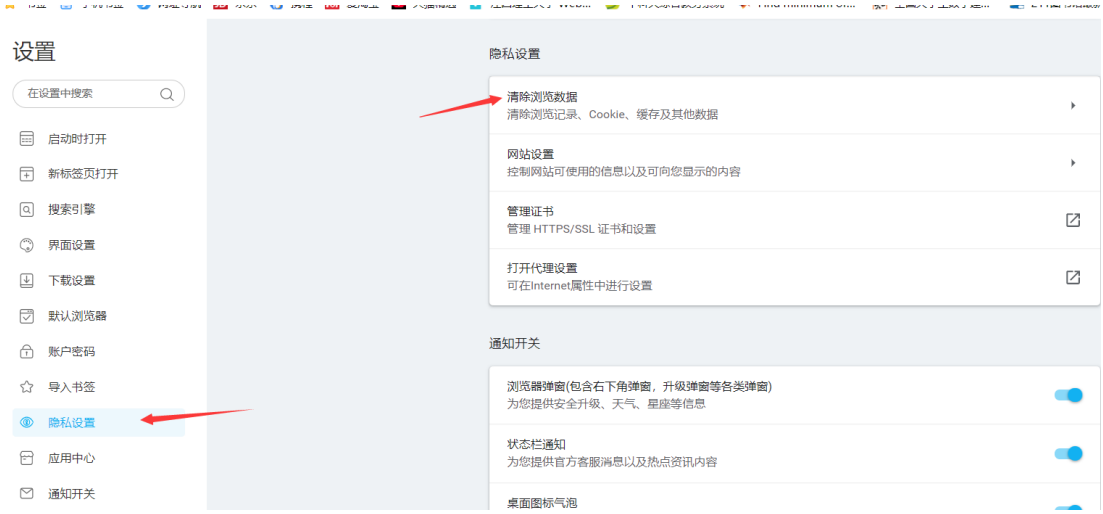
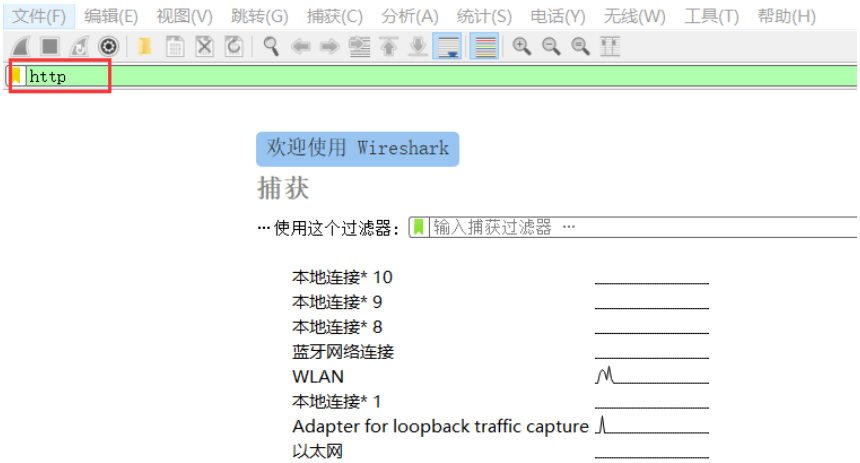
The five experiments can be roughly divided into the following steps (details may be different):

1. Start up web browser and clear cache



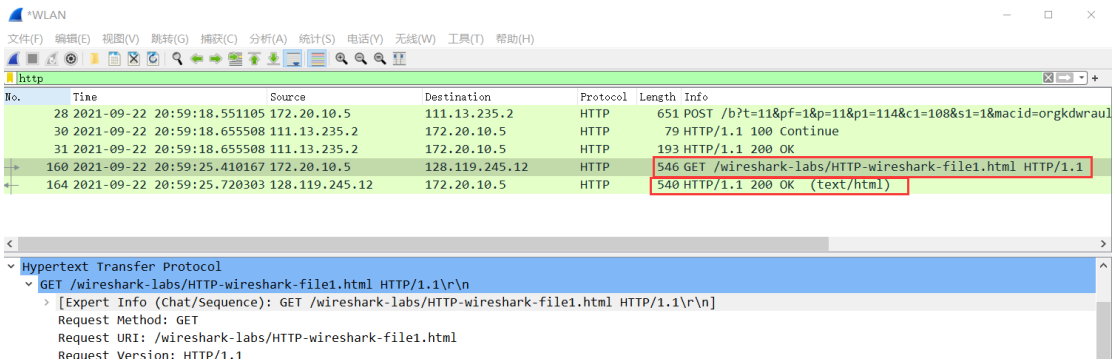
2. Start up the Wireshark packet sniffer, but don't begin packet capture. Enter "http" in the display-filter-specification window.



