Networks

Lab 1

Name : مصطفى محمد رأفت عبد اللطيف

ID : 20011947

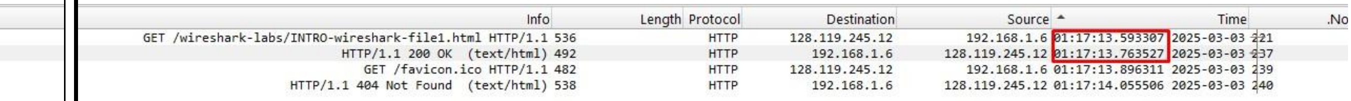
Part I:

Entering http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.

DNS,TCP,SSL

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received?



Info	Length	Protocol	Destination	Source	Time	.No
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1	536	HTTP	128.119.245.12	192.168.1.6	01:17:13.593307 2025-03-03	221
HTTP/1.1 200 OK (text/html)	492	HTTP	192.168.1.6	128.119.245.12	01:17:13.763527 2025-03-03	237
GET /favicon.ico HTTP/1.1	482	HTTP	128.119.245.12	192.168.1.6	01:17:13.896311 2025-03-03	239
HTTP/1.1 404 Not Found (text/html)	538	HTTP	192.168.1.6	128.119.245.12	01:17:14.055506 2025-03-03	240

[Time since request: 0.170220000 seconds]

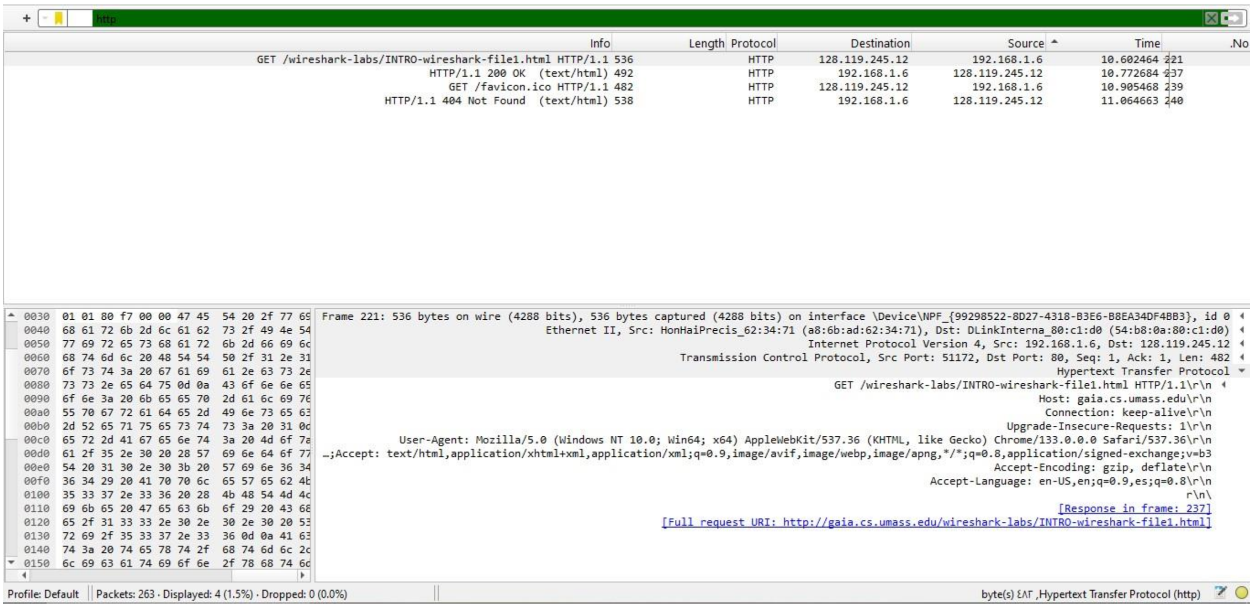
3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?

My Computer address is: 192.168.1.6

address of the gaia.cs.umass.edu: 128.119.245.12

4. Print the two HTTP messages (GET and OK) referred to in question 2 above.

GET:

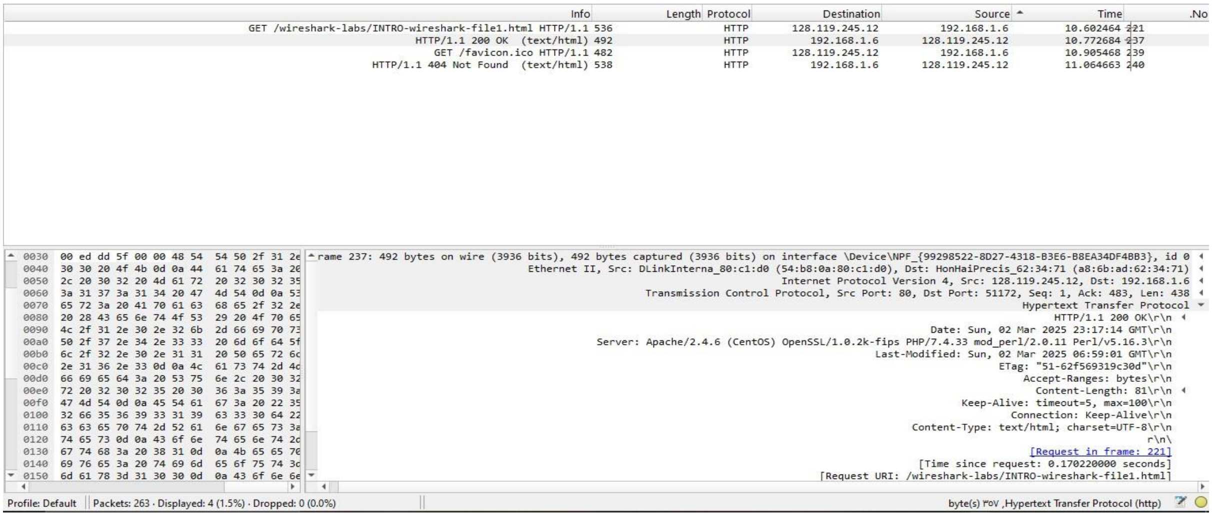


```
http

                                                    Info   Length Protocol     Destination          Source ^          Time   .No
   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 536    HTTP     128.119.245.12       192.168.1.6     10.602464 221
                         HTTP/1.1 200 OK  (text/html) 492         HTTP        192.168.1.6    128.119.245.12     10.772684 237
                              GET /favicon.ico HTTP/1.1 482       HTTP     128.119.245.12       192.168.1.6     10.905468 239
                  HTTP/1.1 404 Not Found  (text/html) 538         HTTP        192.168.1.6    128.119.245.12     11.064663 240
```

```
0030  01 01 80 f7 00 00 47 45  54 20 2f 77 69
0040  68 61 72 6b 2d 6c 61 62  73 2f 49 4e 54
0050  77 69 72 65 73 68 61 72  6b 2d 66 69 6c
0060  68 74 6d 6c 20 48 54 54  50 2f 31 2e 31
0070  6f 73 74 3a 20 67 61 69  61 2e 63 73 2e
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d
00c0  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a
00d0  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77
00e0  54 20 31 30 2e 30 3b 20  57 69 6e 36 34
00f0  36 34 29 20 41 70 70 6c  65 57 65 62 4b
0100  35 33 37 2e 33 36 20 28  4b 48 54 4d 4c
0110  69 6b 65 20 47 65 63 6b  6f 29 20 43 68
0120  65 2f 31 33 33 2e 30 2e  30 2e 30 20 53
0130  72 69 2f 35 33 37 2e 33  36 0d 0a 41 63
0140  74 3a 20 74 65 78 74 2f  68 74 6d 6c 2c
0150  6c 69 63 61 74 69 6f 6e  2f 78 68 74 6d
```

```
Frame 221: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
                                  Ethernet II, Src: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71), Dst: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0)
                                                                       Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
                                                         Transmission Control Protocol, Src Port: 51172, Dst Port: 80, Seq: 1, Ack: 1, Len: 482
                                                                                                              Hypertext Transfer Protocol
                                                                        GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
                                                                                                             Host: gaia.cs.umass.edu\r\n
                                                                                                              Connection: keep-alive\r\n
                                                                                                        Upgrade-Insecure-Requests: 1\r\n
           User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36\r\n
…;Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
                                                                                                        Accept-Encoding: gzip, deflate\r\n
                                                                                             Accept-Language: en-US,en;q=0.9,es;q=0.8\r\n
                                                                                                                                    r\n\
                                                                                                                  [Response in frame: 237]
                                                               [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]

Profile: Default  Packets: 263 · Displayed: 4 (1.5%) · Dropped: 0 (0.0%)                         byte(s) ٤٨٢ ,Hypertext Transfer Protocol (http)
```

