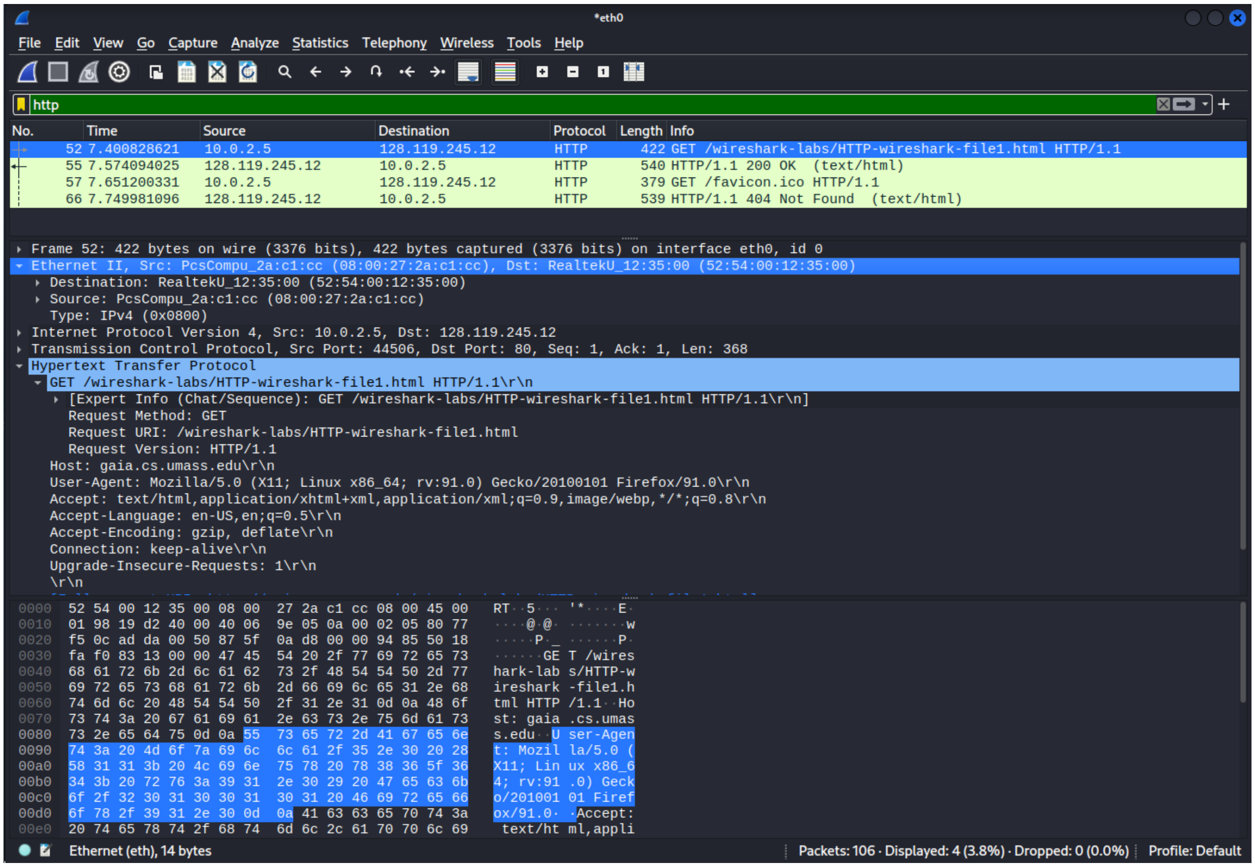
Group 8: Kevin Vo, Mason Godfrey, Thanh Le

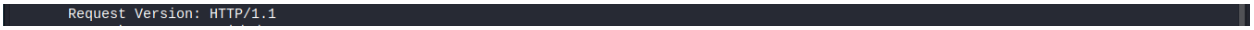
CS5500 - Lab 1: Network Capture with Wireshark

1. The Basic HTTP GET/response interaction


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.   Time          Source           Destination      Protocol  Length Info
   52 7.400828621   10.0.2.5         128.119.245.12   HTTP       422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   55 7.574094025   128.119.245.12   10.0.2.5         HTTP       540 HTTP/1.1 200 OK  (text/html)
   57 7.651200331   10.0.2.5         128.119.245.12   HTTP       379 GET /favicon.ico HTTP/1.1
   66 7.749981096   128.119.245.12   10.0.2.5         HTTP       539 HTTP/1.1 404 Not Found  (text/html)

