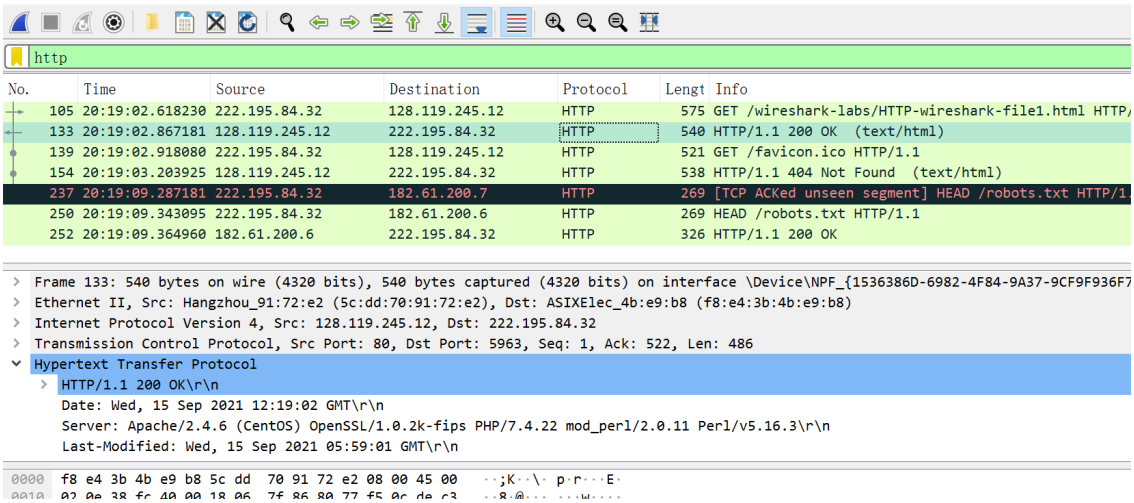
实验二

Wireshark Lab：HTTP

阅读实验文档，按照文档进行各个部分的操作。

1. **The Basic HTTP GET/response interaction**

   按照指示操作，打开wireshark，输入http筛选，等待一会开始捕捉，打开网页http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html，停止捕捉，在wireshark中找到对应部分，如图



   根据捕捉到的结果回答问题：

   1. browser version: 1.1　sever version: 1.1
   2. 在GET中的Hypertext Transfer Protocol下的Accept-Language找到

      Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
   3. 我的电脑地址：222.195.84.32　server地址：128.119.245.12

      在Internet Protocol中找到
   4. Status code在回复的Hypertext Transfer Protocol中找到

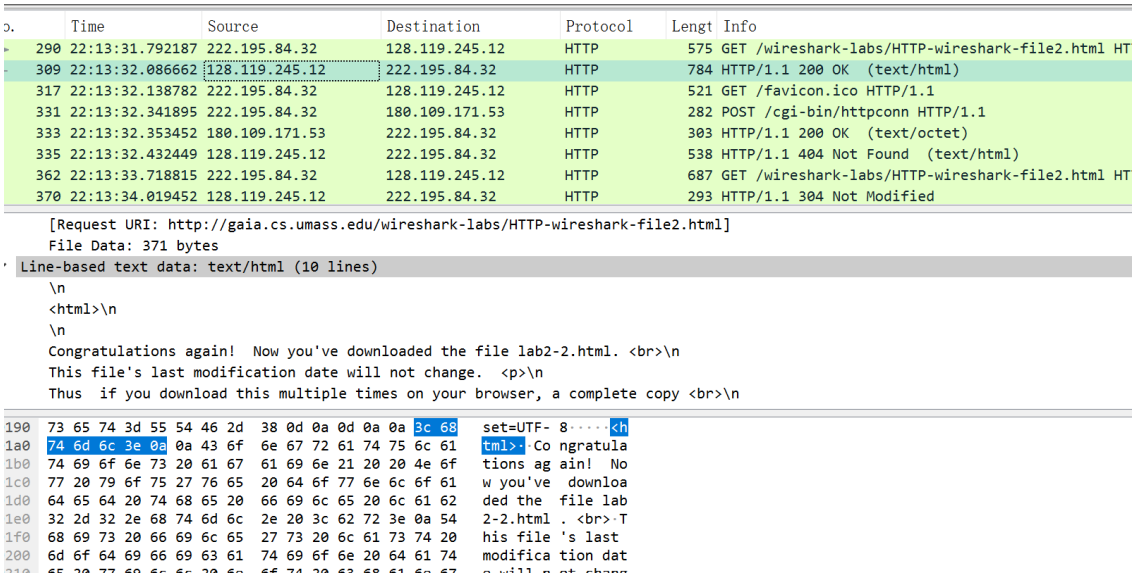
      HTTP/1.1 200 OK\r\n
   5. Last-Modified: Wed, 15 Sep 2021 05:59:01 GMT\r\n
   6. 在回复的Hypertext Transfer Protocol的Content-Length中：