OK:



```
                                                    Info   Length Protocol     Destination          Source ^          Time   .No
   GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1 536    HTTP     128.119.245.12       192.168.1.6     10.602464 221
                         HTTP/1.1 200 OK  (text/html) 492         HTTP        192.168.1.6    128.119.245.12     10.772684 237
                              GET /favicon.ico HTTP/1.1 482       HTTP     128.119.245.12       192.168.1.6     10.905468 239
                  HTTP/1.1 404 Not Found  (text/html) 538         HTTP        192.168.1.6    128.119.245.12     11.064663 240
```

```
0030  00 ed dd 5f 00 00 48 54  54 50 2f 31 2e
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20
0050  2c 20 30 32 20 4d 61 72  20 32 30 32 35
0060  3a 31 37 3a 31 34 20 47  4d 54 0d 0a 53
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64 5f
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72 6c
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 30 32
00e0  72 20 32 30 32 35 20 30  36 3a 35 39 3a
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 35
0100  32 66 35 36 39 33 31 39  63 33 30 64 22
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d
0130  67 74 68 3a 20 38 31 0d  0a 4b 65 65 70
0140  69 76 65 3a 20 74 69 6d  65 6f 75 74 3c
0150  6d 61 78 3d 31 30 30 0d  0a 43 6f 6e 6e
```

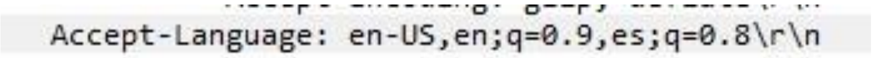
```
rame 237: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
                                Ethernet II, Src: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0), Dst: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71)
                                                                    Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6
                                                      Transmission Control Protocol, Src Port: 80, Dst Port: 51172, Seq: 1, Ack: 483, Len: 438
                                                                                                           Hypertext Transfer Protocol
                                                                                                                    HTTP/1.1 200 OK\r\n
                                                                                             Date: Sun, 02 Mar 2025 23:17:14 GMT\r\n
                                         Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
                                                                                    Last-Modified: Sun, 02 Mar 2025 06:59:01 GMT\r\n
                                                                                                        ETag: "51-62f569319c30d"\r\n
                                                                                                             Accept-Ranges: bytes\r\n
                                                                                                               Content-Length: 81\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\
                                                                                                               [Request in frame: 221]
                                                                                                [Time since request: 0.170220000 seconds]
                                                                                    [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]

Profile: Default  Packets: 263 · Displayed: 4 (1.5%) · Dropped: 0 (0.0%)                         byte(s) ٣٥٧ ,Hypertext Transfer Protocol (http)
```

Part 2:

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server 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=0.9,es;q=0.8\r\n
```

3. What is the IP address of your computer? Of the

gaia.cs.umass.edu server?

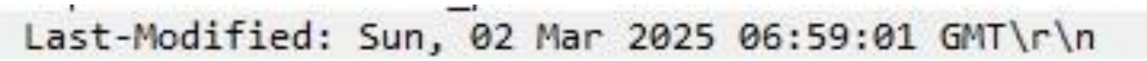
IP Address of my computer: 192.168.1.6

IP of the gaia.cs.umass.edu server: 128.119.245.12

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

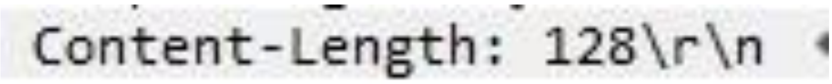
200 OK

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



```
Last-Modified: Sun, 02 Mar 2025 06:59:01 GMT\r\n
```

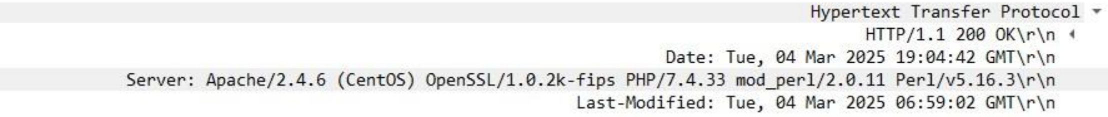
6. How many bytes of content are being returned to your browser?



