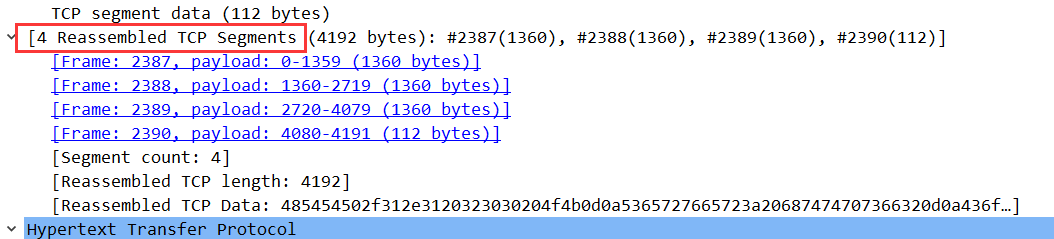


The packet number are the part surrounded by a red frame as shown in the figure.

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

The status code is 200 and phrase is “OK”.

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

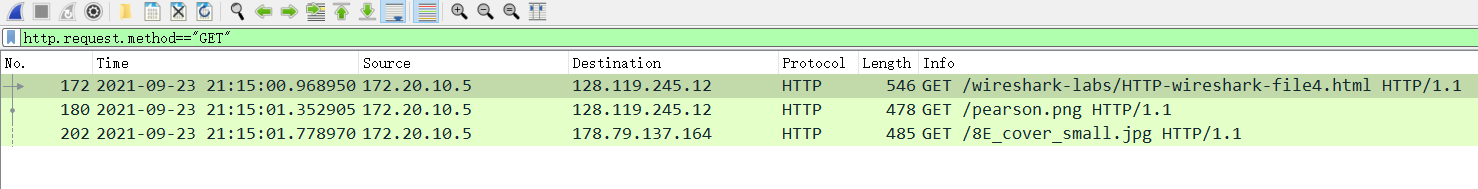


4 TCP segments were needed.

**四、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?**



3 messages.

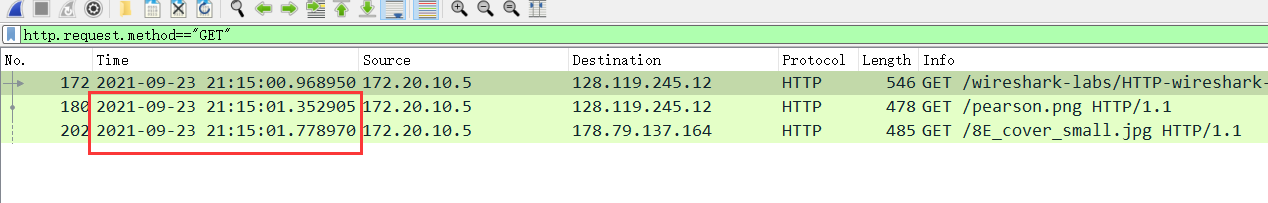
For 172 packet,the request was sent to html.

For 180 packet,the request was sent to pearson.png

For 202 packet,the request was sent to 8E\_cover\_small.jpg

**17. Can you tell whether your browser downloaded the two images serially, or**

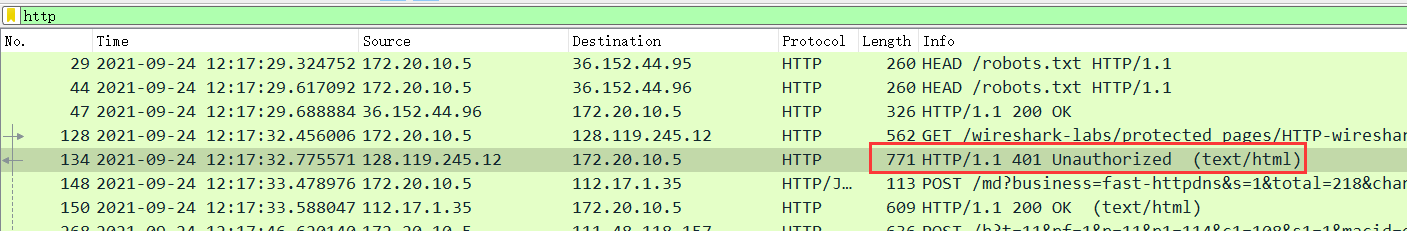
**whether they were downloaded from the two web sites in parallel? Explain.**



In parallel,from the picture we can find that the two request for imag is simultaneous.

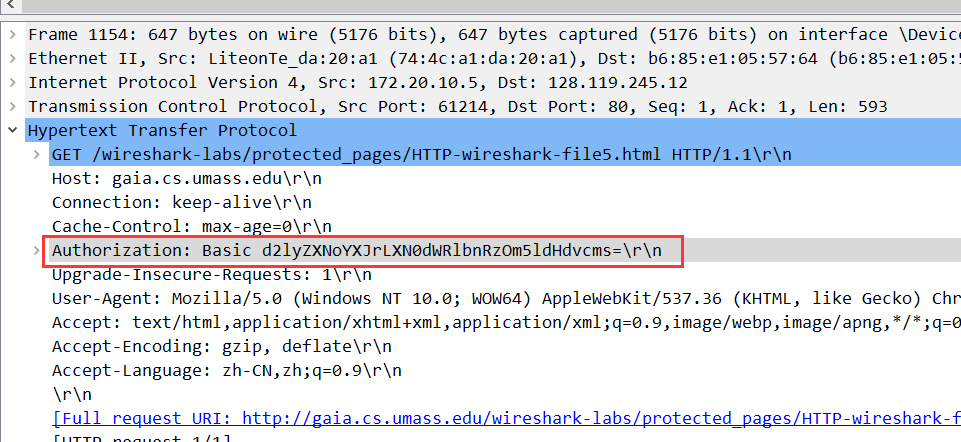
**五、HTTP Authentication**

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



401 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?**



Authorization:Basic d2lyZXNoYXJrLXN0dwRlbnRzOm51dHdvcms=