Frame 52: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_2a:c1:cc (08:00:27:2a:c1:cc), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
  Destination: RealtekU_12:35:00 (52:54:00:12:35:00)
  Source: PcsCompu_2a:c1:cc (08:00:27:2a:c1:cc)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 44506, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
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\r\n]
    Request Method: GET
    Request URI: /wireshark-labs/HTTP-wireshark-file1.html
    Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n

0000  52 54 00 12 35 00 08 00  27 2a c1 cc 08 00 45 00   RT··5··· '*····E·
0010  01 98 19 d2 40 00 40 06  9e 05 0a 00 02 05 80 77   ····@·@· ·······w
0020  f5 0c ad da 00 50 87 5f  0a d8 00 00 94 85 50 18   ·····P·_ ······P·
0030  fa f0 83 13 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
0090  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
00a0  58 31 31 3b 20 4c 69 6e  75 78 20 78 38 36 5f 36   X11; Lin ux x86_6
00b0  34 3b 20 72 76 3a 39 31  2e 30 29 20 47 65 63 6b   4; rv:91 .0) Geck
00c0  6f 2f 32 30 31 30 30 31  30 31 20 46 69 72 65 66   o/201001 01 Firef
00d0  6f 78 2f 39 31 2e 30 0d  0a 41 63 63 65 70 74 3a   ox/91.0· ·Accept:
00e0  20 74 65 78 74 2f 68 74  6d 6c 2c 61 70 70 6c 69    text/ht ml,appli

Ethernet (eth), 14 bytes    Packets: 106 · Displayed: 4 (3.8%) · Dropped: 0 (0.0%)    Profile: Default
```

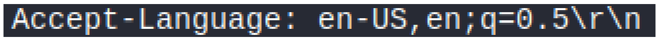
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?



```
    Request Version: HTTP/1.1
```

- Our browser is running HTTP version 1.1

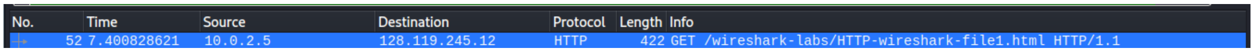
2. What languages (if any) does your browser indicate that it can accept to the server?



```
Accept-Language: en-US,en;q=0.5\r\n
```

- The language that our browser indicate that it can accept to the server is en-US.

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

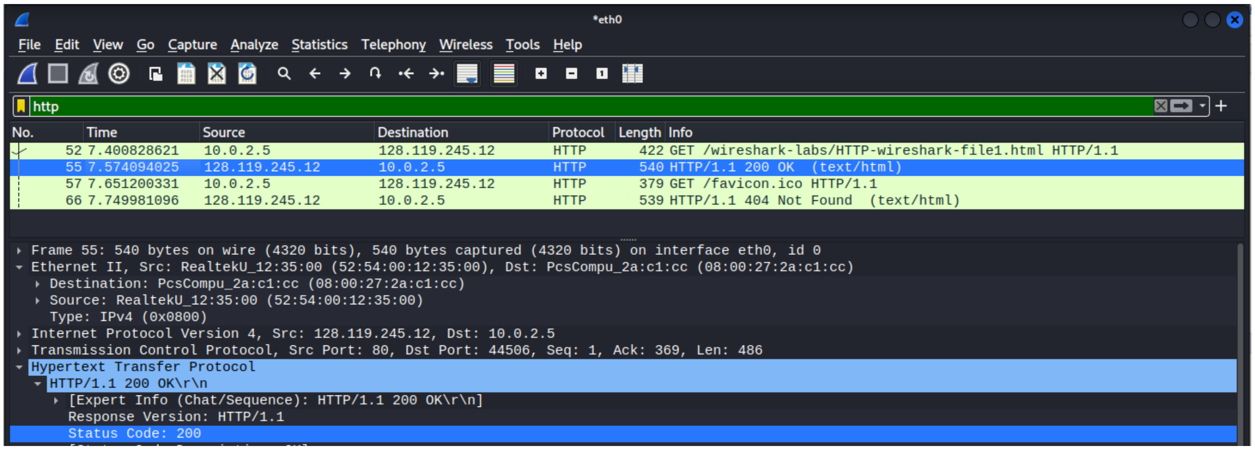