```
Content-Length: 128\r\n
```

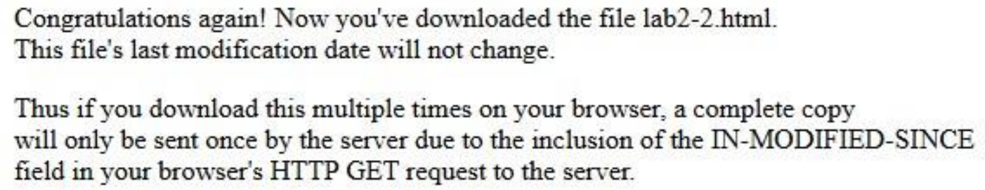
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one

Apache.



```
                                                    Hypertext Transfer Protocol
                                                          HTTP/1.1 200 OK\r\n
                                          Date: Tue, 04 Mar 2025 19:04:42 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
                                 Last-Modified: Tue, 04 Mar 2025 06:59:02 GMT\r\n
```

Part III:



Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.

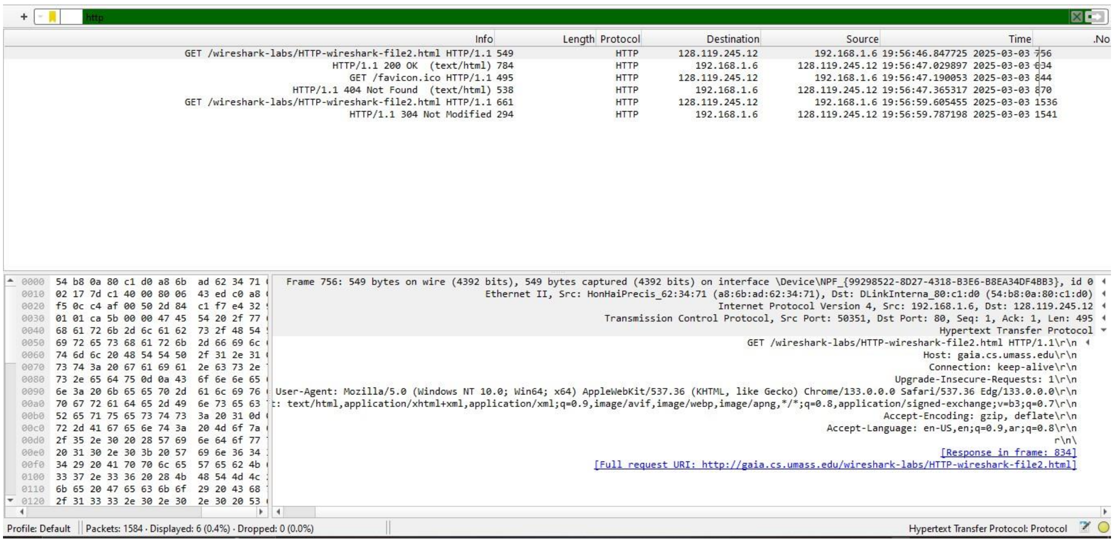
---

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?

there's no IF-MODIFIED-SINCE.

http GET



```
http
                                                    Info  Length Protocol      Destination            Source                               Time    .No
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 549      HTTP    128.119.245.12       192.168.1.6 19:56:46.847725 2025-03-03 756
                          HTTP/1.1 200 OK  (text/html) 784      HTTP       192.168.1.6    128.119.245.12 19:56:47.029897 2025-03-03 834
                             GET /favicon.ico HTTP/1.1 495      HTTP    128.119.245.12       192.168.1.6 19:56:47.190053 2025-03-03 844
                 HTTP/1.1 404 Not Found  (text/html) 538      HTTP       192.168.1.6    128.119.245.12 19:56:47.365317 2025-03-03 870
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 661      HTTP    128.119.245.12       192.168.1.6 19:56:59.605455 2025-03-03 1536
                             HTTP/1.1 304 Not Modified 294      HTTP       192.168.1.6    128.119.245.12 19:56:59.787198 2025-03-03 1541
```

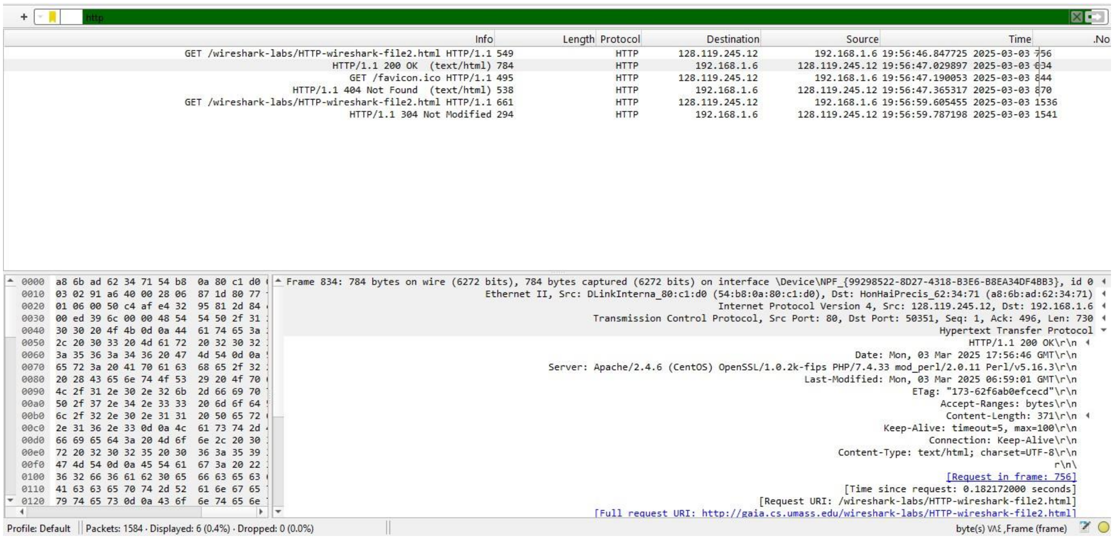
```
0000  54 b8 0a 80 c1 d0 a8 6b  ad 62 34 71
0010  02 17 7d c1 40 00 80 06  43 ed c0 a8
0020  f5 0c c4 af 00 50 2d 84  c1 f7 e4 32
0030  01 01 ca 5b 00 00 47 45  54 20 2f 77
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68
0120  2f 31 33 33 2e 30 2e 30  2e 30 20 53
```

