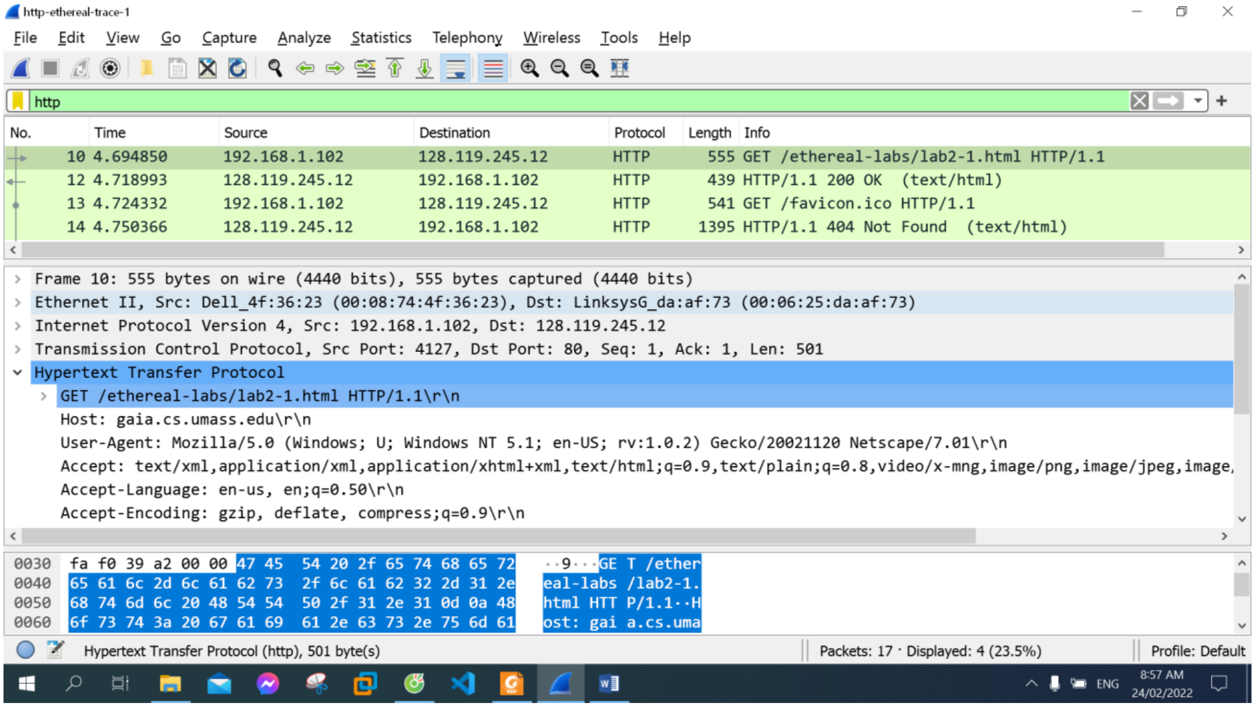
LAB 2A

Wireshark Lab: HTTP v8.0

Name: Hồ Đức Trí

Student No: 1912288

I/ The Basic HTTP GET/response interaction


http-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source          Destination     Protocol Length Info
   10 4.694850    192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-1.html HTTP/1.1
   12 4.718993    128.119.245.12  192.168.1.102   HTTP      439 HTTP/1.1 200 OK  (text/html)
   13 4.724332    192.168.1.102   128.119.245.12  HTTP      541 GET /favicon.ico HTTP/1.1
   14 4.750366    128.119.245.12  192.168.1.102   HTTP     1395 HTTP/1.1 404 Not Found  (text/html)
```

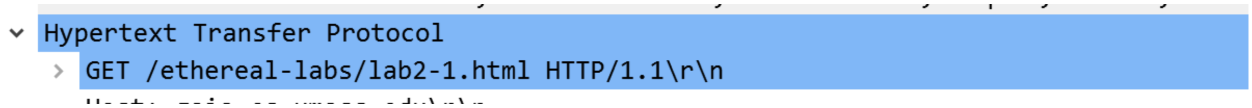
```
> Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
v Hypertext Transfer Protocol
  > GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image,
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
```

```
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 6c 61 62 32 2d 31 2e   eal-labs /lab2-1.
0050  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31 0d 0a 48   html HTT P/1.1··H
0060  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e 75 6d 61   ost: gai a.cs.uma
```

Hypertext Transfer Protocol (http), 501 byte(s)
Packets: 17 · Displayed: 4 (23.5%)
Profile: Default
ENG
8:57 AM
24/02/2022

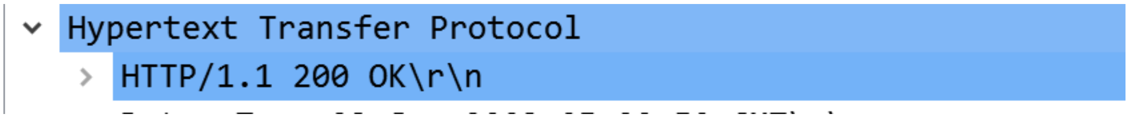
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running HTTP version 1.1:



```
v Hypertext Transfer Protocol
  > GET /ethereal-labs/lab2-1.html HTTP/1.1\r\n
```

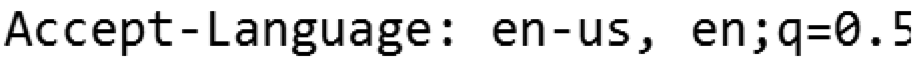
The server is running HTTP version 1.1:



```
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
```

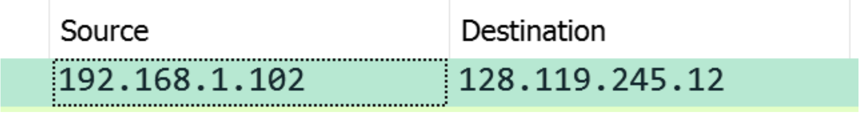
2. What languages (if any) does your browser indicate that it can accept to the server?

en - us



```
Accept-Language: en-us, en;q=0.5
```

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



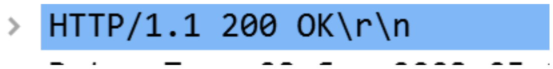
Source	Destination
192.168.1.102	128.119.245.12

Internet address of my computer 192.168.1.102

IP address gaia.cs.umass.edu server is 128.119.245.12

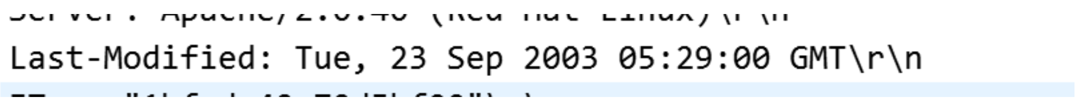
4. What is the status code returned from the server to your browser?

OK 200



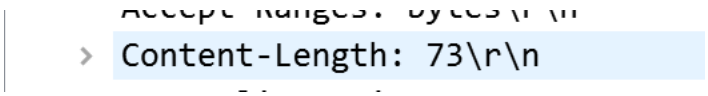
```
HTTP/1.1 200 OK\r\n
```

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



```
Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n
```

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



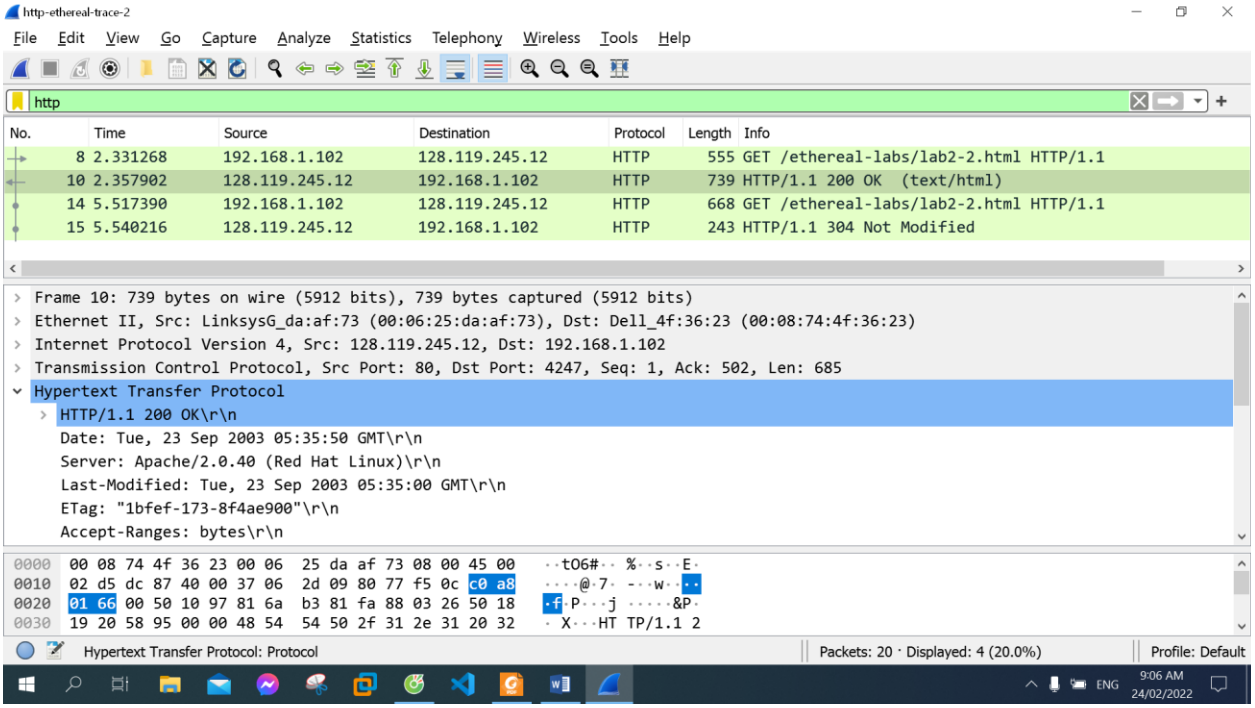
```
Content-Length: 73\r\n
```

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.

Date, Server, Last-Modified… in response message

II/ The HTTP CONDITIONAL GET/response interaction

The first GET message


http-ethereal-trace-2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Profile: Default
ENG
9:06 AM
24/02/2022