```
No.   Time          Source      Destination      Protocol  Length Info
   52 7.400828621   10.0.2.5    128.119.245.12   HTTP       422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
```

- IP address of our computer (Source): 10.0.2.5

- IP address of gaia.cs.umass.edu (Destination): 128.119.245.12

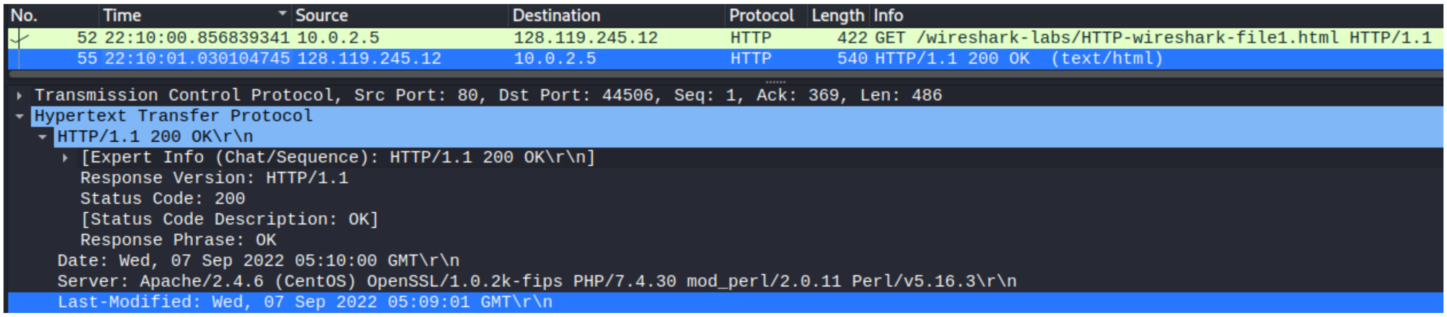
4. What is the status code returned from the server to your browser?


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time          Source          Destination     Protocol Length Info
   52 7.400828621   10.0.2.5        128.119.245.12  HTTP       422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   55 7.574094025   128.119.245.12  10.0.2.5        HTTP       540 HTTP/1.1 200 OK  (text/html)
   57 7.651200331   10.0.2.5        128.119.245.12  HTTP       379 GET /favicon.ico HTTP/1.1
   66 7.749981096   128.119.245.12  10.0.2.5        HTTP       539 HTTP/1.1 404 Not Found  (text/html)

 Frame 55: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface eth0, id 0
 Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_2a:c1:cc (08:00:27:2a:c1:cc)
   Destination: PcsCompu_2a:c1:cc (08:00:27:2a:c1:cc)
   Source: RealtekU_12:35:00 (52:54:00:12:35:00)
   Type: IPv4 (0x0800)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.5
 Transmission Control Protocol, Src Port: 80, Dst Port: 44506, Seq: 1, Ack: 369, Len: 486
 Hypertext Transfer Protocol
   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
```

- The status code that was returned from the server to our browser 200.

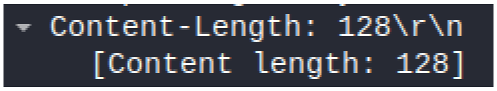
5. When was the HTML file that you are retrieving last modified at the server?



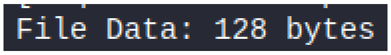
```
No.   Time                          Source          Destination     Protocol Length Info
   52 22:10:00.856839341 10.0.2.5        128.119.245.12  HTTP       422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   55 22:10:01.030104745 128.119.245.12  10.0.2.5        HTTP       540 HTTP/1.1 200 OK  (text/html)

 Transmission Control Protocol, Src Port: 80, Dst Port: 44506, Seq: 1, Ack: 369, Len: 486
 Hypertext Transfer Protocol
   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, 07 Sep 2022 05:10:00 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
   Last-Modified: Wed, 07 Sep 2022 05:09:01 GMT\r\n
```

- The HTML file that we are retrieving was last modified at the server was “Wed, 07 Sep 2022 05:09:01 GMT”.

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



```
 Content-Length: 128\r\n
   [Content length: 128]
```



```
File Data: 128 bytes
```

- 128 bytes of content were returned to our browser.

