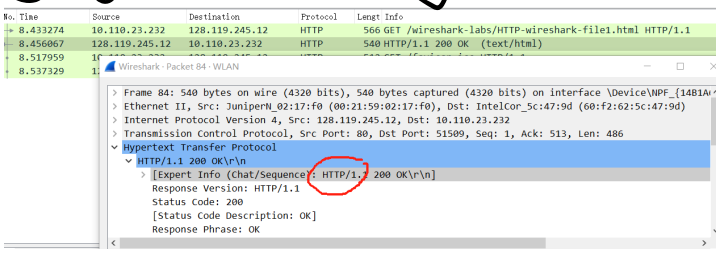
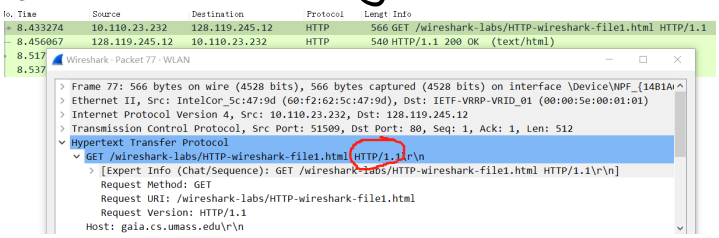
1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running? **(5 Points)**

① my browser is running HTTP 1.1



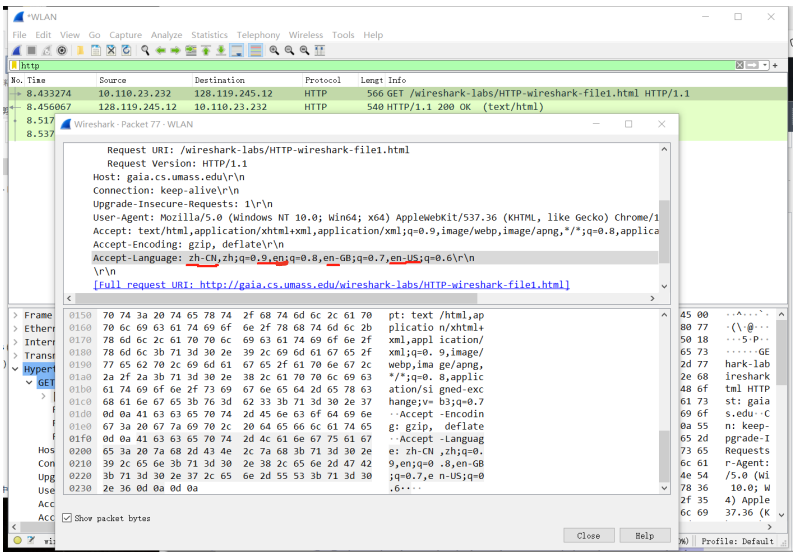
② Server is running HTTP 1.1



I have read and understood the course academic integrity policy

Tooran Liu

2. What languages (if any) does your browser indicate that it can accept to the server? **(5 Points)**



① zh-CN, ch ← Chinese

② en ← English

③ en-GB ← British English

④ en-US ← American English

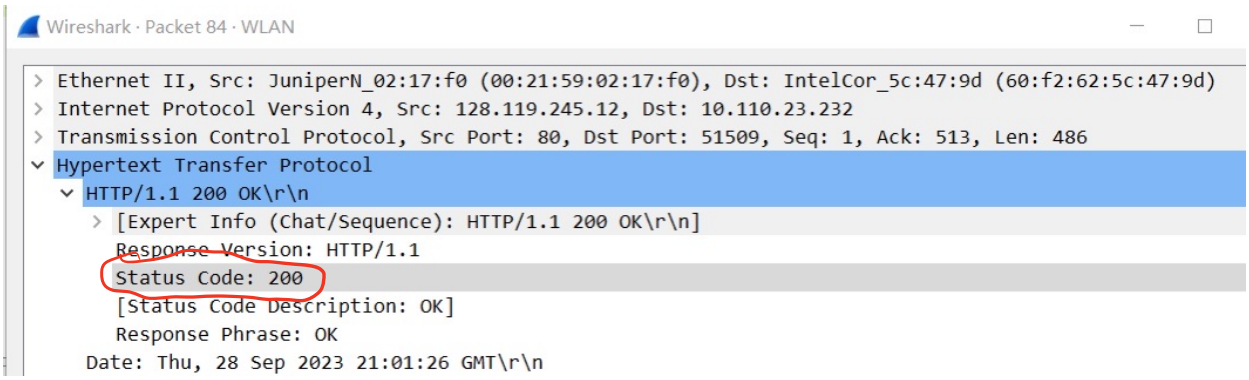
3. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server? **(5 Points)**