```
 Frame 756: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
                          Ethernet II, Src: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71), Dst: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0)
                                                         Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
                                           Transmission Control Protocol, Src Port: 50351, Dst Port: 80, Seq: 1, Ack: 1, Len: 495
                                                                                                    Hypertext Transfer Protocol
                                                                  GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
                                                                                                Host: gaia.cs.umass.edu\r\n
                                                                                                Connection: keep-alive\r\n
                                                                                           Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 Edg/133.0.0.0\r\n
t: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
                                                                                         Accept-Encoding: gzip, deflate\r\n
                                                                                 Accept-Language: en-US,en;q=0.9,ar;q=0.8\r\n
                                                                                                                      r\n\
                                                                                                  [Response in frame: 834]
                                           [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
Profile: Default | Packets: 1584 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%)          Hypertext Transfer Protocol: Protocol
```

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

http response:



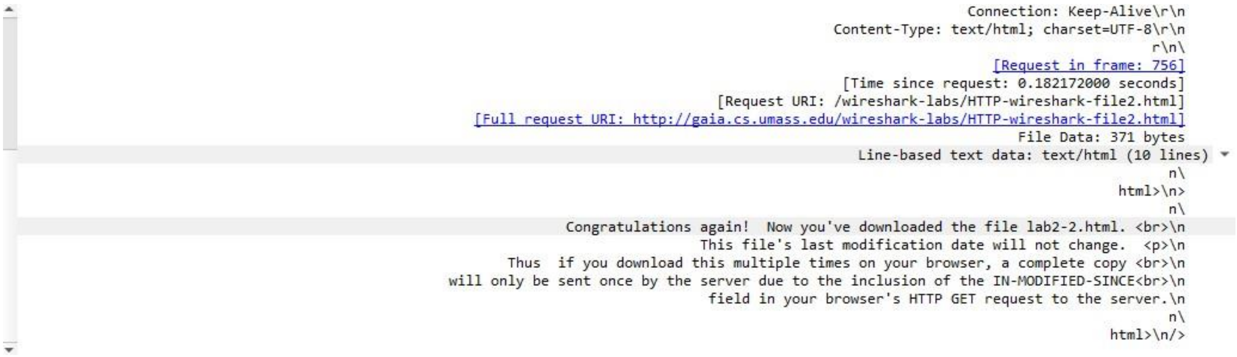
```
http
                                                    Info  Length Protocol      Destination            Source                               Time    .No
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 549      HTTP    128.119.245.12       192.168.1.6 19:56:46.847725 2025-03-03 756
                          HTTP/1.1 200 OK  (text/html) 784      HTTP       192.168.1.6    128.119.245.12 19:56:47.029897 2025-03-03 834
                             GET /favicon.ico HTTP/1.1 495      HTTP    128.119.245.12       192.168.1.6 19:56:47.190053 2025-03-03 844
                 HTTP/1.1 404 Not Found  (text/html) 538      HTTP       192.168.1.6    128.119.245.12 19:56:47.365317 2025-03-03 870
    GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 661      HTTP    128.119.245.12       192.168.1.6 19:56:59.605455 2025-03-03 1536
                             HTTP/1.1 304 Not Modified 294      HTTP       192.168.1.6    128.119.245.12 19:56:59.787198 2025-03-03 1541
```

```
0000  a8 6b ad 62 34 71 54 b8  0a 80 c1 d0
0010  03 02 91 a6 40 00 28 06  87 1d 80 77
0020  01 06 00 50 c4 af e4 32  95 81 2d 84
0030  00 ed 39 6c 00 00 48 54  54 50 2f 31
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a
0050  2c 20 30 33 20 4d 61 72  20 32 30 32
0060  3a 35 36 3a 34 36 20 47  4d 54 0d 0a
0070  65 72 3a 20 41 70 61 63  68 65 2f 32
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70
00a0  50 2f 37 2e 34 2e 33 33  20 6d 6f 64
00b0  6c 2f 32 2e 30 2e 31 31  20 50 65 72
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d
00d0  66 69 65 64 3a 20 4d 6f  6e 2c 20 30
00e0  72 20 32 30 32 35 20 30  36 3a 35 39
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22
0100  36 32 66 36 61 62 30 65  66 63 65 63
0110  41 63 63 65 70 74 2d 52  61 6e 67 65
0120  79 74 65 73 0d 0a 43 6f  6e 74 65 6e
```

```
 Frame 834: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
                          Ethernet II, Src: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0), Dst: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71)
                                                         Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6
                                         Transmission Control Protocol, Src Port: 80, Dst Port: 50351, Seq: 1, Ack: 496, Len: 730
                                                                                                    Hypertext Transfer Protocol
                                                                                                          HTTP/1.1 200 OK\r\n
                                                                                       Date: Mon, 03 Mar 2025 17:56:46 GMT\r\n
                                  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
                                                                               Last-Modified: Mon, 03 Mar 2025 06:59:01 GMT\r\n
                                                                                                 ETag: "173-62f6ab0efcecd"\r\n
                                                                                                     Accept-Ranges: bytes\r\n
                                                                                                      Content-Length: 371\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\
                                                                                                   [Request in frame: 756]
                                                                                     [Time since request: 0.182172000 seconds]
                                                                       [Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
                                           [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
Profile: Default | Packets: 1584 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%)          byte(s) ٧٨٤ ,Frame (frame)
```

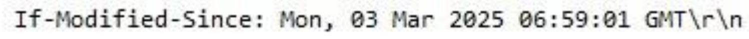
the contents of the file:



```
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
r\n\
[Request in frame: 756]
[Time since request: 0.182172000 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
Line-based text data: text/html (10 lines)
n\
html>\n>
n\
Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change.  <p>\n
Thus  if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
n\
html>\n/>
```

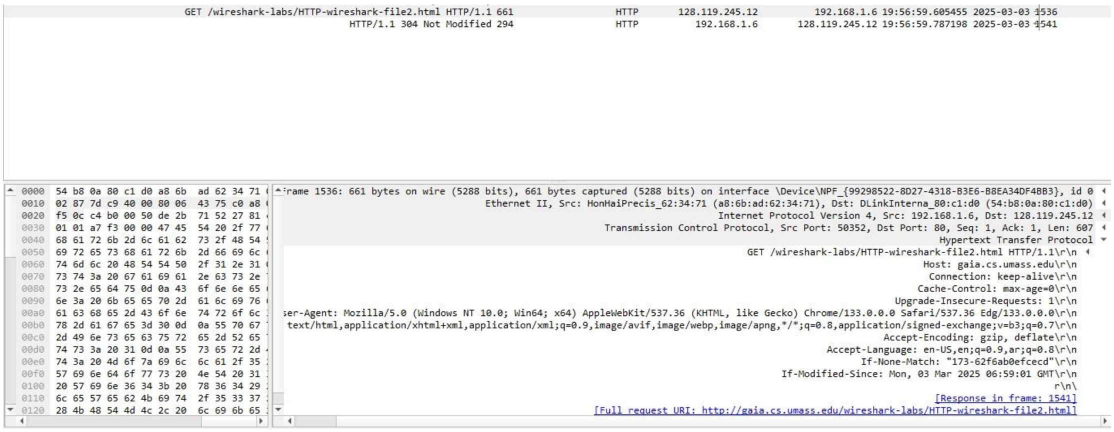
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

there's a IF-MODIFIED-SINCE.