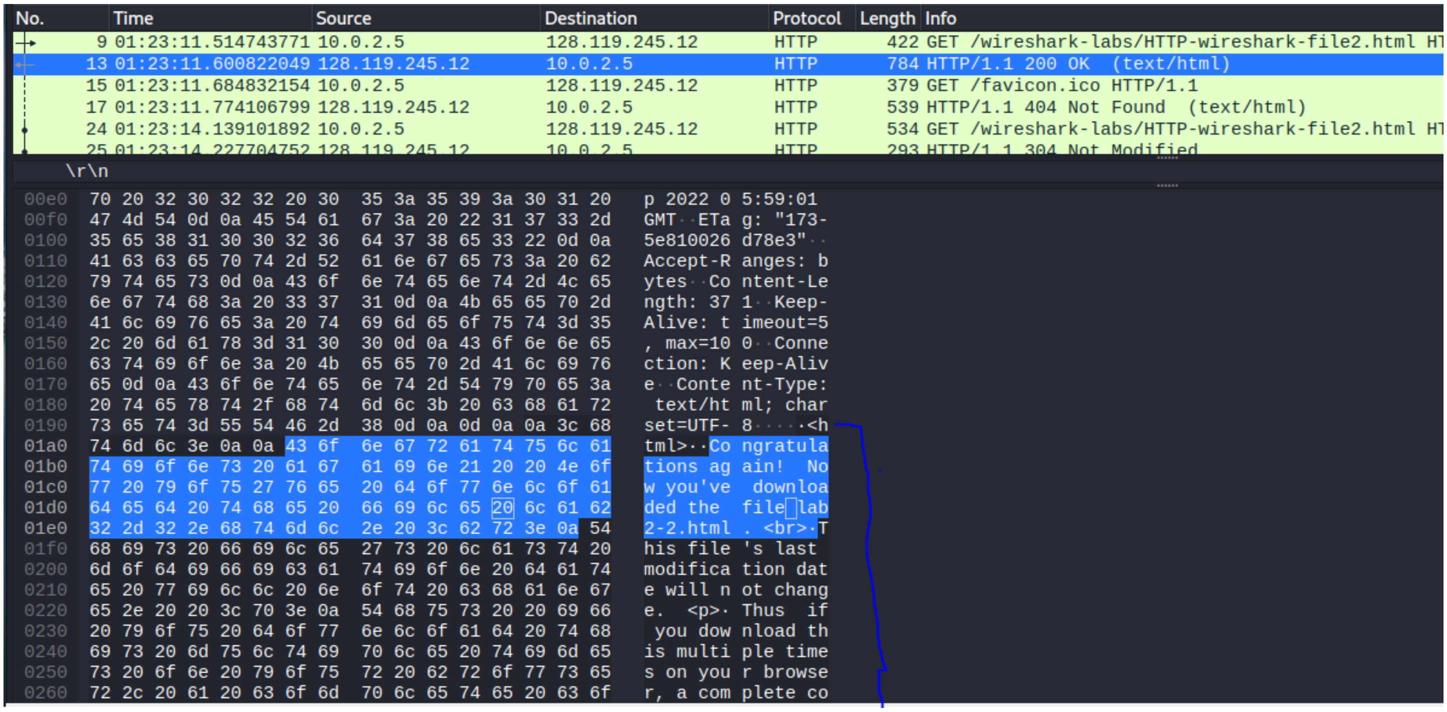
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

- No, I clicked all parts of the header and found that they all correspond to something in the 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?

