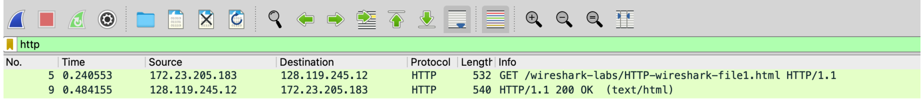
The Basic HTTP GET/response interaction

here is my result:



http

No.	Time	Source	Destination	Protocol	Length	Info
5	0.240553	172.23.205.183	128.119.245.12	HTTP	532	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
9	0.484155	128.119.245.12	172.23.205.183	HTTP	540	HTTP/1.1 200 OK (text/html)

Figure 1: result

we can see there are 2 HTTP messages: * HTTP GET * HTTP response OK

here is get message:

```
Frame 5: 532 bytes on wire (4256 bits), 532 bytes captured (4256 bits) on interface en0, id
Ethernet II, Src: Apple_65:60:2a (cc:08:fa:65:60:2a), Dst: NewH3CTe_aa:3e:01 (fc:60:9b:aa:3e
Internet Protocol Version 4, Src: 172.23.205.183, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 55540, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
            [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, I
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
    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/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 9]
```

here is http response

```
Frame 9: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en0, id
Ethernet II, Src: NewH3CTe_aa:3e:01 (fc:60:9b:aa:3e:01), Dst: Apple_65:60:2a (cc:08:fa:65:60
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.23.205.183
Transmission Control Protocol, Src Port: 80, Dst Port: 55540, Seq: 1, Ack: 479, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 27 Oct 2023 04:24:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.
    Last-Modified: Thu, 26 Oct 2023 05:59:02 GMT\r\n
    ETag: "80-6089844c7567c"\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-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.243602000 seconds]
    [Request in frame: 5]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

Q&A

Q1

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

```
GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
```

Q2

> What languages (if any) does your browser indicate that it can accept to the server? my broswer accept zh-CN(Chinese)

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
```

Q3

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

- my IP:172.23.205.183
- gaia.cs.umass.edu server IP:28.119.245.12

```
Internet Protocol Version 4, Src: 172.23.205.183, Dst: 128.119.245.12
```

Q4

> What is the status code returned from the server to your browser? 200

```
HTTP/1.1 200 OK\r\n
```

Q5

> When was the HTML file that you are retrieving last modified at the server? Thu, 26 Oct 2023 05:59:02 GMT

```
Last-Modified: Thu, 26 Oct 2023 05:59:02 GMT\r\n
```

Q6

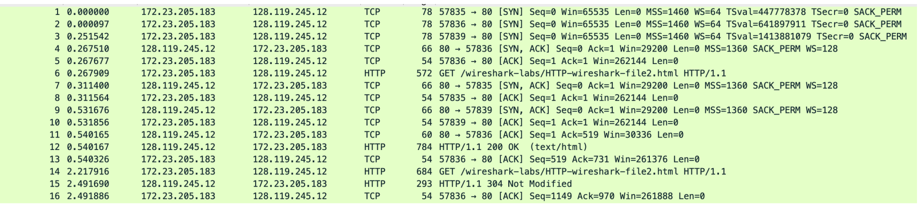
> How many bytes of content are being returned to your browser? 540 bytes

```
Frame 9: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface en0, id
```

Q7

> 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?

The HTTP CONDITIONAL GET/response interaction



```
 1 0.000000   172.23.205.183   128.119.245.12   TCP     78 57835 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=447778378 TSecr=0 SACK_PERM
 2 0.000097   172.23.205.183   128.119.245.12   TCP     78 57836 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=641897911 TSecr=0 SACK_PERM
 3 0.251542   172.23.205.183   128.119.245.12   TCP     78 57839 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=1413881079 TSecr=0 SACK_PERM
 4 0.267510   128.119.245.12   172.23.205.183   TCP     66 80 → 57836 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM WS=128
 5 0.267677   172.23.205.183   128.119.245.12   TCP     54 57836 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 6 0.267909   172.23.205.183   128.119.245.12   HTTP   572 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 7 0.311400   128.119.245.12   172.23.205.183   TCP     66 80 → 57835 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM WS=128
 8 0.311564   172.23.205.183   128.119.245.12   TCP     54 57835 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
 9 0.531676   128.119.245.12   172.23.205.183   TCP     66 80 → 57839 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM WS=128
10 0.531856   172.23.205.183   128.119.245.12   TCP     54 57839 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
11 0.540165   128.119.245.12   172.23.205.183   TCP     60 80 → 57836 [ACK] Seq=1 Ack=519 Win=30336 Len=0
12 0.540167   128.119.245.12   172.23.205.183   HTTP   784 HTTP/1.1 200 OK  (text/html)
13 0.540326   172.23.205.183   128.119.245.12   TCP     54 57836 → 80 [ACK] Seq=519 Ack=731 Win=261376 Len=0
14 2.217916   172.23.205.183   128.119.245.12   HTTP   684 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
15 2.491690   128.119.245.12   172.23.205.183   HTTP   293 HTTP/1.1 304 Not Modified
16 2.491886   172.23.205.183   128.119.245.12   TCP     54 57836 → 80 [ACK] Seq=1149 Ack=970 Win=261888 Len=0
```