```
If-Modified-Since: Mon, 03 Mar 2025 06:59:01 GMT\r\n
```

after refresh http GET:



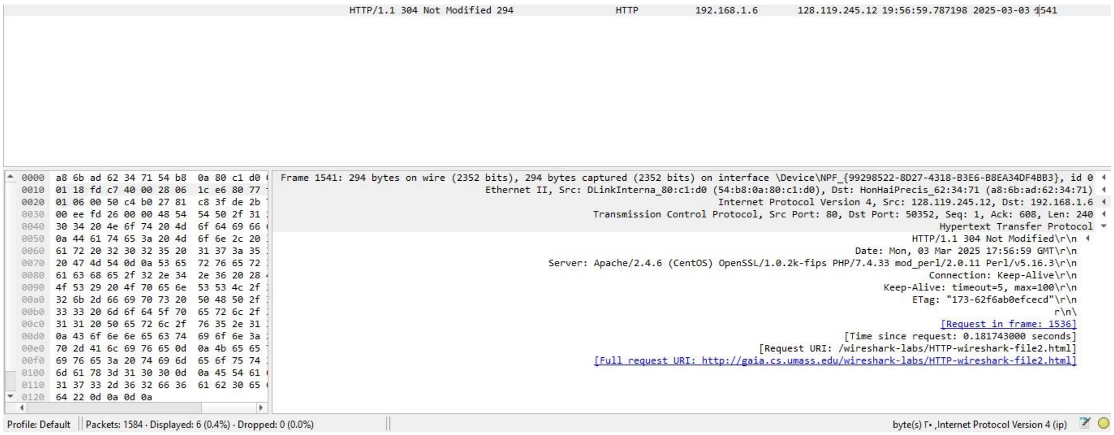
```
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1 661     HTTP   128.119.245.12      192.168.1.6 19:56:59.605455 2025-03-03 1536
                    HTTP/1.1 304 Not Modified 294     HTTP      192.168.1.6   128.119.245.12 19:56:59.787198 2025-03-03 1541
```

```
0000  54 b8 0a 80 c1 d0 a8 6b  ad 62 34 71
0010  02 87 7d c9 40 00 80 06  43 75 c0 a8
0020  f5 0c c4 b0 00 50 de 2b  71 52 27 81
0030  01 01 a7 f3 00 00 47 45  54 20 2f 77
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76
00a0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c
00b0  78 2d 61 67 65 3d 30 0d  0a 55 70 67
00c0  2d 49 6e 73 65 63 75 72  65 2d 52 65
00d0  74 73 3a 20 31 0d 0a 55  73 65 72 2d
00e0  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35
00f0  57 69 6e 64 6f 77 73 20  4e 54 20 31
0100  20 57 69 6e 36 34 3b 20  78 36 34 29
0110  6c 65 57 65 62 4b 69 74  2f 35 33 37
0120  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65
```

```
rame 1536: 661 bytes on wire (5288 bits), 661 bytes captured (5288 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
Ethernet II, Src: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71), Dst: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0)
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50352, Dst Port: 80, Seq: 1, Ack: 1, Len: 607
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file2.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
Upgrade-Insecure-Requests: 1\r\n
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 Edg/133.0.0.0\r\n
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,ar;q=0.8\r\n
If-None-Match: "173-62f6ab0efcecd"\r\n
If-Modified-Since: Mon, 03 Mar 2025 06:59:01 GMT\r\n
r\n\
[Response in frame: 1541]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

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



```
HTTP/1.1 304 Not Modified 294        HTTP      192.168.1.6      128.119.245.12 19:56:59.787198 2025-03-03 1541
```