No.	Time	Source	Destination	Protocol	Lengt	Info
→	8.433274	10.110.23.232	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
←	8.456067	128.119.245.12	10.110.23.232	HTTP	540	HTTP/1.1 200 OK (text/html)

IP address of my computer : 10.110.23.232

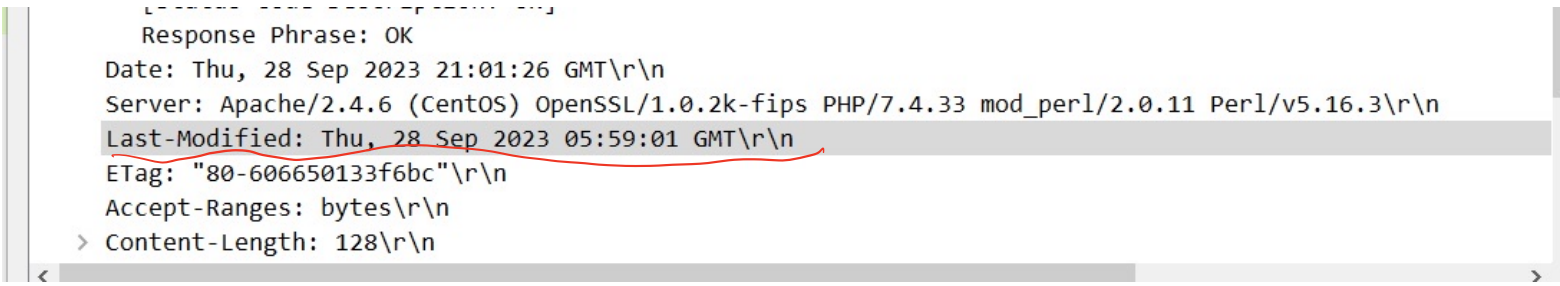
IP address of server : 128.119.245.12

4. What is the status code returned from the server to your browser? **(5 Points)**



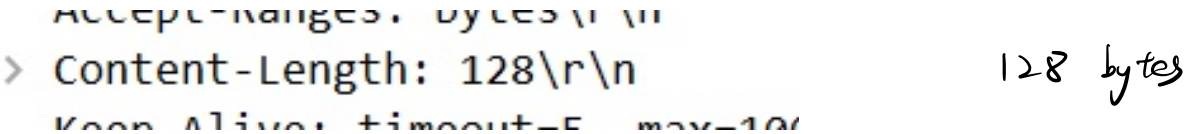
Status code: 200

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



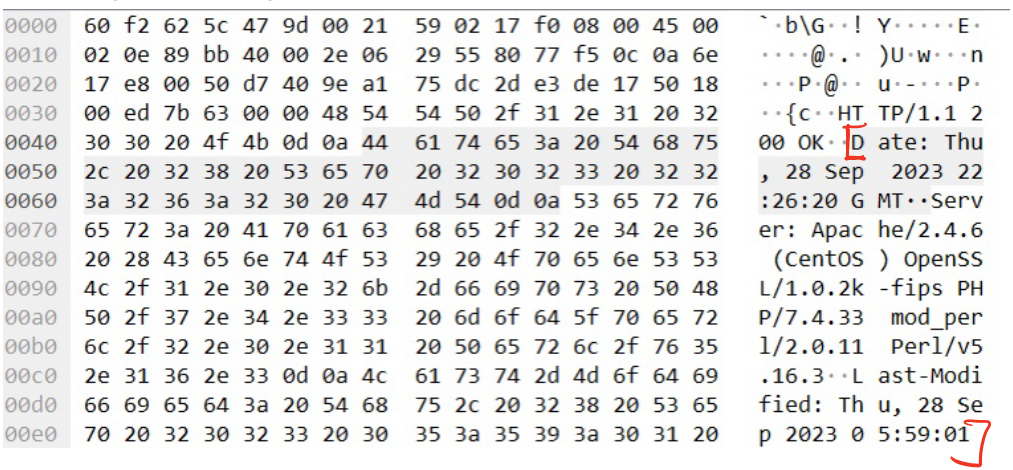
Last modified Thu 09/28/2023 05:59:01 GMT

6. How many bytes of content are being returned to your browser? **(5 Points)**



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. **(5 Points)**



every thing list side by Ascall are list in the header, but none of them display in packet listing window.