```
No.   Time        Source          Destination     Protocol  Length  Info
    8 2.331268    192.168.1.102   128.119.245.12  HTTP       555 GET /ethereal-labs/lab2-2.html HTTP/1.1
   10 2.357902    128.119.245.12  192.168.1.102   HTTP       739 HTTP/1.1 200 OK  (text/html)
   14 5.517390    192.168.1.102   128.119.245.12  HTTP       668 GET /ethereal-labs/lab2-2.html HTTP/1.1
   15 5.540216    128.119.245.12  192.168.1.102   HTTP       243 HTTP/1.1 304 Not Modified
```

```
> Frame 10: 739 bytes on wire (5912 bits), 739 bytes captured (5912 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 1, Ack: 502, Len: 685
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:35:50 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:35:00 GMT\r\n
    ETag: "1bfef-173-8f4ae900"\r\n
    Accept-Ranges: bytes\r\n
```

```
0000  00 08 74 4f 36 23 00 06  25 da af 73 08 00 45 00   ··tO6#·· %··s··E·
0010  02 d5 dc 87 40 00 37 06  2d 09 80 77 f5 0c c0 a8   ····@·7· -··w····
0020  01 66 00 50 10 97 81 6a  b3 81 fa 88 03 26 50 18   ·f·P···j ·····&P·
0030  19 20 58 95 00 00 48 54  54 50 2f 31 2e 31 20 32   · X···HT TP/1.1 2
```

```
Hypertext Transfer Protocol: Protocol          Packets: 20 · Displayed: 4 (20.0%)
```

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?

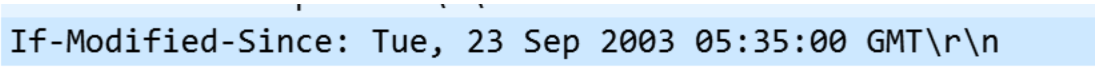
No

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

Yes. Because the Line-based text data in OK message responses to the GET message.

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?

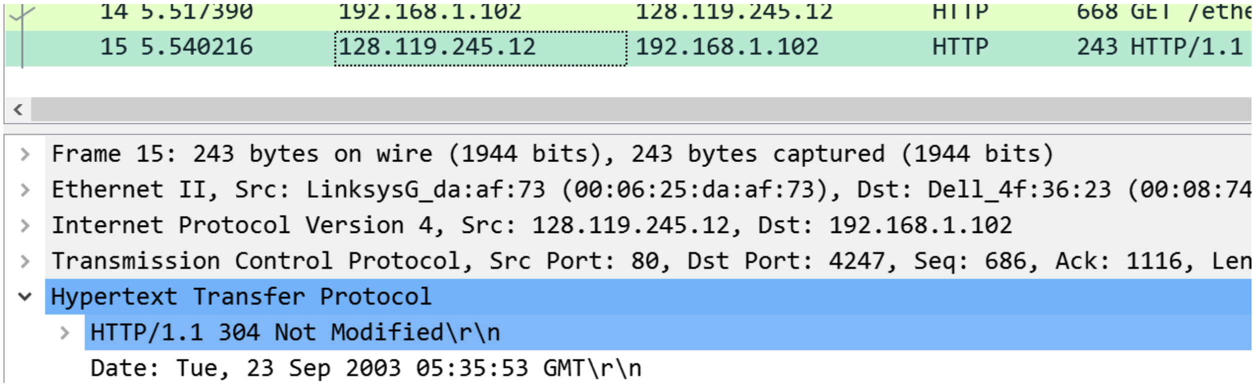
Yes.



```
If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
```

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.

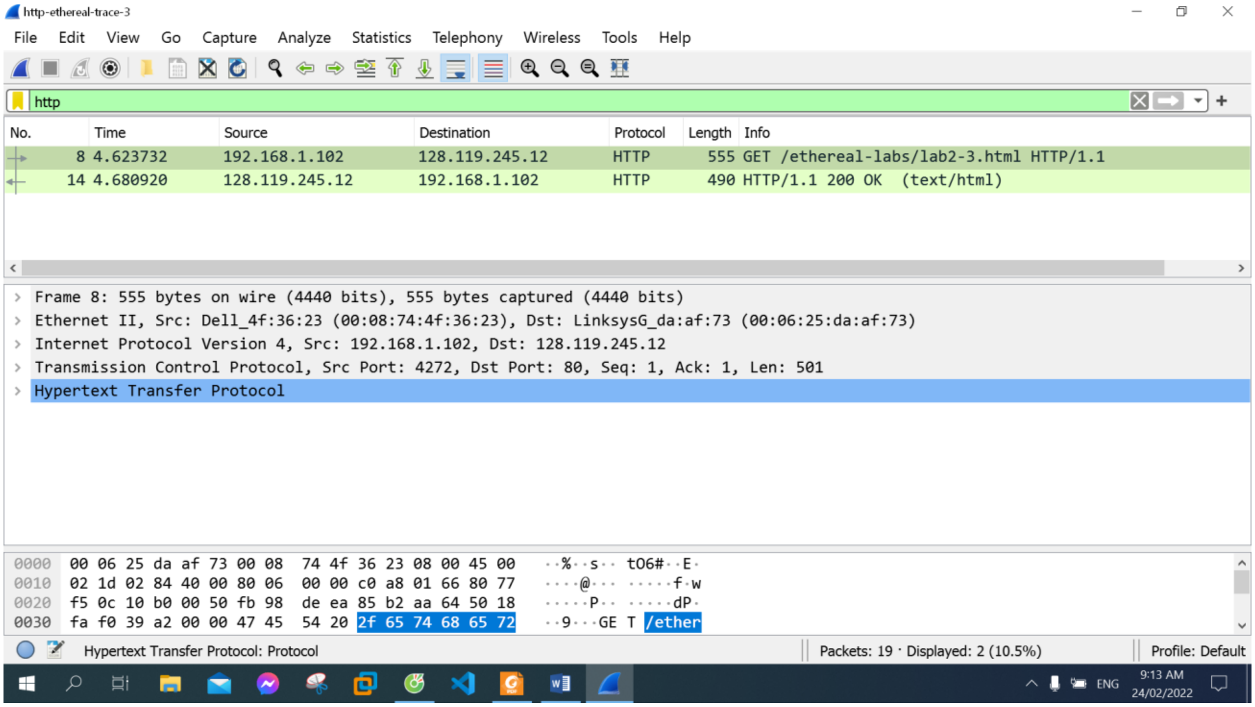