3. Enter the website.
4. Stop Wireshark packet capture

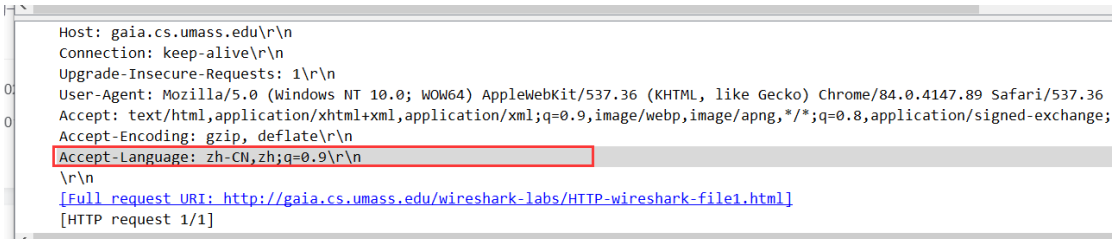
一、The Basic HTTP GET/response interaction

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



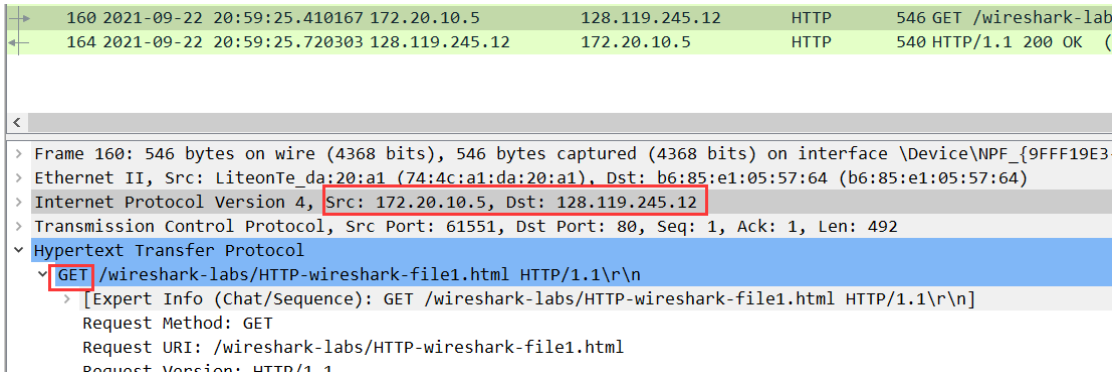
Both are running HTTP version 1.1

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



Accept-Language:zh-CN,zh

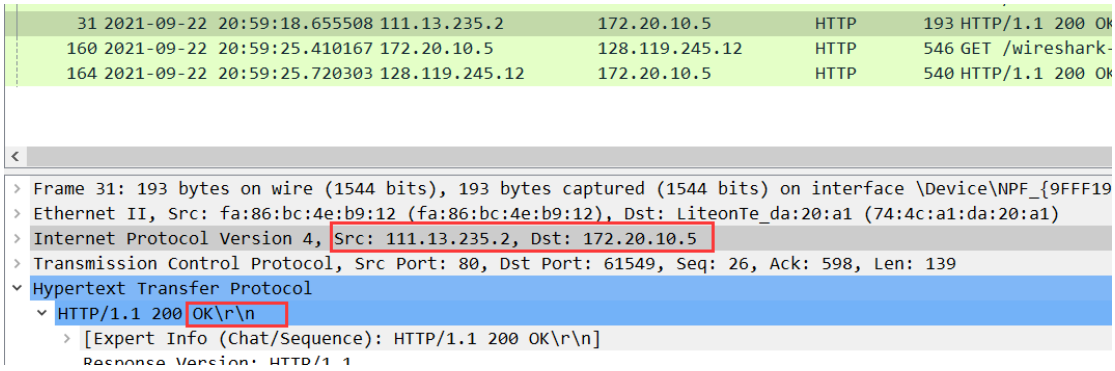
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?