Figure 2: Alt text

Q8

> 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 ## Q9 Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

I think server explicitly return the contents of the file, since the length of the response is 730

```
Transmission Control Protocol, Src Port: 80, Dst Port: 57836, Seq: 1, Ack: 519, Len: 730
```

Q10

> 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 and the following information is time I send previous GET request.

```
If-Modified-Since: Fri, 27 Oct 2023 05:59:02 GMT\r\n
```

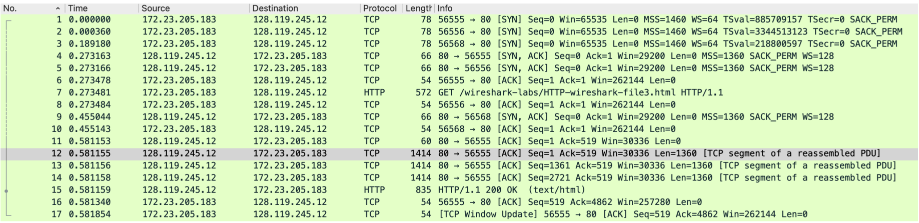
Q11

> 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

status code is `[HTTP/1.1 304 Not Modified\r\n]` and server not explicitly returnt he content since the length of HTTP response is 239, which is less than 730

```
[HTTP/1.1 304 Not Modified\r\n]
...
Transmission Control Protocol, Src Port: 80, Dst Port: 57836, Seq: 731, Ack: 1149, Len: 239
```

Retrieving Long Documents



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.23.205.183	128.119.245.12	TCP	78	56555 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=885709157 TSecr=0 SACK_PERM
2	0.000360	172.23.205.183	128.119.245.12	TCP	78	56556 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3344513123 TSecr=0 SACK_PERM
3	0.189180	172.23.205.183	128.119.245.12	TCP	78	56568 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=218800597 TSecr=0 SACK_PERM
4	0.273163	128.119.245.12	172.23.205.183	TCP	66	80 → 56555 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM WS=128
5	0.273166	128.119.245.12	172.23.205.183	TCP	66	80 → 56556 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM WS=128
6	0.273478	172.23.205.183	128.119.245.12	TCP	54	56555 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
7	0.273481	172.23.205.183	128.119.245.12	HTTP	572	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
8	0.273484	172.23.205.183	128.119.245.12	TCP	54	56556 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
9	0.455044	128.119.245.12	172.23.205.183	TCP	66	80 → 56568 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1360 SACK_PERM WS=128
10	0.455143	172.23.205.183	128.119.245.12	TCP	54	56568 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
11	0.581153	128.119.245.12	172.23.205.183	TCP	60	80 → 56555 [ACK] Seq=1 Ack=519 Win=30336 Len=0
12	0.581155	128.119.245.12	172.23.205.183	TCP	1414	80 → 56555 [ACK] Seq=1 Ack=519 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
13	0.581156	128.119.245.12	172.23.205.183	TCP	1414	80 → 56555 [ACK] Seq=1361 Ack=519 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
14	0.581158	128.119.245.12	172.23.205.183	TCP	1414	80 → 56555 [ACK] Seq=2721 Ack=519 Win=30336 Len=1360 [TCP segment of a reassembled PDU]
15	0.581159	128.119.245.12	172.23.205.183	HTTP	835	HTTP/1.1 200 OK (text/html)
16	0.581340	172.23.205.183	128.119.245.12	TCP	54	56555 → 80 [ACK] Seq=519 Ack=4862 Win=257280 Len=0
17	0.581854	172.23.205.183	128.119.245.12	TCP	54	[TCP Window Update] 56555 → 80 [ACK] Seq=519 Ack=4862 Win=262144 Len=0

Q12 >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? * 1 HTTP GET request * packet number 7

Q13

> Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request? packet number 12,13,14,15

```
[4 Reassembled TCP Segments (4861 bytes): #12(1360), #13(1360), #14(1360), #15(781)]
    [Frame: 12, payload: 0-1359 (1360 bytes)]
    [Frame: 13, payload: 1360-2719 (1360 bytes)]
    [Frame: 14, payload: 2720-4079 (1360 bytes)]
    [Frame: 15, payload: 4080-4860 (781 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203237204f6
```

Q14

What is the status code and phrase in the response? 200 OK

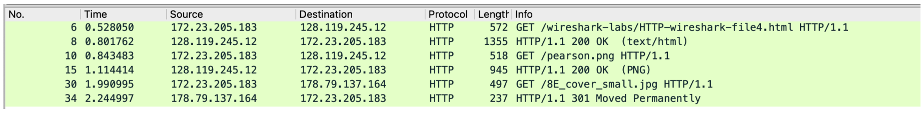
```
HTTP/1.1 200 OK\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
```