```
14 5.517390   192.168.1.102   128.119.245.12   HTTP   668 GET /ethe
15 5.540216   128.119.245.12  192.168.1.102    HTTP   243 HTTP/1.1
```

```
> Frame 15: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 4247, Seq: 686, Ack: 1116, Len
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n
```

No, the redirection response code server did not return the contents of the file. The HTTP 304 Not Modified client indicates that there is no need to retransmit the requested resources.

III/ Retrieving Long Documents



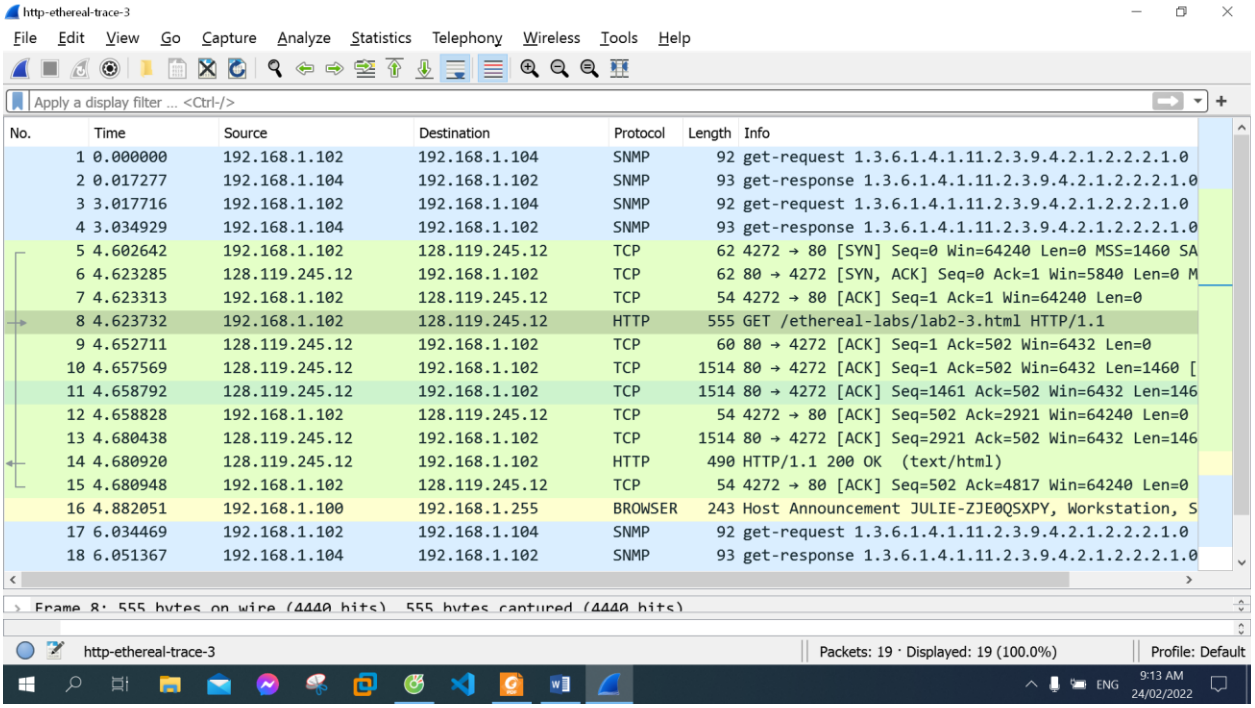
http-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.  Time      Source          Destination     Protocol Length Info
   8 4.623732  192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-3.html HTTP/1.1
  14 4.680920  128.119.245.12  192.168.1.102   HTTP      490 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4272, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
> Hypertext Transfer Protocol
```

```
0000  00 06 25 da af 73 00 08  74 4f 36 23 08 00 45 00   ··%··s·· tO6#··E·
0010  02 1d 02 84 40 00 80 06  00 00 c0 a8 01 66 80 77   ····@··· ·····f·w
0020  f5 0c 10 b0 00 50 fb 98  de ea 85 b2 aa 64 50 18   ·····P·· ·····dP·
0030  fa f0 39 a2 00 00 47 45  54 20 2f 65 74 68 65 72   ··9···GE T /ether
```

```
Hypertext Transfer Protocol: Protocol    Packets: 19 · Displayed: 2 (10.5%)    Profile: Default
```