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?

```
> Internet Protocol Version 4, Src: 128.119.245.1
> Transmission Control Protocol, Src Port: 80, Ds
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Wed, 22 Sep 2021 12:59:26 GMT\r\n
```

Status Code:200

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

```
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Wed, 22 Sep 2021 12:59:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.23 mod_
    Last-Modified: Wed, 22 Sep 2021 05:59:01 GMT\r\n
    ETag: "80-5cc8f35fb78e7"\r\n
    Accept-Ranges: bytes\r\n
```

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

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

```
    Last-Modified: Wed, 22 Sep 2021 05:59:01 GMT\r\n
    ETag: "80-5cc8f35fb78e7"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
```

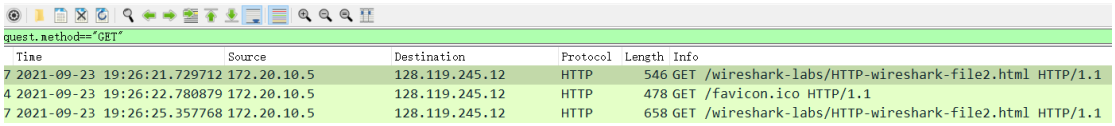
Content-Length:128

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.

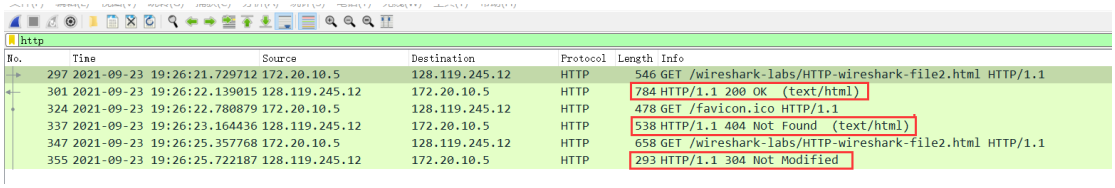
二、The HTTP CONDITIONAL GET/response interaction

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.

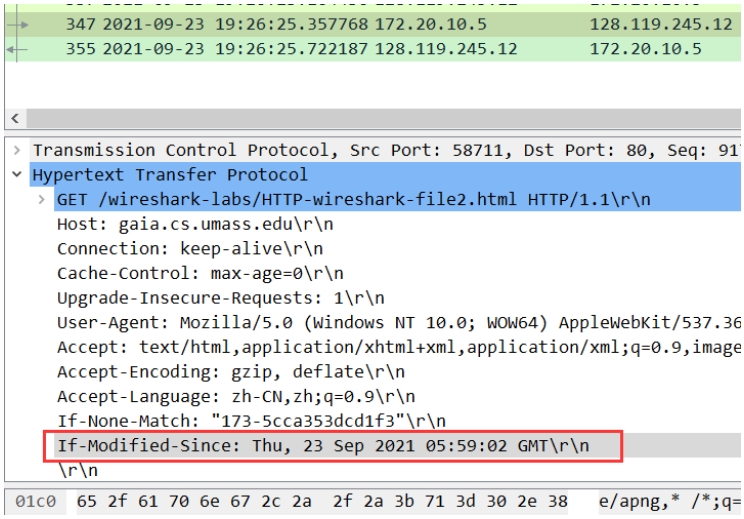
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



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?



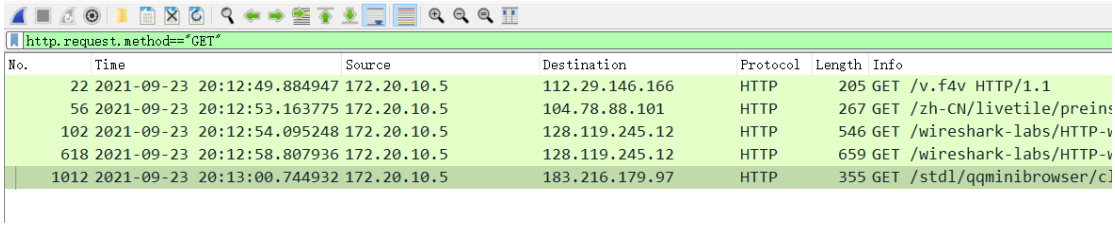
Information follows header is the server response last-modified time.

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?