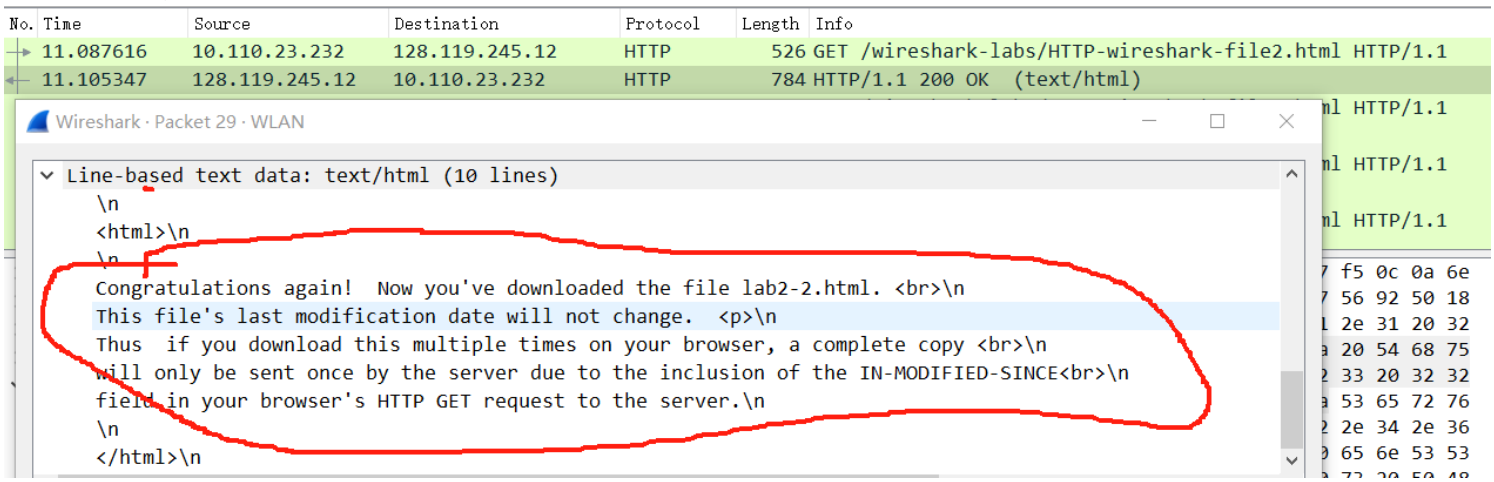
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET? **(5 Points)**

No

```
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file2.html
    Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
\r\n
```

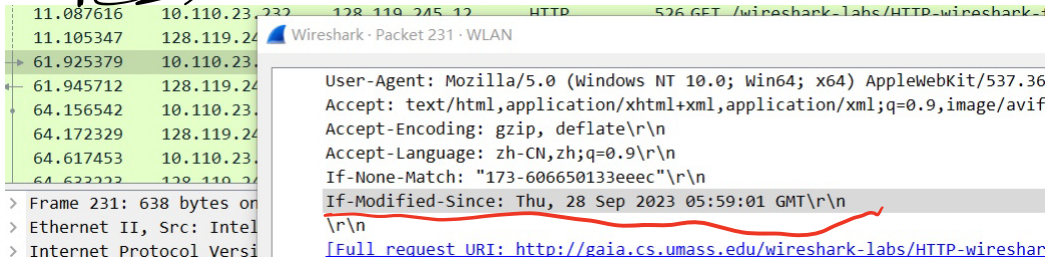
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell? **(5 Points)**

Yes, here show the content in HTML



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[2]? If so, what information follows the "IF-MODIFIED-SINCE:" header? **(5 Points)**