http-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
http-ethereal-trace-3
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default
ENG
9:13 AM
24/02/2022

```
No.    Time      Source          Destination     Protocol Length Info
     1 0.000000  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
     2 0.017277  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
     3 3.017716  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
     4 3.034929  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
     5 4.602642  192.168.1.102   128.119.245.12  TCP        62 4272 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SA
     6 4.623285  128.119.245.12  192.168.1.102   TCP        62 80 → 4272 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
     7 4.623313  192.168.1.102   128.119.245.12  TCP        54 4272 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
     8 4.623732  192.168.1.102   128.119.245.12  HTTP      555 GET /ethereal-labs/lab2-3.html HTTP/1.1
     9 4.652711  128.119.245.12  192.168.1.102   TCP        60 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=0
    10 4.657569  128.119.245.12  192.168.1.102   TCP      1514 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=1460 [
    11 4.658792  128.119.245.12  192.168.1.102   TCP      1514 80 → 4272 [ACK] Seq=1461 Ack=502 Win=6432 Len=146
    12 4.658828  192.168.1.102   128.119.245.12  TCP        54 4272 → 80 [ACK] Seq=502 Ack=2921 Win=64240 Len=0
    13 4.680438  128.119.245.12  192.168.1.102   TCP      1514 80 → 4272 [ACK] Seq=2921 Ack=502 Win=6432 Len=146
    14 4.680920  128.119.245.12  192.168.1.102   HTTP      490 HTTP/1.1 200 OK  (text/html)
    15 4.680948  192.168.1.102   128.119.245.12  TCP        54 4272 → 80 [ACK] Seq=502 Ack=4817 Win=64240 Len=0
    16 4.882051  192.168.1.100   192.168.1.255   BROWSER   243 Host Announcement JULIE-ZJE0QSXPY, Workstation, S
    17 6.034469  192.168.1.102   192.168.1.104   SNMP       92 get-request 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0
    18 6.051367  192.168.1.104   192.168.1.102   SNMP       93 get-response 1.3.6.1.4.1.11.2.3.9.4.2.1.2.2.2.1.0

> Frame 8: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
```

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?

    1 messages.

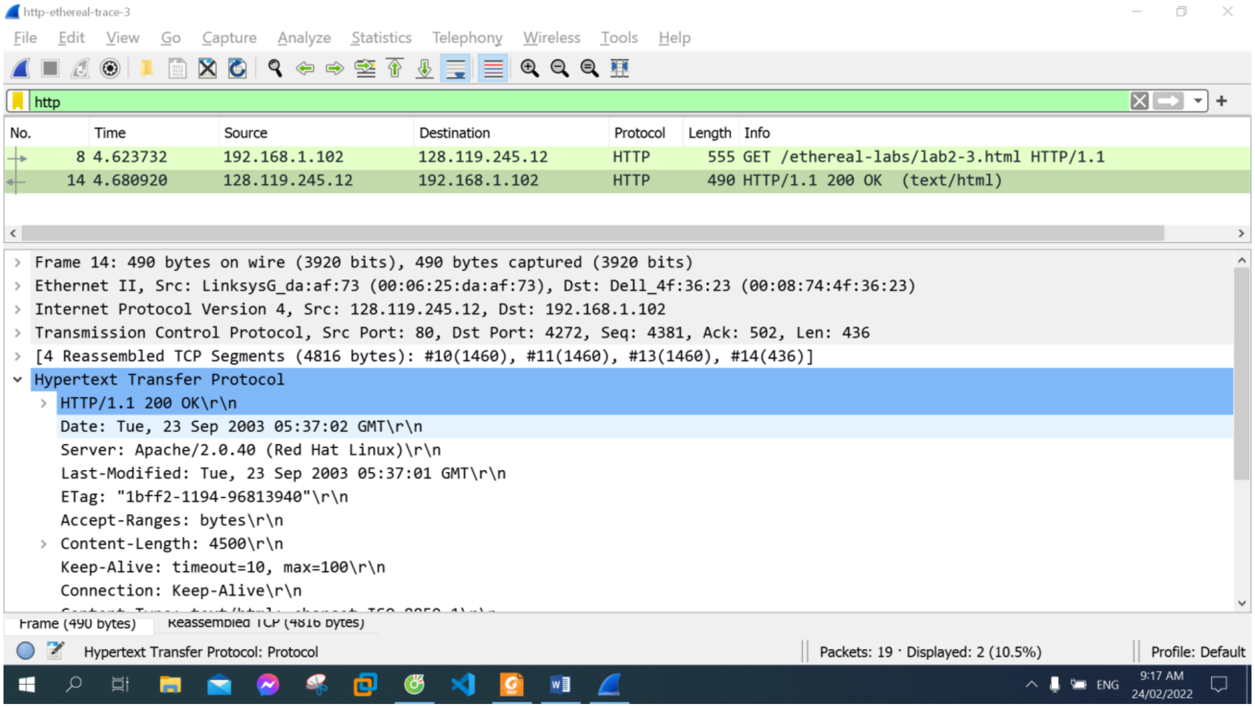
    Package number 8.