Q15

How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? 4

```
[4 Reassembled TCP Segments (4861 bytes): #12(1360), #13(1360), #14(1360), #15(781)]
    [Frame: 12, payload: 0-1359 (1360 bytes)]
    [Frame: 13, payload: 1360-2719 (1360 bytes)]
    [Frame: 14, payload: 2720-4079 (1360 bytes)]
    [Frame: 15, payload: 4080-4860 (781 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204672692c203237204f6
```

HTML Documents with Embedded Objects



No.	Time	Source	Destination	Protocol	Length	Info
6	0.528050	172.23.205.183	128.119.245.12	HTTP	572	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
8	0.801762	128.119.245.12	172.23.205.183	HTTP	1355	HTTP/1.1 200 OK (text/html)
10	0.843483	172.23.205.183	128.119.245.12	HTTP	518	GET /pearson.png HTTP/1.1
15	1.114414	128.119.245.12	172.23.205.183	HTTP	945	HTTP/1.1 200 OK (PNG)
30	1.990995	172.23.205.183	178.79.137.164	HTTP	497	GET /8E_cover_small.jpg HTTP/1.1
34	2.244997	178.79.137.164	172.23.205.183	HTTP	237	HTTP/1.1 301 Moved Permanently

Figure 3: Alt text

Q16

> How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent? 3 HTTP GET request and they are send to * `Host: gaia.cs.umass.edu\r\n` * `Host: gaia.cs.umass.edu\r\n` * `Host: kurose.cslash.net\r\n`

This is slightly different from the pdf description of v8.0, the cover's src is changed from`caite.cs.umass.edu`to`kurose.cslash.net`.

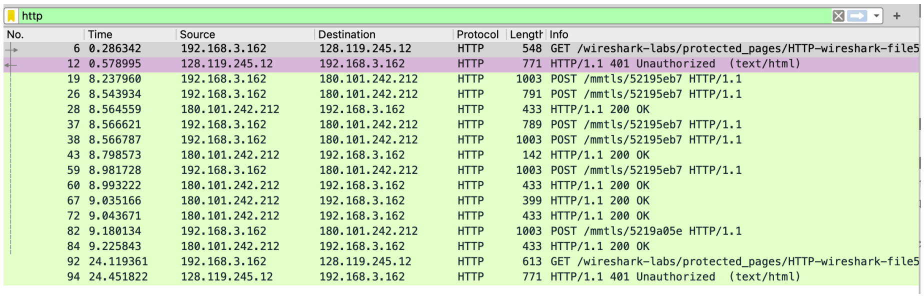
here is HTML source code:

```
<!-- publisher's logo  -->
<img src="http://gaia.cs.umass.edu/pearson.png" width="140" height="82">
<!-- cover  -->
<img src="http://kurose.cslash.net/8E_cover_small.jpg" width="168" height="220">
```

Q17

> Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain. I guess browser downloaded the two images serially(but not quite sure), for the reasons that as for time displayed by wireshark, the GET request were not sent at same time

HTTP Authentication



http

No.	Time	Source	Destination	Protocol	Length	Info
6	0.286342	192.168.3.162	128.119.245.12	HTTP	548	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5
12	0.578995	128.119.245.12	192.168.3.162	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
19	8.237960	192.168.3.162	180.101.242.212	HTTP	1003	POST /mmtls/52195eb7 HTTP/1.1
26	8.543934	192.168.3.162	180.101.242.212	HTTP	791	POST /mmtls/52195eb7 HTTP/1.1
28	8.564559	180.101.242.212	192.168.3.162	HTTP	433	HTTP/1.1 200 OK
37	8.566621	192.168.3.162	180.101.242.212	HTTP	789	POST /mmtls/52195eb7 HTTP/1.1
38	8.566787	192.168.3.162	180.101.242.212	HTTP	1003	POST /mmtls/52195eb7 HTTP/1.1
43	8.798573	180.101.242.212	192.168.3.162	HTTP	142	HTTP/1.1 200 OK
59	8.981728	192.168.3.162	180.101.242.212	HTTP	1003	POST /mmtls/52195eb7 HTTP/1.1
60	8.993222	180.101.242.212	192.168.3.162	HTTP	433	HTTP/1.1 200 OK
67	9.035166	180.101.242.212	192.168.3.162	HTTP	399	HTTP/1.1 200 OK
72	9.043671	180.101.242.212	192.168.3.162	HTTP	433	HTTP/1.1 200 OK
82	9.180134	192.168.3.162	180.101.242.212	HTTP	1003	POST /mmtls/5219a05e HTTP/1.1
84	9.225843	180.101.242.212	192.168.3.162	HTTP	433	HTTP/1.1 200 OK
92	24.119361	192.168.3.162	128.119.245.12	HTTP	613	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5
94	24.451822	128.119.245.12	192.168.3.162	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)

Figure 4: Alt text

Q18

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

200OK

Q19

When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message? Authorization field

```
Authorization: Basic YWRtaW46MTIzNDU2\r\n
    Credentials: admin:123456
```