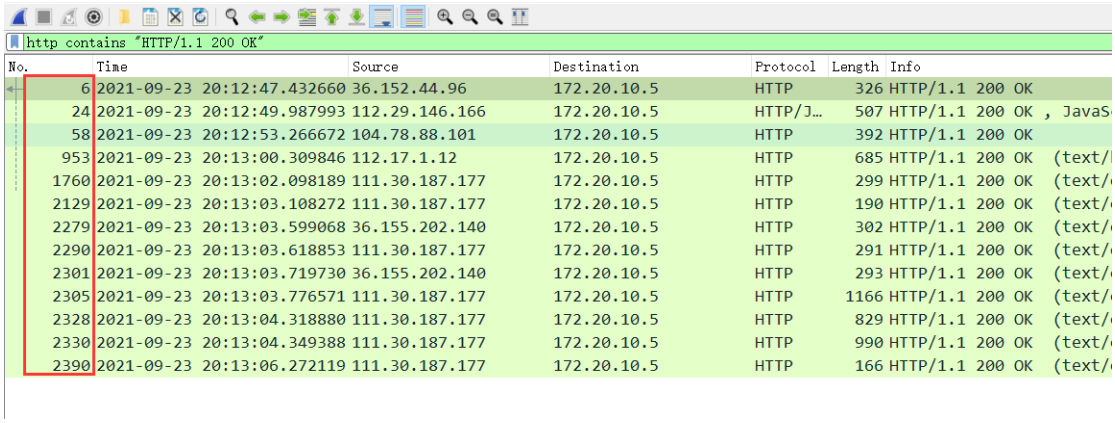


http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
22	2021-09-23 20:12:49.884947	172.20.10.5	112.29.146.166	HTTP	205	GET /v.f4v HTTP/1.1
56	2021-09-23 20:12:53.163775	172.20.10.5	104.78.88.101	HTTP	267	GET /zh-CN/livetile/preins
102	2021-09-23 20:12:54.095248	172.20.10.5	128.119.245.12	HTTP	546	GET /wireshark-labs/HTTP-w
618	2021-09-23 20:12:58.807936	172.20.10.5	128.119.245.12	HTTP	659	GET /wireshark-labs/HTTP-w
1012	2021-09-23 20:13:00.744932	172.20.10.5	183.216.179.97	HTTP	355	GET /stdl/qqminibrowser/cl

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?



http contains "HTTP/1.1 200 OK"

No.	Time	Source	Destination	Protocol	Length	Info
6	2021-09-23 20:12:47.432660	36.152.44.96	172.20.10.5	HTTP	326	HTTP/1.1 200 OK
24	2021-09-23 20:12:49.987993	112.29.146.166	172.20.10.5	HTTP/J…	507	HTTP/1.1 200 OK , JavaS
58	2021-09-23 20:12:53.266672	104.78.88.101	172.20.10.5	HTTP	392	HTTP/1.1 200 OK
953	2021-09-23 20:13:00.309846	112.17.1.12	172.20.10.5	HTTP	685	HTTP/1.1 200 OK (text/
1760	2021-09-23 20:13:02.098189	111.30.187.177	172.20.10.5	HTTP	299	HTTP/1.1 200 OK (text/
2129	2021-09-23 20:13:03.108272	111.30.187.177	172.20.10.5	HTTP	190	HTTP/1.1 200 OK (text/
2279	2021-09-23 20:13:03.599068	36.155.202.140	172.20.10.5	HTTP	302	HTTP/1.1 200 OK (text/
2290	2021-09-23 20:13:03.618853	111.30.187.177	172.20.10.5	HTTP	291	HTTP/1.1 200 OK (text/
2301	2021-09-23 20:13:03.719730	36.155.202.140	172.20.10.5	HTTP	293	HTTP/1.1 200 OK (text/
2305	2021-09-23 20:13:03.776571	111.30.187.177	172.20.10.5	HTTP	1166	HTTP/1.1 200 OK (text/
2328	2021-09-23 20:13:04.318880	111.30.187.177	172.20.10.5	HTTP	829	HTTP/1.1 200 OK (text/
2330	2021-09-23 20:13:04.349388	111.30.187.177	172.20.10.5	HTTP	990	HTTP/1.1 200 OK (text/
2390	2021-09-23 20:13:06.272119	111.30.187.177	172.20.10.5	HTTP	166	HTTP/1.1 200 OK (text/

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?

```
    TCP segment data (112 bytes)
  [4 Reassembled TCP Segments (4192 bytes): #2387(1360), #2388(1360), #2389(1360), #2390(112)]
    [Frame: 2387, payload: 0-1359 (1360 bytes)]
    [Frame: 2388, payload: 1360-2719 (1360 bytes)]
    [Frame: 2389, payload: 2720-4079 (1360 bytes)]
    [Frame: 2390, payload: 4080-4191 (112 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4192]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a5365727665723a20687474707366320d0a436f…]
  Hypertext Transfer Protocol
```

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?

http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
172	2021-09-23 21:15:00.968950	172.20.10.5	128.119.245.12	HTTP	546	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
180	2021-09-23 21:15:01.352905	172.20.10.5	128.119.245.12	HTTP	478	GET /pearson.png HTTP/1.1
202	2021-09-23 21:15:01.778970	172.20.10.5	178.79.137.164	HTTP	485	GET /8E_cover_small.jpg HTTP/1.1

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.