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

    Package number 14.

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

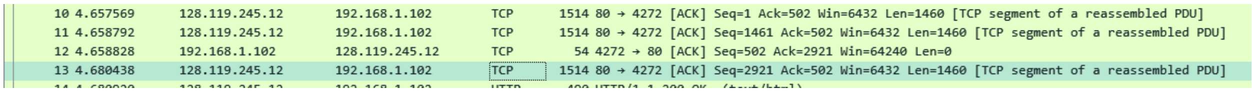
    200 OK.


http-ethereal-trace-3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Frame (490 bytes)
Reassembled TCP (4816 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 19 · Displayed: 2 (10.5%)
Profile: Default
ENG
9:17 AM
24/02/2022

```
No.  Time        Source          Destination     Protocol  Length  Info
  8  4.623732    192.168.1.102   128.119.245.12  HTTP        555   GET /ethereal-labs/lab2-3.html HTTP/1.1
 14  4.680920    128.119.245.12  192.168.1.102   HTTP        490   HTTP/1.1 200 OK  (text/html)
```

```
> Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 4272, Seq: 4381, Ack: 502, Len: 436
> [4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Tue, 23 Sep 2003 05:37:02 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
    Last-Modified: Tue, 23 Sep 2003 05:37:01 GMT\r\n
    ETag: "1bff2-1194-96813940"\r\n
    Accept-Ranges: bytes\r\n
  > Content-Length: 4500\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
```

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

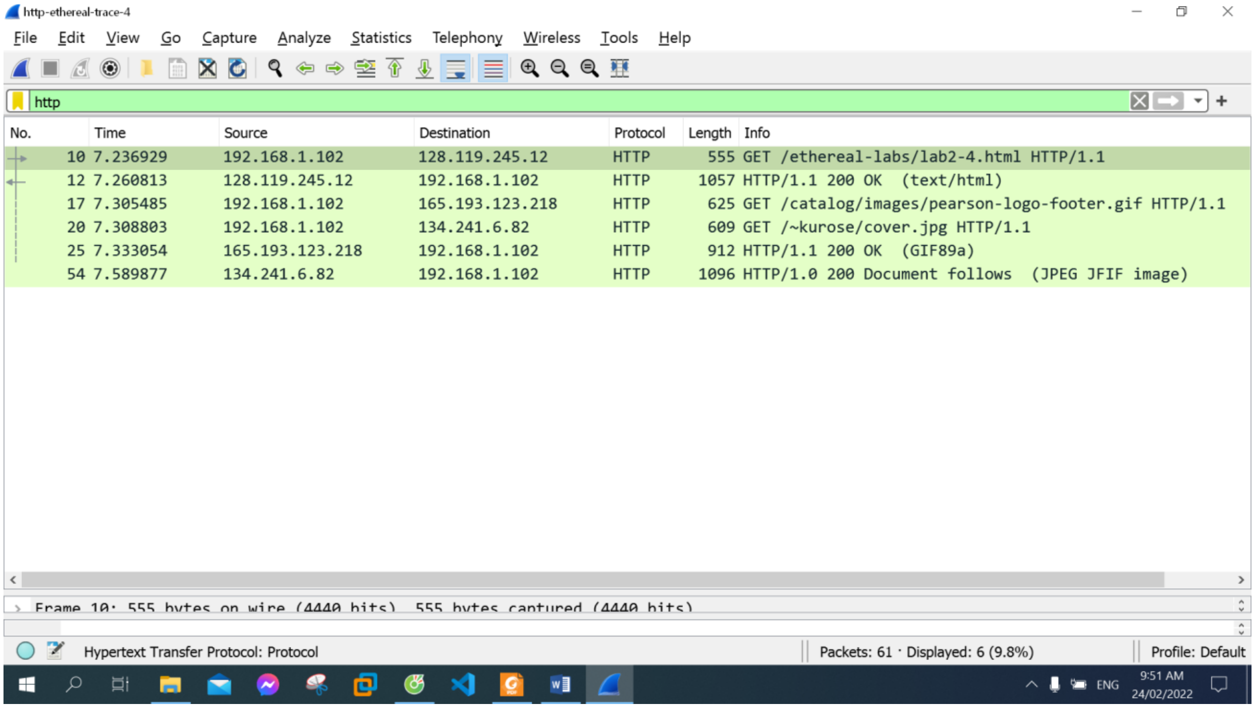


```
10 4.657569   128.119.245.12   192.168.1.102    TCP   1514 80 → 4272 [ACK] Seq=1 Ack=502 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
11 4.658792   128.119.245.12   192.168.1.102    TCP   1514 80 → 4272 [ACK] Seq=1461 Ack=502 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
12 4.658828   192.168.1.102    128.119.245.12   TCP     54 4272 → 80 [ACK] Seq=502 Ack=2921 Win=64240 Len=0
13 4.680438   128.119.245.12   192.168.1.102    TCP   1514 80 → 4272 [ACK] Seq=2921 Ack=502 Win=6432 Len=1460 [TCP segment of a reassembled PDU]
```

3 segments, package number 10, 11, 13.