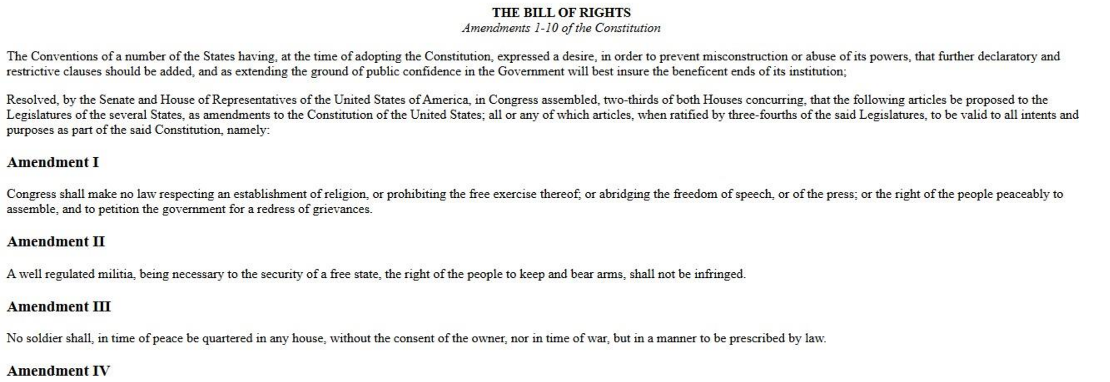
```
0000  a8 6b ad 62 34 71 54 b8  0a 80 c1 d0
0010  01 18 fd c7 40 00 28 06  1c e6 80 77
0020  01 06 00 50 c4 b0 27 81  c8 3f de 2b
0030  00 ee fd 26 00 00 48 54  54 50 2f 31
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66
0050  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20
0060  61 72 20 32 30 32 35 20  31 37 3a 35
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f
00b0  33 33 20 6d 6f 64 5f 70  65 72 6c 2f
00c0  31 31 20 50 65 72 6c 2f  76 35 2e 31
00d0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a
00e0  70 2d 41 6c 69 76 65 0d  0a 4b 65 65
00f0  69 76 65 3a 20 74 69 6d  65 6f 75 74
0100  6d 61 78 3d 31 30 30 0d  0a 45 54 61
0110  31 37 33 2d 36 32 66 36  61 62 30 65
0120  64 22 0d 0a 0d 0a
```

```
Frame 1541: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
Ethernet II, Src: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0), Dst: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6
Transmission Control Protocol, Src Port: 80, Dst Port: 50352, Seq: 1, Ack: 608, Len: 240
Hypertext Transfer Protocol
HTTP/1.1 304 Not Modified\r\n
Date: Mon, 03 Mar 2025 17:56:59 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=100\r\n
ETag: "173-62f6ab0efcecd"\r\n
r\n\
[Request in frame: 1536]
[Time since request: 0.181743000 seconds]
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

Profile: Default
Packets: 1584 · Displayed: 6 (0.4%) · Dropped: 0 (0.0%)
byte(s) ٢٠ ,Internet Protocol Version 4 (ip)

it does not return the contents again. The server tells the client that the file is still the same and there's no change from the browsers cache after the refresh.

Part IV:



THE BILL OF RIGHTS

Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

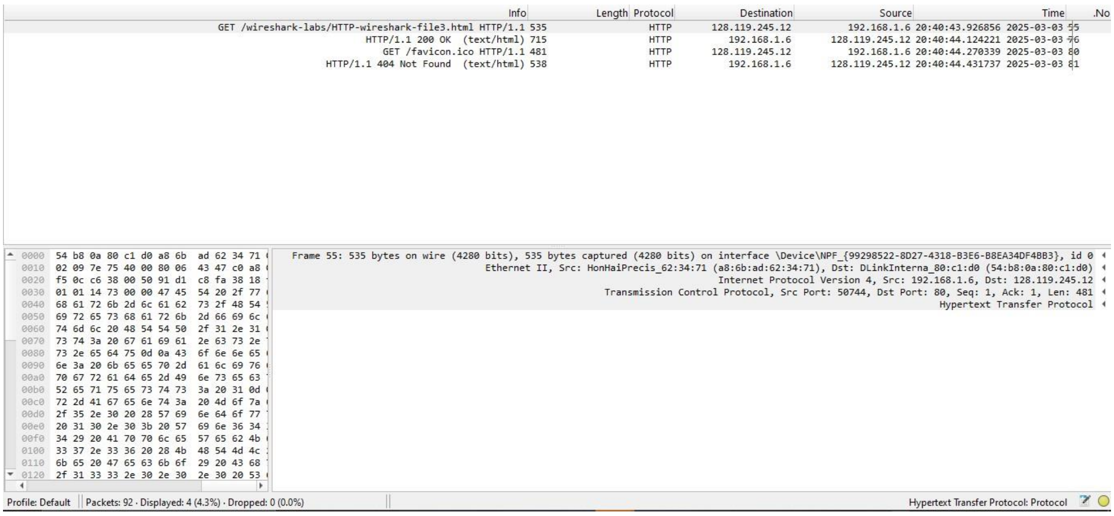
Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

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?

one http GET request, Packet number 55.



```
                                                     Info   Length Protocol     Destination            Source                          Time  .No
    GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 535       HTTP    128.119.245.12       192.168.1.6 20:40:43.926856 2025-03-03 55
                             HTTP/1.1 200 OK  (text/html) 715       HTTP       192.168.1.6    128.119.245.12 20:40:44.124221 2025-03-03 76
                               GET /favicon.ico HTTP/1.1 481       HTTP    128.119.245.12       192.168.1.6 20:40:44.270339 2025-03-03 80
                       HTTP/1.1 404 Not Found  (text/html) 538       HTTP       192.168.1.6    128.119.245.12 20:40:44.431737 2025-03-03 81
```

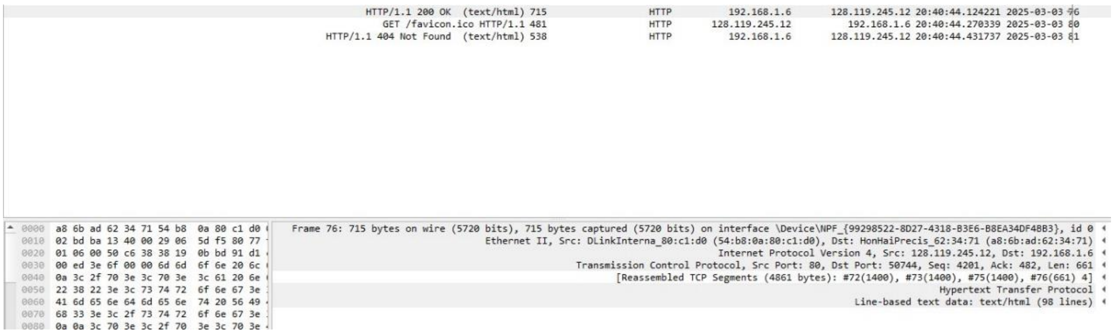
```
0000  54 b8 0a 80 c1 d0 a8 6b  ad 62 34 71
0010  02 09 7e 75 40 00 80 06  43 47 c0 a8
0020  f5 0c c6 38 00 50 91 d1  c8 fa 38 18
0030  01 01 14 73 00 00 47 45  54 20 2f 77
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68
0120  2f 31 33 33 2e 30 2e 30  2e 30 20 53
```

```
Frame 55: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
             Ethernet II, Src: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71), Dst: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0)
                                                 Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
                                   Transmission Control Protocol, Src Port: 50744, Dst Port: 80, Seq: 1, Ack: 1, Len: 481
                                                                                            Hypertext Transfer Protocol
```

Profile: Default | Packets: 92 · Displayed: 4 (4.3%) · Dropped: 0 (0.0%) | Hypertext Transfer Protocol: Protocol

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

Packet number 76.