- No

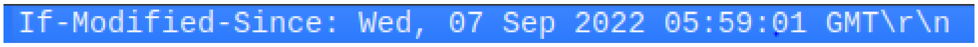
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?



```
No.   Time               Source          Destination     Protocol  Length Info
   9 01:23:11.514743771 10.0.2.5        128.119.245.12  HTTP         422 GET /wireshark-labs/HTTP-wireshark-file2.html HT
  13 01:23:11.600822049 128.119.245.12  10.0.2.5        HTTP         784 HTTP/1.1 200 OK  (text/html)
  15 01:23:11.684832154 10.0.2.5        128.119.245.12  HTTP         379 GET /favicon.ico HTTP/1.1
  17 01:23:11.774106799 128.119.245.12  10.0.2.5        HTTP         539 HTTP/1.1 404 Not Found  (text/html)
  24 01:23:14.139101892 10.0.2.5        128.119.245.12  HTTP         534 GET /wireshark-labs/HTTP-wireshark-file2.html HT
  25 01:23:14.227704752 128.119.245.12  10.0.2.5        HTTP         293 HTTP/1.1 304 Not Modified
    \r\n
00e0  70 20 32 30 32 32 20 30  35 3a 35 39 3a 30 31 20   p 2022 0 5:59:01
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 37 33 2d   GMT··ETa g: "173-
0100  35 65 38 31 30 30 32 36  64 37 38 65 33 22 0d 0a   5e810026 d78e3"··
0110  41 63 63 65 70 74 2d 52  61 6e 67 65 73 3a 20 62   Accept-R anges: b
0120  79 74 65 73 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   ytes··Co ntent-Le
0130  6e 67 74 68 3a 20 33 37  31 0d 0a 4b 65 65 70 2d   ngth: 37 1··Keep-
0140  41 6c 69 76 65 3a 20 74  69 6d 65 6f 75 74 3d 35   Alive: t imeout=5
0150  2c 20 6d 61 78 3d 31 30  30 0d 0a 43 6f 6e 6e 65   , max=10 0··Conne
0160  63 74 69 6f 6e 3a 20 4b  65 65 70 2d 41 6c 69 76   ction: K eep-Aliv
0170  65 0d 0a 43 6f 6e 74 65  6e 74 2d 54 79 70 65 3a   e··Conte nt-Type:
0180  20 74 65 78 74 2f 68 74  6d 6c 3b 20 63 68 61 72    text/ht ml; char
0190  73 65 74 3d 55 54 46 2d  38 0d 0a 0d 0a 0a 3c 68   set=UTF- 8·····<h
01a0  74 6d 6c 3e 0a 0a 43 6f  6e 67 72 61 74 75 6c 61   tml>··Co ngratula
01b0  74 69 6f 6e 73 20 61 67  61 69 6e 21 20 20 4e 6f   tions ag ain!  No
01c0  77 20 79 6f 75 27 76 65  20 64 6f 77 6e 6c 6f 61   w you've  downloa
01d0  64 65 64 20 74 68 65 20  66 69 6c 65 20 6c 61 62   ded the  file lab
01e0  32 2d 32 2e 68 74 6d 6c  2e 20 3c 62 72 3e 0a 54   2-2.html . <br>·T
01f0  68 69 73 20 66 69 6c 65  27 73 20 6c 61 73 74 20   his file 's last
0200  6d 6f 64 69 66 69 63 61  74 69 6f 6e 20 64 61 74   modifica tion dat
0210  65 20 77 69 6c 6c 20 6e  6f 74 20 63 68 61 6e 67   e will n ot chang
0220  65 2e 20 20 3c 70 3e 0a  54 68 75 73 20 20 69 66   e.  <p>· Thus  if
0230  20 79 6f 75 20 64 6f 77  6e 6c 6f 61 64 20 74 68    you dow nload th
0240  69 73 20 6d 75 6c 74 69  70 6c 65 20 74 69 6d 65   is multi ple time
0250  73 20 6f 6e 20 79 6f 75  72 20 62 72 6f 77 73 65   s on you r browse
0260  72 2c 20 61 20 63 6f 6d  70 6c 65 74 65 20 63 6f   r, a com plete co
```

- Yes, the server did explicitly return the contents of the file. We can tell by looking between the html tags.

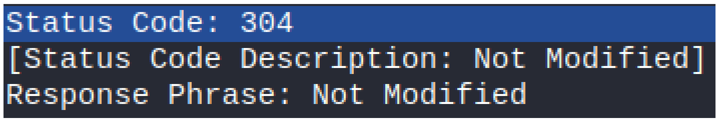
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?



```
If-Modified-Since: Wed, 07 Sep 2022 05:59:01 GMT\r\n
```

- Yes, "Wed, 07 Sep 2022 05:59:01 GMT\r\n" is the day and time in GMT of when the page was last modified/refreshed.

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.

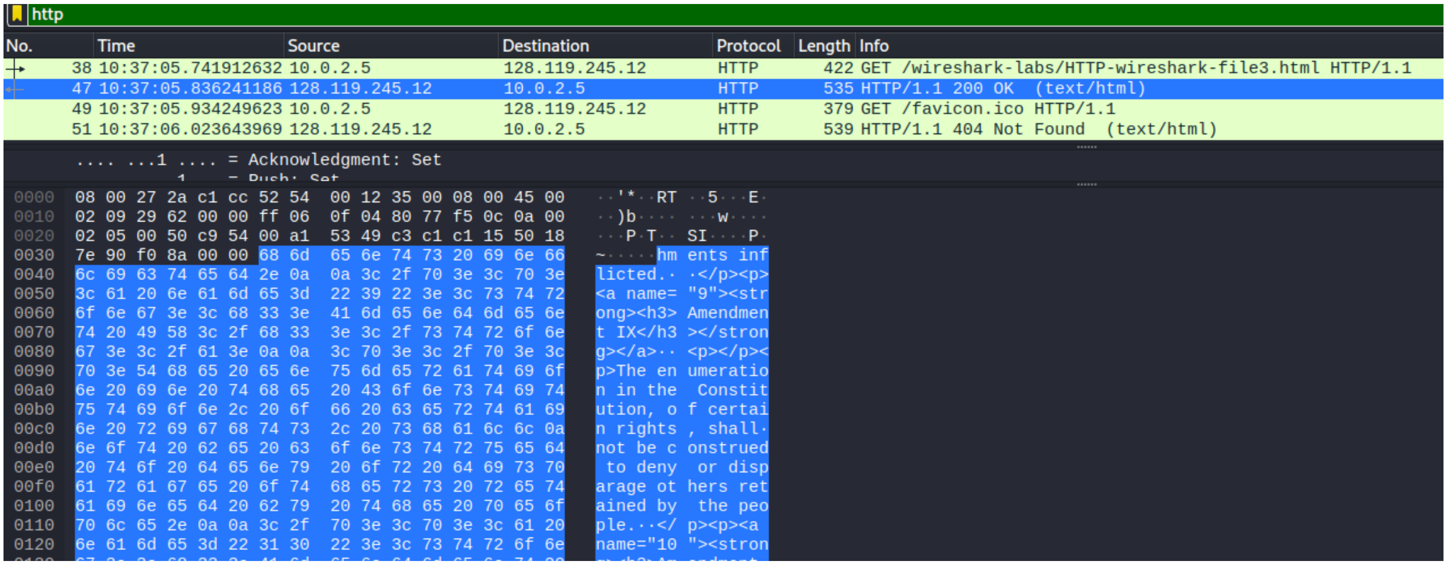


```
Status Code: 304
[Status Code Description: Not Modified]
Response Phrase: Not Modified
```