IV/ 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-ethereal-trace-4
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
ENG
9:51 AM
24/02/2022

```
No.   Time       Source           Destination      Protocol  Length Info
   10 7.236929   192.168.1.102    128.119.245.12   HTTP       555 GET /ethereal-labs/lab2-4.html HTTP/1.1
   12 7.260813   128.119.245.12   192.168.1.102    HTTP      1057 HTTP/1.1 200 OK  (text/html)
   17 7.305485   192.168.1.102    165.193.123.218  HTTP       625 GET /catalog/images/pearson-logo-footer.gif HTTP/1.1
   20 7.308803   192.168.1.102    134.241.6.82     HTTP       609 GET /~kurose/cover.jpg HTTP/1.1
   25 7.333054   165.193.123.218  192.168.1.102    HTTP       912 HTTP/1.1 200 OK  (GIF89a)
   54 7.589877   134.241.6.82     192.168.1.102    HTTP      1096 HTTP/1.0 200 Document follows  (JPEG JFIF image)

> Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)

Hypertext Transfer Protocol: Protocol      Packets: 61 · Displayed: 6 (9.8%)      Profile: Default
```

3 messages.

128.119.245.12,

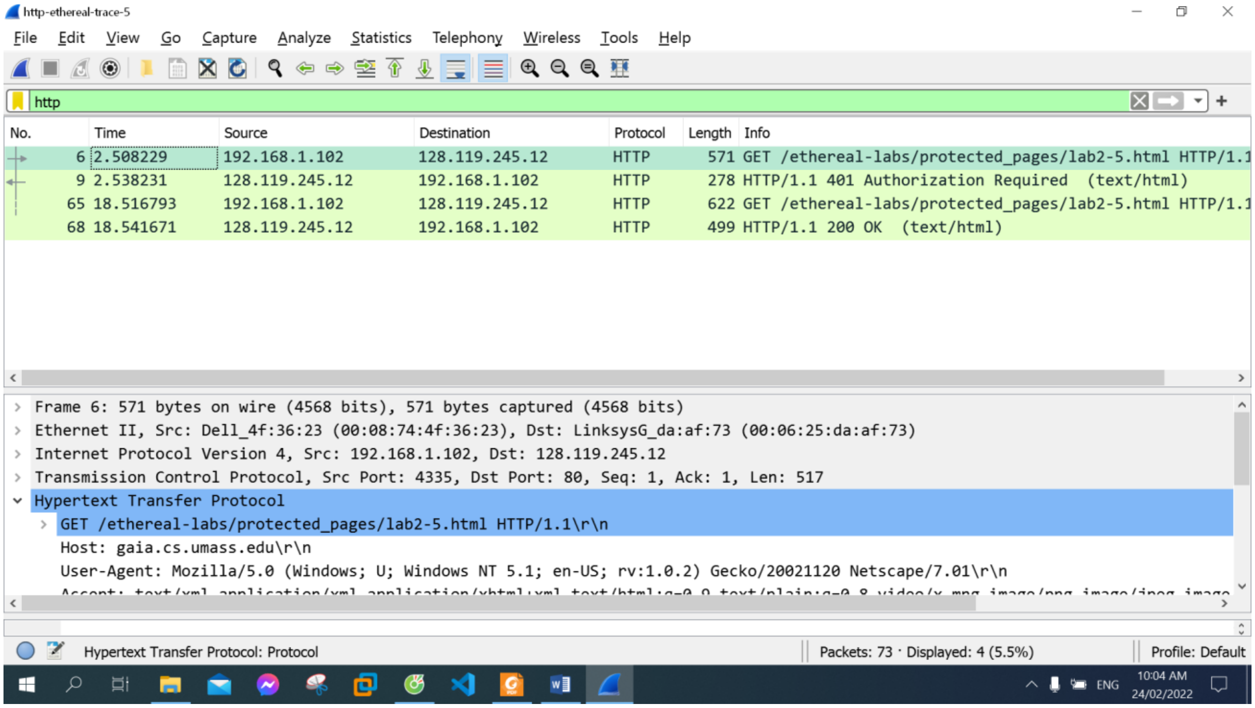
165.193.123.218,

134.241.6.82

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.