```
                             HTTP/1.1 200 OK  (text/html) 715       HTTP       192.168.1.6    128.119.245.12 20:40:44.124221 2025-03-03 76
                               GET /favicon.ico HTTP/1.1 481       HTTP    128.119.245.12       192.168.1.6 20:40:44.270339 2025-03-03 80
                       HTTP/1.1 404 Not Found  (text/html) 538       HTTP       192.168.1.6    128.119.245.12 20:40:44.431737 2025-03-03 81
```

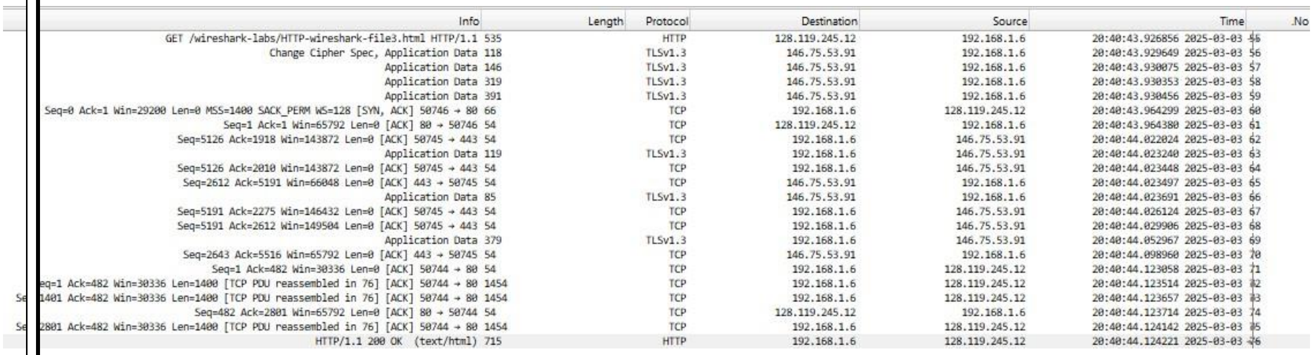
```
0000  a8 6b ad 62 34 71 54 b8  0a 80 c1 d0
0010  02 bd ba 13 40 00 29 06  5d f5 80 77
0020  01 06 00 50 c6 38 38 19  0b bd 91 d1
0030  00 ed 3e 6f 00 00 6d 6d  6f 6e 20 6c
0040  0a 3c 2f 70 3e 3c 70 3e  3c 61 20 6e
0050  22 38 22 3e 3c 73 74 72  6f 6e 67 3e
0060  41 6d 65 6e 64 6d 65 6e  74 20 56 49
0070  68 33 3e 3c 2f 73 74 72  6f 6e 67 3e
0080  0a 0a 3c 70 3e 3c 2f 70  3e 3c 70 3e
```