      Content-Length: 128\r\n

      [Content length: 128]
   7. 有，例如：server

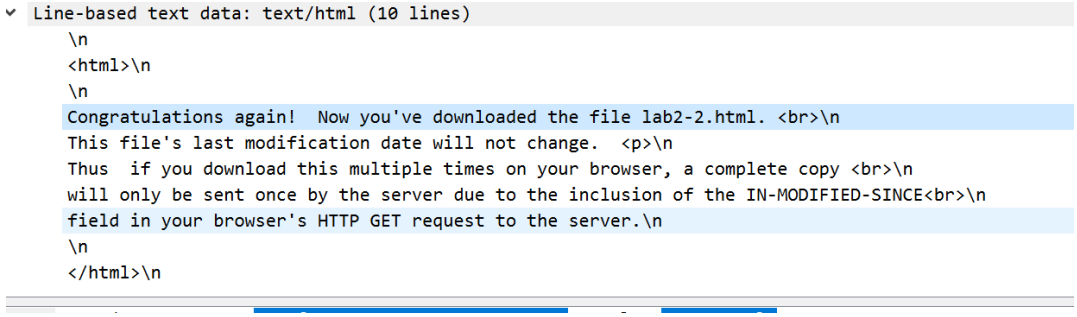
2. **The HTTP CONDITIONAL GET/response interaction**

按照操作清楚缓存后重新进入网站http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html，在刷新一次，在wireshark中成功抓包：



回答问题：

8. 并没有发现
9. 有，在Line-based text data：text/html（10 lines）中



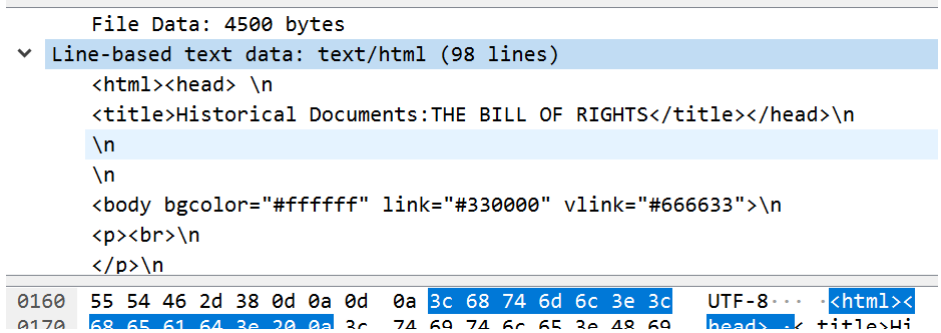
10. 有，显示If-Modified-Since: Wed, 15 Sep 2021 05:59:01 GMT\r\n
11. 回复HTTP/1.1 304 Not Modified\r\n，因为这个页面的缓存还在，文件并没有改变，所以就没有回复内容，直接使用缓存就行