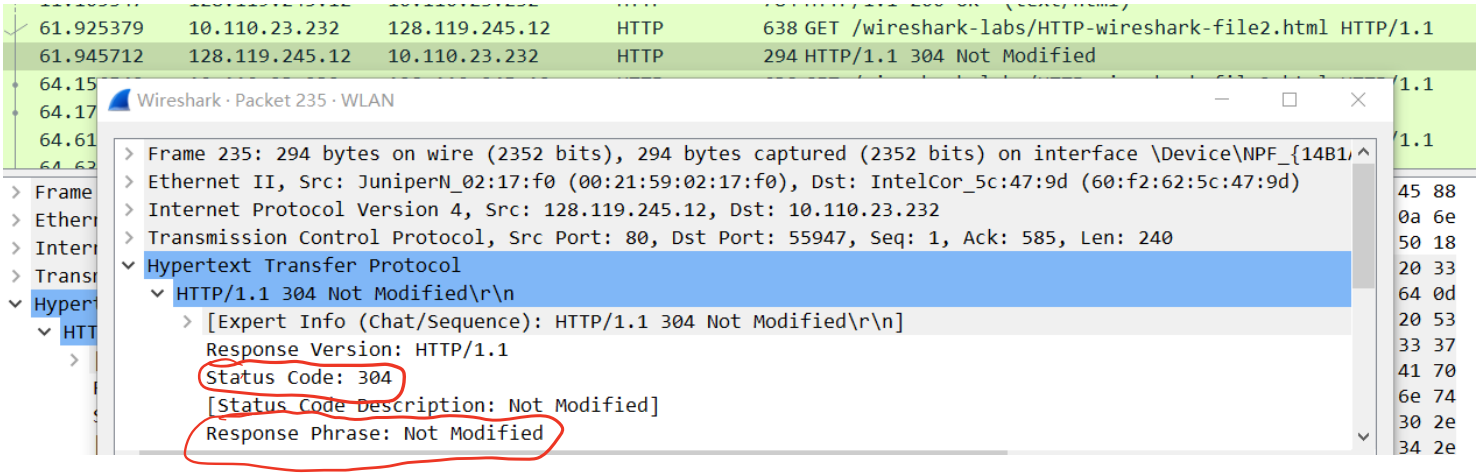
Yes, The following information is date and time.

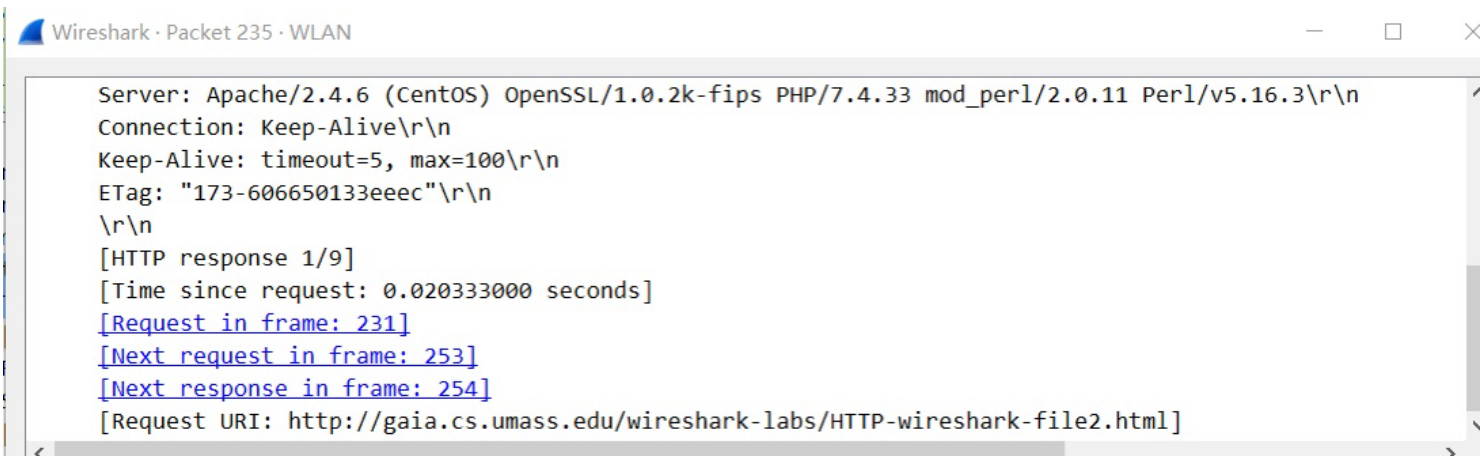


11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain. **(5 Points)**

status code and phrase : 304 Not Modified.