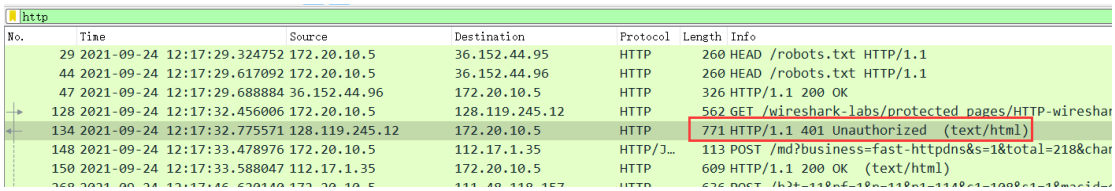
http.request.method=="GET"

No.	Time	Source	Destination	Protocol	Length	Info
172	2021-09-23 21:15:00.968950	172.20.10.5	128.119.245.12	HTTP	546	GET /wireshark-labs/HTTP-wireshark-
180	2021-09-23 21:15:01.352905	172.20.10.5	128.119.245.12	HTTP	478	GET /pearson.png HTTP/1.1
202	2021-09-23 21:15:01.778970	172.20.10.5	178.79.137.164	HTTP	485	GET /8E_cover_small.jpg HTTP/1.1

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

五、HTTP Authentication

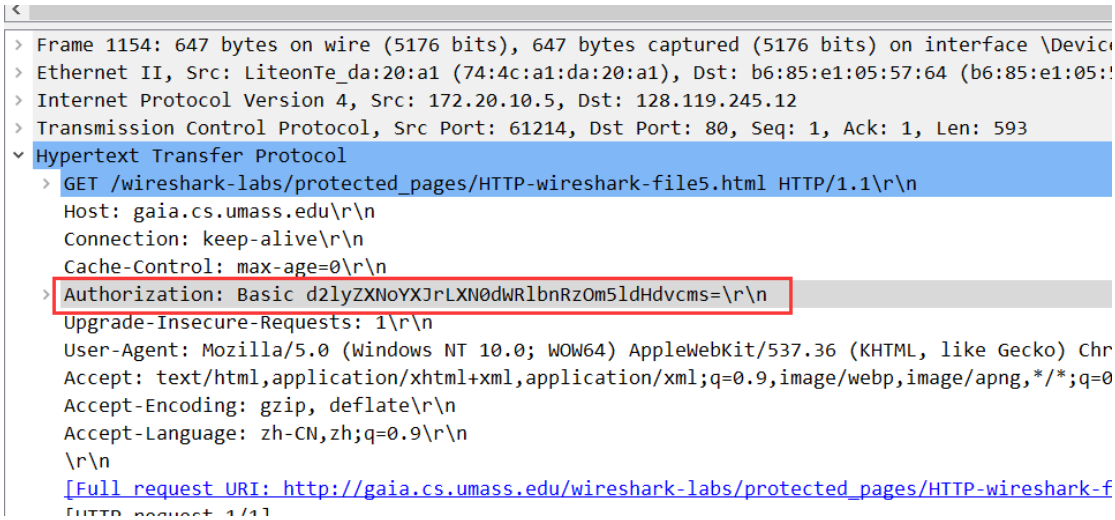
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?



No.	Time	Source	Destination	Protocol	Length	Info
29	2021-09-24 12:17:29.324752	172.20.10.5	36.152.44.95	HTTP	260	HEAD /robots.txt HTTP/1.1
44	2021-09-24 12:17:29.617092	172.20.10.5	36.152.44.96	HTTP	260	HEAD /robots.txt HTTP/1.1
47	2021-09-24 12:17:29.688884	36.152.44.96	172.20.10.5	HTTP	326	HTTP/1.1 200 OK
128	2021-09-24 12:17:32.456006	172.20.10.5	128.119.245.12	HTTP	562	GET /wireshark-labs/protected_pages/HTTP-wireshar
134	2021-09-24 12:17:32.775571	128.119.245.12	172.20.10.5	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
148	2021-09-24 12:17:33.478976	172.20.10.5	112.17.1.35	HTTP/J…	113	POST /md?business=fast-httpdns&s=1&total=218&char
150	2021-09-24 12:17:33.588047	112.17.1.35	172.20.10.5	HTTP	609	HTTP/1.1 200 OK (text/html)

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?



```
> Frame 1154: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits) on interface \Devic
> Ethernet II, Src: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1), Dst: b6:85:e1:05:57:64 (b6:85:e1:05:
> Internet Protocol Version 4, Src: 172.20.10.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 61214, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: zh-CN,zh;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-f
```

Authorization:Basic d2lyZXNoYXJrLXN0dwRlbnRzOm51dHdvcms=