3. **Retrieving Long Documents**

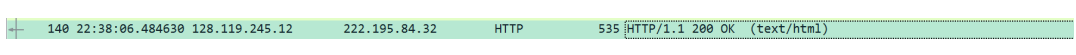
类似2中的操作，清除缓存，进入网站http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html并捕获。

回答问题

12. 只有一个GET request，含有GET message for the Bill or Rights的：



13. 包含相应的包：



14. status code and phrase：200 OK

15. 需要4个

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 222.195.84.32
> Transmission Control Protocol, Src Port: 80, Dst Port: 6768, Seq: 4381, Ack: 522,
v [4 Reassembled TCP Segments (4861 bytes): #136(1460), #139(1460), #137(1460), #140
    [Frame: 136, payload: 0-1459 (1460 bytes)]
    [Frame: 139, payload: 1460-2919 (1460 bytes)]
    [Frame: 137, payload: 2920-4379 (1460 bytes)]
    [Frame: 140, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
```

```
0160  55 54 46 2d 38 0d 0a 0d  0a 3c 68 74 6d 6c 3e 3c   UTF-8··· ·<html><
0170  68 65 61 64 3e 20 0a 3c  74 69 74 6c 65 3e 48 69   head> ·< title>Hi
0180  73 74 6f 72 69 63 61 6c  20 44 6f 63 75 6d 65 6e   storical  Documen
```

4. **HTML Documents with Embedded Objects**

和上面操作类似，清除缓存，进入网站http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html，捕获。

回答问题：

16.

No.	Time	Source	Destination	Protocol	Lengt	Info
63	22:54:10.604404	222.195.84.32	128.119.245.12	HTTP	575	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
76	22:54:10.897932	128.119.245.12	222.195.84.32	HTTP	1355	HTTP/1.1 200 OK (text/html)
77	22:54:10.927432	222.195.84.32	128.119.245.12	HTTP	521	GET /pearson.png HTTP/1.1
84	22:54:11.207557	128.119.245.12	222.195.84.32	HTTP	745	HTTP/1.1 200 OK (PNG)
88	22:54:11.389047	222.195.84.32	178.79.137.164	HTTP	488	GET /8E_cover_small.jpg HTTP/1.1
92	22:54:11.845996	178.79.137.164	222.195.84.32	HTTP	225	HTTP/1.1 301 Moved Permanently

发送了三个HTTP GET请求，地址是128.119.245.12 128.119.145.12 178.79.137.164

17. 根据捕捉到的结果，应该是串行下载，当pearson.png请求并收到后，发送了BE_cover_small.jpg的请求

	77	22:54:10.927432	222.195.84.32	128.119.245.12	HTTP	521 GET /pearson.png HTTP/1.1
	84	22:54:11.207557	128.119.245.12	222.195.84.32	HTTP	745 HTTP/1.1 200 OK (PNG)
	88	22:54:11.389047	222.195.84.32	178.79.137.164	HTTP	488 GET /8E_cover_small.jpg HTTP/1.1
	92	22:54:11.845996	178.79.137.164	222.195.84.32	HTTP	225 HTTP/1.1 301 Moved Permanently

5. **HTTP Authentication**

类似的，清楚缓存，进入网站http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html，输入信息，成功抓包。

http

No.	Time	Source	Destination	Protocol	Lengt	Info
60	23:08:29.077375	222.195.84.32	128.119.245.12	HTTP	591	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
81	23:08:29.398670	128.119.245.12	222.195.84.32	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
107	23:08:40.800813	222.195.84.32	128.119.245.12	HTTP	676	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
110	23:08:41.103603	128.119.245.12	222.195.84.32	HTTP	544	HTTP/1.1 200 OK (text/html)

回答问题：

18. response：HTTP/1.1 401 Unauthorized (text/html)

19. 多了Authorization部分

```
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
v   Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
        Credentials: wireshark-students:network
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
```