No contents return





I think is because of the contents is already save in local cache. And when header contains "IF-MODIFIED-SINCE:" when client sent request in the second time. also server check the contents is indeed not changed then, server just reply "Not modified" in header instead of send back whole contents. It probably design for save internet resourse.

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 Points)**

① only one HTTP GET

② packet number 23

23	2.106218	10.110.23.232	128.119.245.12	HTTP	552 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
24	2.122001	128.119.245.12	10.110.23.232	TCP	56 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=0
25	2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
26	2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
27	2.124871	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=2921 Win=131328 Len=0
28	2.125050	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=2921 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
29	2.125050	128.119.245.12	10.110.23.232	HTTP	535 HTTP/1.1 200 OK (text/html)
30	2.125131	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=4862 Win=131328 Len=0
31	2.133054	142.250.65.174	10.110.23.232	TLSv1.2	121 Application Data

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? **(5 Points)**

number 29

23	2.106218	10.110.23.232	128.119.245.12	HTTP	552 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
24	2.122001	128.119.245.12	10.110.23.232	TCP	56 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=0
25	2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
26	2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
27	2.124871	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=2921 Win=131328 Len=0
28	2.125050	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=2921 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
29	2.125050	128.119.245.12	10.110.23.232	HTTP	535 HTTP/1.1 200 OK (text/html)
30	2.125131	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=4862 Win=131328 Len=0
31	2.133054	142.250.65.174	10.110.23.232	TLSv1.2	121 Application Data

14. What is the status code and phrase in the response? **(5 Points)**

200 ok

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? **(5 Points)**

There are three TCP segments carry text of Bill of Rights

23	2.106218	10.110.23.232	128.119.245.12	HTTP	552 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
24	2.122001	128.119.245.12	10.110.23.232	TCP	56 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=0
25	2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
26	2.124761	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=1461 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
27	2.124871	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=2921 Win=131328 Len=0
28	2.125050	128.119.245.12	10.110.23.232	TCP	1514 80 → 60734 [ACK] Seq=2921 Ack=499 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
29	2.125050	128.119.245.12	10.110.23.232	HTTP	535 HTTP/1.1 200 OK (text/html)
30	2.125131	10.110.23.232	128.119.245.12	TCP	54 60734 → 80 [ACK] Seq=499 Ack=4862 Win=131328 Len=0
31	2.133054	142.250.65.174	10.110.23.232	TLSv1.2	121 Application Data

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent? **(5 Points)**

3 HTTP GET request

http

No.	Time	Source	Destination	Protocol	Lengt	Info
630	3.192628	10.110.23.232	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4…
640	3.211569	128.119.245.12	10.110.23.232	HTTP	1355	HTTP/1.1 200 OK (text/html)
684	3.383861	10.110.23.232	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
693	3.402328	128.119.245.12	10.110.23.232	HTTP	745	HTTP/1.1 200 OK (PNG)
697	3.457309	10.110.23.232	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
699	3.526943	178.79.137.164	10.110.23.232	HTTP	225	HTTP/1.1 301 Moved Permanently