My browser downloaded the two images from the two web sites in parallel. Because the second image sends the request right after the first image's GET command

V/ HTTP Authentication



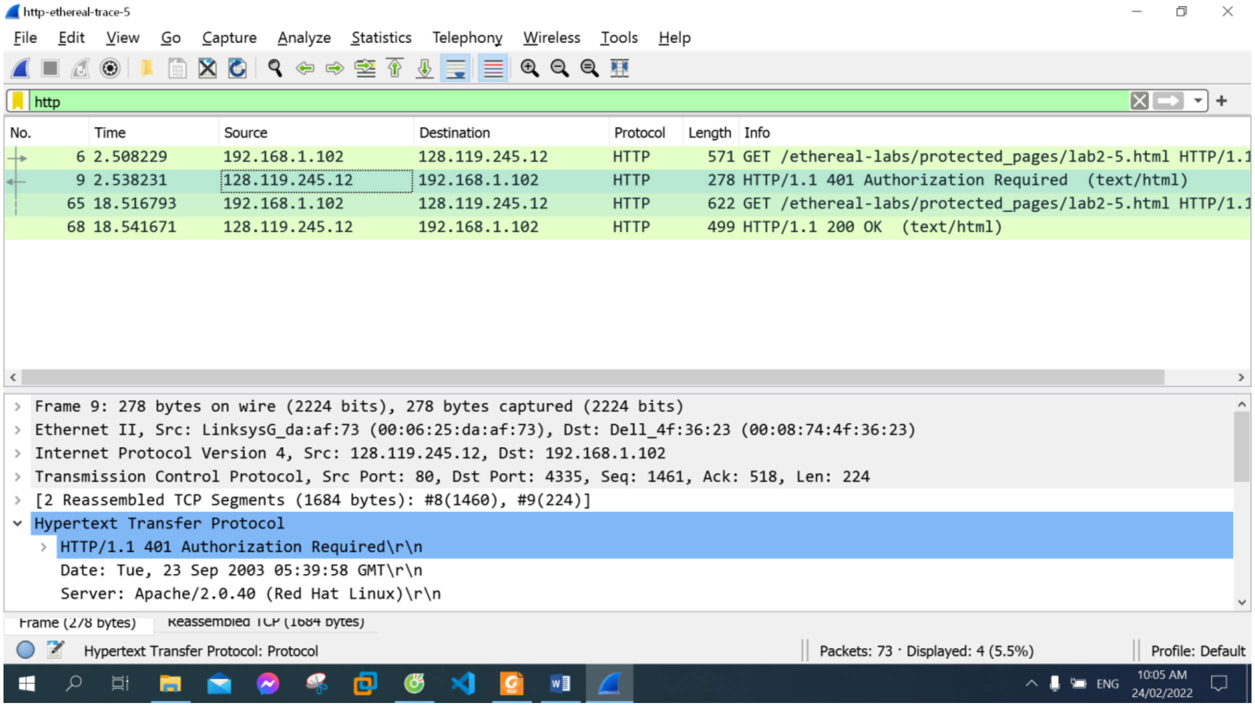
http-ethereal-trace-5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source          Destination     Protocol  Length  Info
  6   2.508229    192.168.1.102   128.119.245.12  HTTP      571     GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
  9   2.538231    128.119.245.12  192.168.1.102   HTTP      278     HTTP/1.1 401 Authorization Required  (text/html)
 65   18.516793   192.168.1.102   128.119.245.12  HTTP      622     GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
 68   18.541671   128.119.245.12  192.168.1.102   HTTP      499     HTTP/1.1 200 OK  (text/html)
```

```
> Frame 6: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 517
v Hypertext Transfer Protocol
  > GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image
```

Hypertext Transfer Protocol: Protocol
Packets: 73 · Displayed: 4 (5.5%)
Profile: Default
ENG
10:04 AM
24/02/2022

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



http-ethereal-trace-5
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time        Source          Destination     Protocol  Length  Info
  6   2.508229    192.168.1.102   128.119.245.12  HTTP      571     GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
  9   2.538231    128.119.245.12  192.168.1.102   HTTP      278     HTTP/1.1 401 Authorization Required  (text/html)
 65   18.516793   192.168.1.102   128.119.245.12  HTTP      622     GET /ethereal-labs/protected_pages/lab2-5.html HTTP/1.1
 68   18.541671   128.119.245.12  192.168.1.102   HTTP      499     HTTP/1.1 200 OK  (text/html)
```

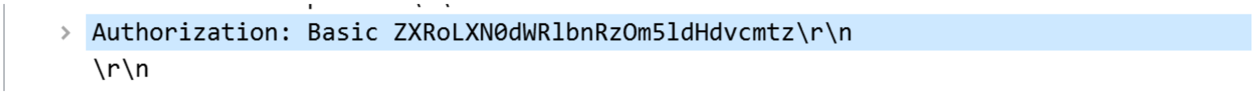
```
> Frame 9: 278 bytes on wire (2224 bits), 278 bytes captured (2224 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 1461, Ack: 518, Len: 224
> [2 Reassembled TCP Segments (1684 bytes): #8(1460), #9(224)]
v Hypertext Transfer Protocol
  > HTTP/1.1 401 Authorization Required\r\n
    Date: Tue, 23 Sep 2003 05:39:58 GMT\r\n
    Server: Apache/2.0.40 (Red Hat Linux)\r\n
```

Frame (278 bytes)
Reassembled TCP (1684 bytes)
Hypertext Transfer Protocol: Protocol
Packets: 73 · Displayed: 4 (5.5%)
Profile: Default
ENG
10:05 AM
24/02/2022

401 Authorization Required

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

The field Authorization



```
Authorization: Basic ZXRoLXN0dWRlbnRzOm5ldHdvcmtz\r\n
\r\n
```