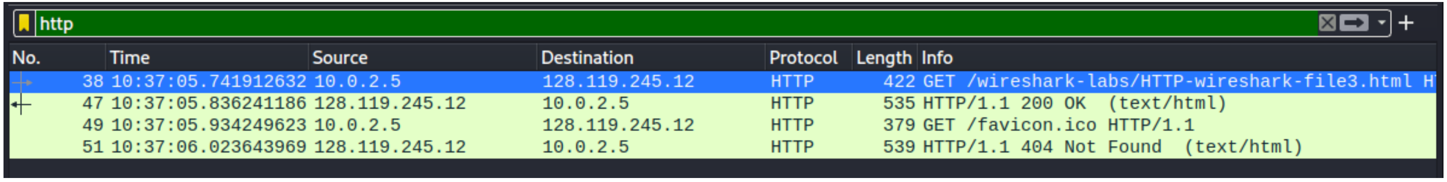
- HTTP status code: 304
- Phrase returned: Not Modified
- No, the server did not explicitly return contents of the file
- Explanation: The server found that the file had not been modified and did not return the contents of the file. The status code was 304 and the description was 'not modified'.

3. 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
No.   Time                Source          Destination     Protocol Length Info
   38 10:37:05.741912632 10.0.2.5        128.119.245.12  HTTP      422 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   47 10:37:05.836241186 128.119.245.12  10.0.2.5        HTTP      535 HTTP/1.1 200 OK  (text/html)
   49 10:37:05.934249623 10.0.2.5        128.119.245.12  HTTP      379 GET /favicon.ico HTTP/1.1
   51 10:37:06.023643969 128.119.245.12  10.0.2.5        HTTP      539 HTTP/1.1 404 Not Found  (text/html)

      .... ...1 .... = Acknowledgment: Set
                1    = Push: Set

0000  08 00 27 2a c1 cc 52 54  00 12 35 00 08 00 45 00   ··'*··RT ··5···E·
0010  02 09 29 62 00 00 ff 06  0f 04 80 77 f5 0c 0a 00   ··)b···· ···w····
0020  02 05 00 50 c9 54 00 a1  53 49 c3 c1 c1 15 50 18   ···P·T·· SI····P·
0030  7e 90 f0 8a 00 00 68 6d  65 6e 74 73 20 69 6e 66   ~·····hm ents inf
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.· ·</p><p>
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73 74 72   <a name= "9"><str
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d 65 6e   ong><h3> Amendmen
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72 6f 6e   t IX</h3 ></stron
0080  67 3e 3c 2f 61 3e 0a 0a  3c 70 3e 3c 2f 70 3e 3c   g></a>·· <p></p><
0090  70 3e 54 68 65 20 65 6e  75 6d 65 72 61 74 69 6f   p>The en umeratio
00a0  6e 20 69 6e 20 74 68 65  20 43 6f 6e 73 74 69 74   n in the  Constit
00b0  75 74 69 6f 6e 2c 20 6f  66 20 63 65 72 74 61 69   ution, o f certai
00c0  6e 20 72 69 67 68 74 73  2c 20 73 68 61 6c 6c 0a   n rights , shall·
00d0  6e 6f 74 20 62 65 20 63  6f 6e 73 74 72 75 65 64   not be c onstrued
00e0  20 74 6f 20 64 65 6e 79  20 6f 72 20 64 69 73 70    to deny  or disp
00f0  61 72 61 67 65 20 6f 74  68 65 72 73 20 72 65 74   arage ot hers ret
0100  61 69 6e 65 64 20 62 79  20 74 68 65 20 70 65 6f   ained by  the peo
0110  70 6c 65 2e 0a 0a 3c 2f  70 3e 3c 70 3e 3c 61 20   ple.··</ p><p><a 
0120  6e 61 6d 65 3d 22 31 30  22 3e 3c 73 74 72 6f 6e   name="10 "><stron
```