for the first two request, 128.119.245.12

for the cover image, 178.79.137.164

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. **(10 Points)**

626	3.192066	128.119.245.12	10.110.23.232	TCP	66	80 → 62790 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
628	3.192220	10.110.23.232	128.119.245.12	TCP	54	62790 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
630	3.192628	10.110.23.232	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
631	3.193340	128.119.245.12	10.110.23.232	TCP	66	80 → 62791 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
632	3.193396	10.110.23.232	128.119.245.12	TCP	54	62791 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
635	3.209164	128.119.245.12	10.110.23.232	TCP	56	80 → 62790 [ACK] Seq=1 Ack=473 Win=30336 Len=0
640	3.211569	128.119.245.12	10.110.23.232	HTTP	1355	HTTP/1.1 200 OK (text/html)
647	3.254993	10.110.23.232	128.119.245.12	TCP	54	62790 → 80 [ACK] Seq=473 Ack=1302 Win=130048 Len=0
688	3.388183	155.33.2.2	10.110.23.232	DNS	156	Standard query response 0xb993 HTTP…
689	3.388757	10.110.23.232	178.79.137.164	TCP	66	62794 → 80 [SYN] Seq=0 Win=64240 Le…
690	3.400798	128.119.245.12	10.110.23.232	TCP	1514	80 → 62790 [ACK] Seq=1302 Ack=891 W…
691	3.400798	128.119.245.12	10.110.23.232	TCP	1514	80 → 62790 [ACK] Seq=2762 Ack=891 W…
692	3.400887	10.110.23.232	128.119.245.12	TCP	54	62790 → 80 [ACK] Seq=891 Ack=4222 W…
693	3.402328	128.119.245.12	10.110.23.232	HTTP	745	HTTP/1.1 200 OK (PNG)
694	3.444598	10.110.23.232	128.119.245.12	TCP	54	62790 → 80 [ACK] Seq=891 Ack=4913 W…
695	3.457004	178.79.137.164	10.110.23.232	TCP	66	80 → 62794 [SYN, ACK] Seq=0 Ack=1 W…
696	3.457074	10.110.23.232	178.79.137.164	TCP	54	62794 → 80 [ACK] Seq=1 Ack=1 Win=13…
697	3.457309	10.110.23.232	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
698	3.526943	178.79.137.164	10.110.23.232	TCP	56	80 → 62794 [ACK] Seq=1 Ack=386 Win=…
699	3.526943	178.79.137.164	10.110.23.232	HTTP	225	HTTP/1.1 301 Moved Permanently

The IP 178.79.137.164 only send packet after all packet from IP 128.119.245.12 finished sent all packet, it follow the time order

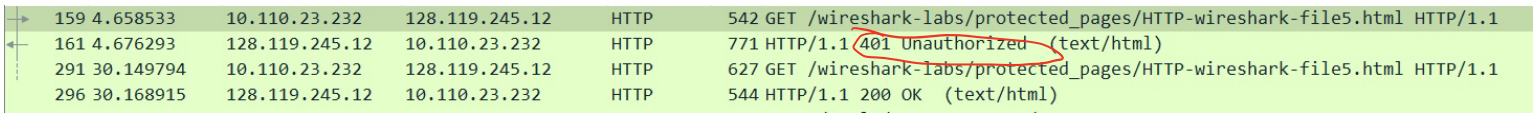
No packets from different sources are set alternately even once.

Besides, there are two request one after another for two image.

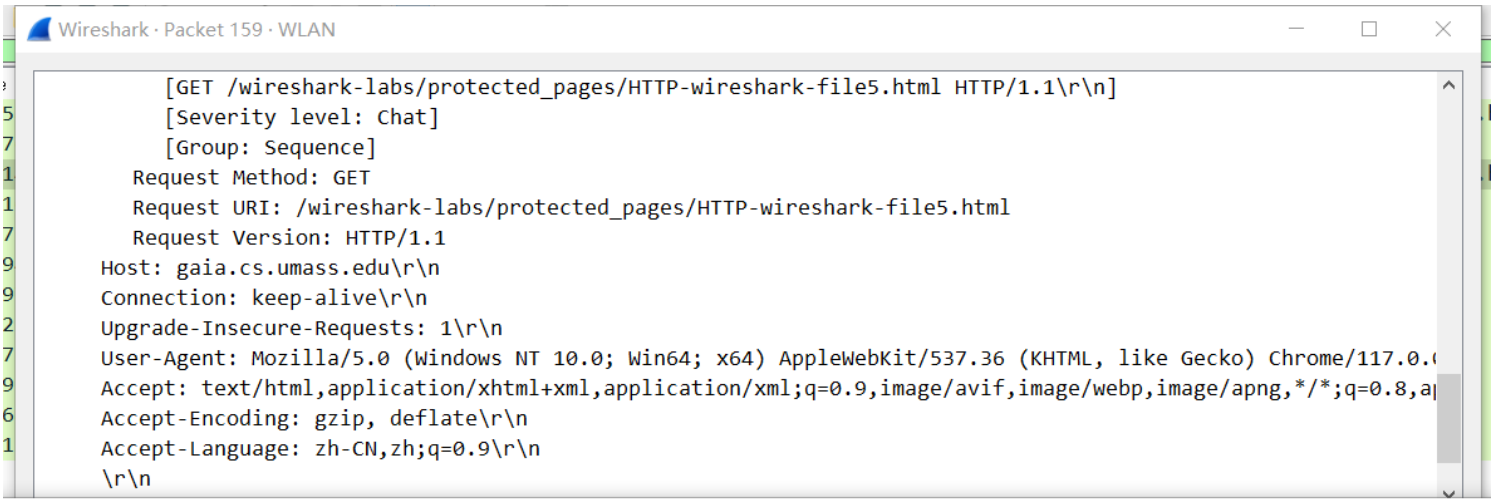
so, two images was sent serially, I think.