```
http
No.   Time                Source          Destination     Protocol Length Info
   38 10:37:05.741912632 10.0.2.5        128.119.245.12  HTTP      422 GET /wireshark-labs/HTTP-wireshark-file3.html H
   47 10:37:05.836241186 128.119.245.12  10.0.2.5        HTTP      535 HTTP/1.1 200 OK  (text/html)
   49 10:37:05.934249623 10.0.2.5        128.119.245.12  HTTP      379 GET /favicon.ico HTTP/1.1
   51 10:37:06.023643969 128.119.245.12  10.0.2.5        HTTP      539 HTTP/1.1 404 Not Found  (text/html)
```

- One HTTP GET request message was sent by our browser as we ignored the one for the favicon. The packet number in the trace that contains the get message for the Bill of Rights is 47.

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

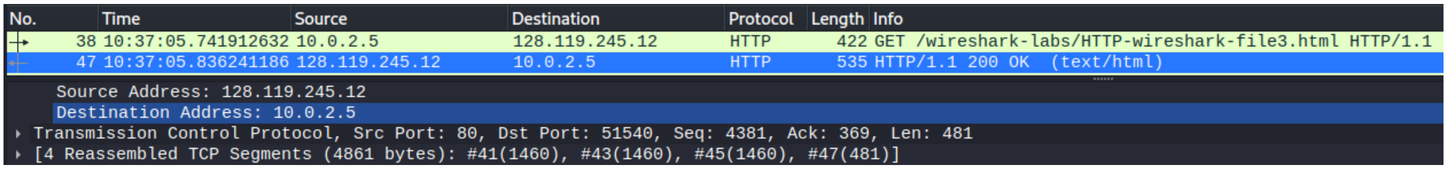
- packet number 47 contains that status code and phrase association with the response to the HTTP GET request.

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

- The status code is: 200

- The phrase in response 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?

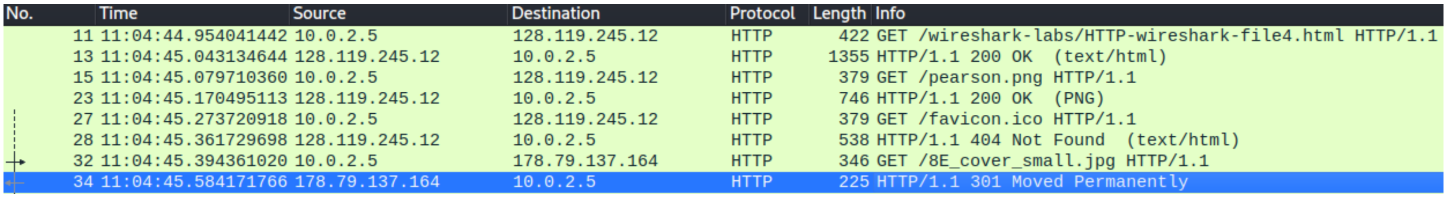


```
No.   Time                Source          Destination     Protocol Length Info
   38 10:37:05.741912632 10.0.2.5        128.119.245.12  HTTP      422 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   47 10:37:05.836241186 128.119.245.12  10.0.2.5        HTTP      535 HTTP/1.1 200 OK  (text/html)

    Source Address: 128.119.245.12
    Destination Address: 10.0.2.5
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 51540, Seq: 4381, Ack: 369, Len: 481
▸ [4 Reassembled TCP Segments (4861 bytes): #41(1460), #43(1460), #45(1460), #47(481)]
```

- There were 4 data-containing TCP segments

4. HTML Documents with Embedded Objects

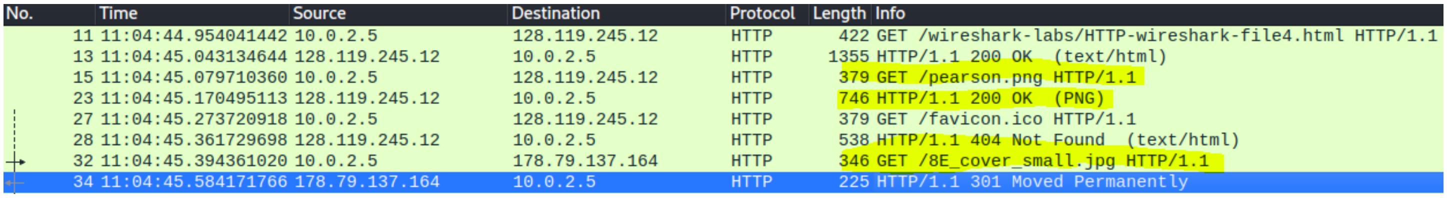
16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?



```
No.     Time                Source          Destination     Protocol Length Info
     11 11:04:44.954041442 10.0.2.5        128.119.245.12  HTTP      422 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
     13 11:04:45.043134644 128.119.245.12  10.0.2.5        HTTP     1355 HTTP/1.1 200 OK  (text/html)
     15 11:04:45.079710360 10.0.2.5        128.119.245.12  HTTP      379 GET /pearson.png HTTP/1.1
     23 11:04:45.170495113 128.119.245.12  10.0.2.5        HTTP      746 HTTP/1.1 200 OK  (PNG)
     27 11:04:45.273720918 10.0.2.5        128.119.245.12  HTTP      379 GET /favicon.ico HTTP/1.1
     28 11:04:45.361729698 128.119.245.12  10.0.2.5        HTTP      538 HTTP/1.1 404 Not Found  (text/html)
     32 11:04:45.394361020 10.0.2.5        178.79.137.164  HTTP      346 GET /8E_cover_small.jpg HTTP/1.1
     34 11:04:45.584171766 178.79.137.164  10.0.2.5        HTTP      225 HTTP/1.1 301 Moved Permanently
```

- Minus the favicon one, we have 3 HTTP GET request message sent, where they were all sent to Internet addresses 128.119.245.12 and 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.



```
No.     Time                Source          Destination     Protocol Length Info
     11 11:04:44.954041442 10.0.2.5        128.119.245.12  HTTP      422 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
     13 11:04:45.043134644 128.119.245.12  10.0.2.5        HTTP     1355 HTTP/1.1 200 OK  (text/html)
     15 11:04:45.079710360 10.0.2.5        128.119.245.12  HTTP      379 GET /pearson.png HTTP/1.1
     23 11:04:45.170495113 128.119.245.12  10.0.2.5        HTTP      746 HTTP/1.1 200 OK  (PNG)
     27 11:04:45.273720918 10.0.2.5        128.119.245.12  HTTP      379 GET /favicon.ico HTTP/1.1
     28 11:04:45.361729698 128.119.245.12  10.0.2.5        HTTP      538 HTTP/1.1 404 Not Found  (text/html)
     32 11:04:45.394361020 10.0.2.5        178.79.137.164  HTTP      346 GET /8E_cover_small.jpg HTTP/1.1
     34 11:04:45.584171766 178.79.137.164  10.0.2.5        HTTP      225 HTTP/1.1 301 Moved Permanently
```

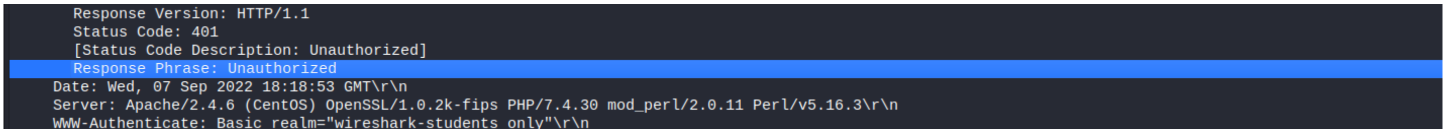
- We believe the two images were downloaded serially since the HTTP GET message for pearson.png was sent and a response for it was given before the HTTP GET message of the 8E_cover_small.jpg image was even sent as a request.

5. HTTP Authentication

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

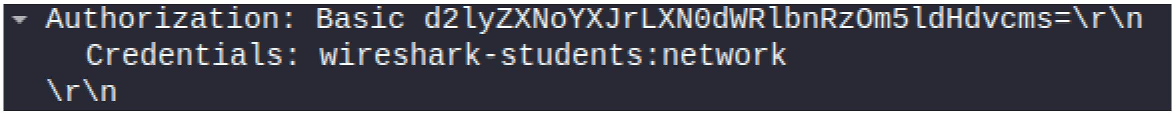
- status code: 401

- response phrase: Unauthorized



```
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
     Date: Wed, 07 Sep 2022 18:18:53 GMT\r\n
     Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
     WWW-Authenticate: Basic realm="wireshark-students only"\r\n
```

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



```
▾ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
     Credentials: wireshark-students:network
  \r\n
```