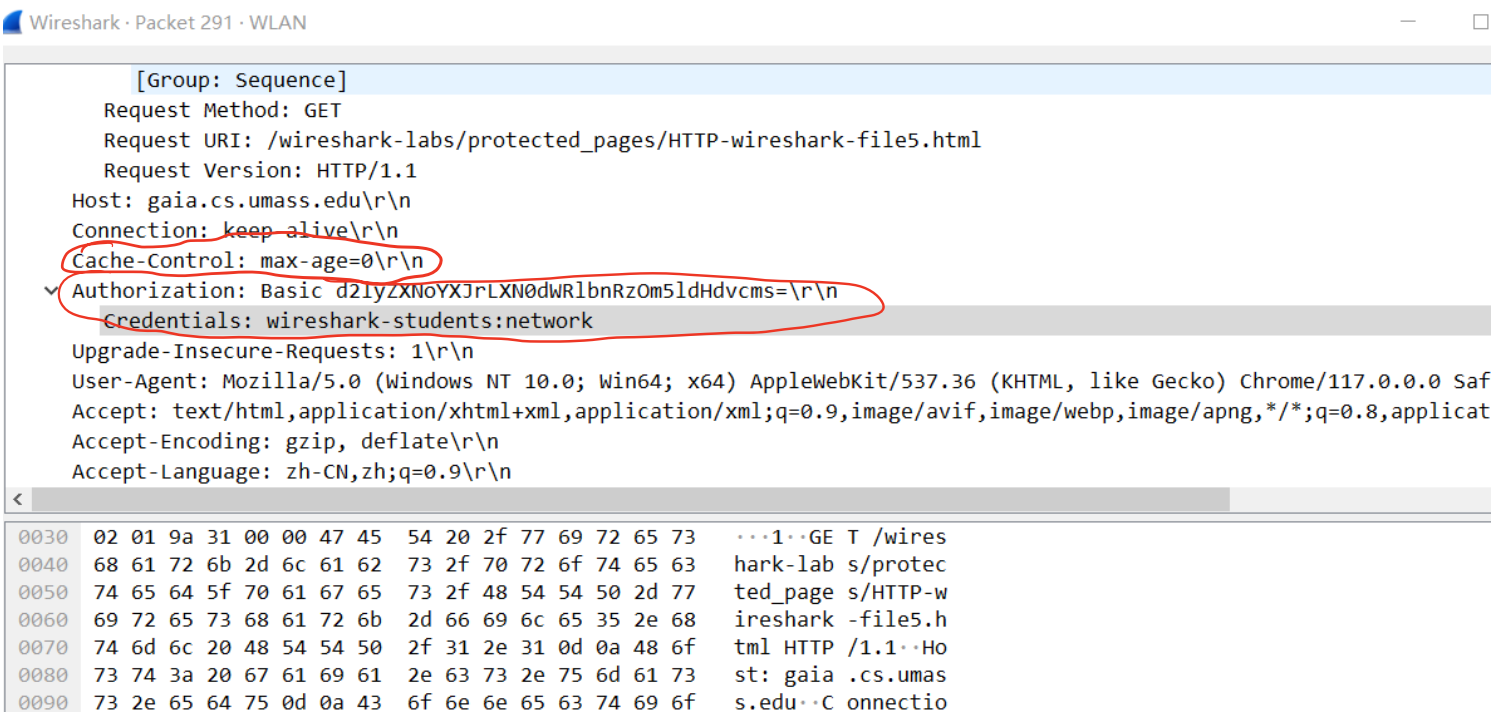
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser? **(5 Points)**

in the first time. response is 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? **(5 Points)**





Cache-control: max-age = 0
and Authorization information and credentials