```
Frame 76: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface \Device\NPF_{99298522-8D27-4318-B3E6-B8EA34DF4BB3}, id 0
             Ethernet II, Src: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0), Dst: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71)
                                                 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.6
                             Transmission Control Protocol, Src Port: 80, Dst Port: 50744, Seq: 4201, Ack: 482, Len: 661
                                [Reassembled TCP Segments (4861 bytes): #72(1400), #73(1400), #75(1400), #76(661) 4]
                                                                                            Hypertext Transfer Protocol
                                                                              Line-based text data: text/html (98 lines)
```

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

200 OK

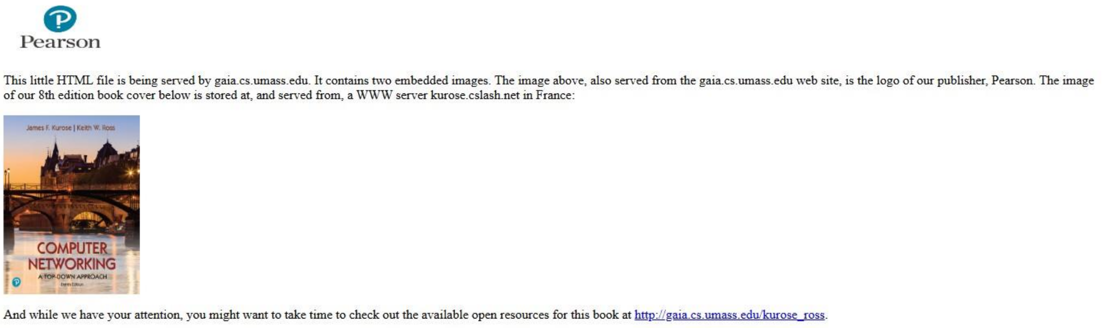
15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights? 7 TCP.



Info	Length	Protocol	Destination	Source	Time	.No
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1	535	HTTP	128.119.245.12	192.168.1.6	20:40:43.926856 2025-03-03	55
Change Cipher Spec, Application Data	118	TLSv1.3	146.75.53.91	192.168.1.6	20:40:43.929649 2025-03-03	56
Application Data	146	TLSv1.3	146.75.53.91	192.168.1.6	20:40:43.930075 2025-03-03	57
Application Data	319	TLSv1.3	146.75.53.91	192.168.1.6	20:40:43.930353 2025-03-03	58
Application Data	391	TLSv1.3	146.75.53.91	192.168.1.6	20:40:43.930456 2025-03-03	59
Seq=0 Ack=1 Win=29200 Len=0 MSS=1400 SACK_PERM WS=128 [SYN, ACK] 50746 → 80	66	TCP	192.168.1.6	128.119.245.12	20:40:43.964299 2025-03-03	60
Seq=1 Ack=1 Win=65792 Len=0 [ACK] 80 → 50746	54	TCP	128.119.245.12	192.168.1.6	20:40:43.964380 2025-03-03	61
Seq=5126 Ack=1918 Win=143872 Len=0 [ACK] 50745 → 443	54	TCP	192.168.1.6	146.75.53.91	20:40:44.022024 2025-03-03	62
Application Data	119	TLSv1.3	192.168.1.6	146.75.53.91	20:40:44.023240 2025-03-03	63
Seq=5126 Ack=2010 Win=143872 Len=0 [ACK] 50745 → 443	54	TCP	192.168.1.6	146.75.53.91	20:40:44.023448 2025-03-03	64
Seq=2612 Ack=5191 Win=66048 Len=0 [ACK] 443 → 50745	54	TCP	146.75.53.91	192.168.1.6	20:40:44.023497 2025-03-03	65
Application Data	85	TLSv1.3	146.75.53.91	192.168.1.6	20:40:44.023691 2025-03-03	66
Seq=5191 Ack=2275 Win=146432 Len=0 [ACK] 50745 → 443	54	TCP	192.168.1.6	146.75.53.91	20:40:44.026124 2025-03-03	67
Seq=5191 Ack=2612 Win=149504 Len=0 [ACK] 50745 → 443	54	TCP	192.168.1.6	146.75.53.91	20:40:44.029906 2025-03-03	68
Application Data	379	TLSv1.3	192.168.1.6	146.75.53.91	20:40:44.052967 2025-03-03	69
Seq=2643 Ack=5516 Win=65792 Len=0 [ACK] 443 → 50745	54	TCP	146.75.53.91	192.168.1.6	20:40:44.098960 2025-03-03	70
Seq=1 Ack=482 Win=30336 Len=0 [ACK] 50744 → 80	54	TCP	192.168.1.6	128.119.245.12	20:40:44.123058 2025-03-03	71
Seq=1 Ack=482 Win=30336 Len=1400 [TCP PDU reassembled in 76] [ACK] 50744 → 80	1454	TCP	192.168.1.6	128.119.245.12	20:40:44.123514 2025-03-03	72
Seq=1401 Ack=482 Win=30336 Len=1400 [TCP PDU reassembled in 76] [ACK] 50744 → 80	1454	TCP	192.168.1.6	128.119.245.12	20:40:44.123657 2025-03-03	73
Seq=482 Ack=2801 Win=65792 Len=0 [ACK] 80 → 50744	54	TCP	128.119.245.12	192.168.1.6	20:40:44.123714 2025-03-03	74
Seq=2801 Ack=482 Win=30336 Len=1400 [TCP PDU reassembled in 76] [ACK] 50744 → 80	1454	TCP	192.168.1.6	128.119.245.12	20:40:44.124142 2025-03-03	75
HTTP/1.1 200 OK (text/html)	715	HTTP	192.168.1.6	128.119.245.12	20:40:44.124221 2025-03-03	76

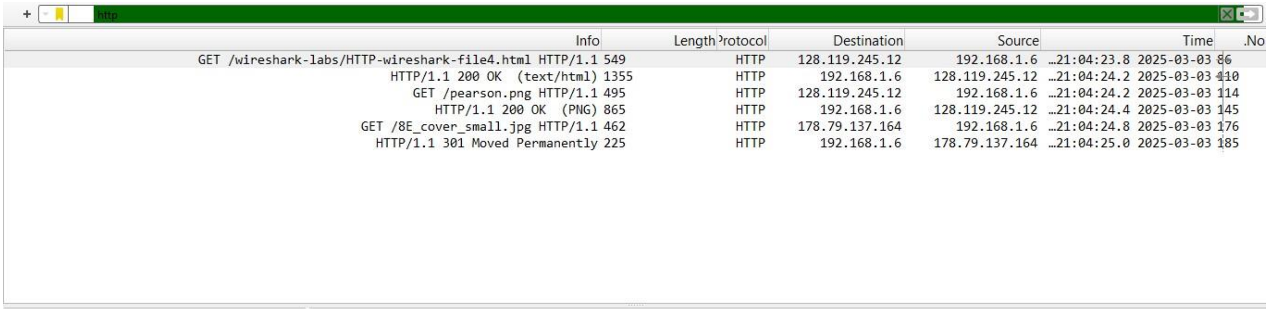
Part V:

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



This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France:

And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.



Info	Length	Protocol	Destination	Source	Time	.No
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1	549	HTTP	128.119.245.12	192.168.1.6	…21:04:23.8 2025-03-03	86
HTTP/1.1 200 OK (text/html)	1355	HTTP	192.168.1.6	128.119.245.12	…21:04:24.2 2025-03-03	110
GET /pearson.png HTTP/1.1	495	HTTP	128.119.245.12	192.168.1.6	…21:04:24.2 2025-03-03	114
HTTP/1.1 200 OK (PNG)	865	HTTP	192.168.1.6	128.119.245.12	…21:04:24.4 2025-03-03	145
GET /8E_cover_small.jpg HTTP/1.1	462	HTTP	178.79.137.164	192.168.1.6	…21:04:24.8 2025-03-03	176
HTTP/1.1 301 Moved Permanently	225	HTTP	192.168.1.6	178.79.137.164	…21:04:25.0 2025-03-03	185

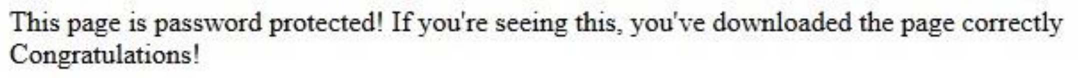
3 GET requests to addresses 2 sent to 128.119.245.12 and one to 178.79.137.164

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.

the browser downloaded 2 images serially as get for first image and response for first then get for second and response for the second.

Part VI:

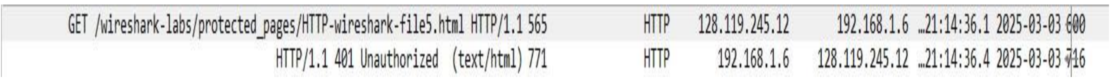
HTTP Authentication



This page is password protected! If you're seeing this, you've downloaded the page correctly Congratulations!

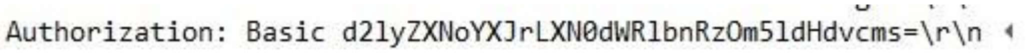
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

401 UNUTHORIZED

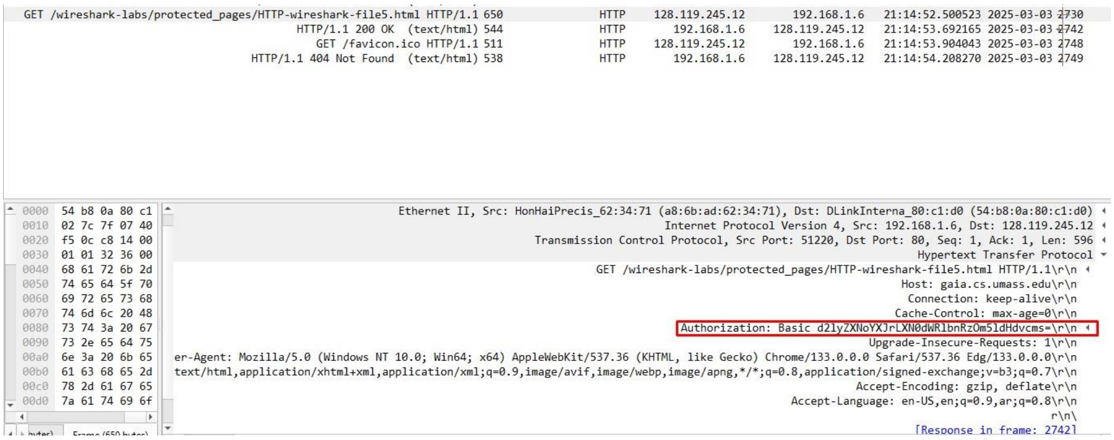


```
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 565   HTTP  128.119.245.12   192.168.1.6  …21:14:36.1 2025-03-03 600
                            HTTP/1.1 401 Unauthorized  (text/html) 771   HTTP     192.168.1.6  128.119.245.12 …21:14:36.4 2025-03-03 716
```

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
```



```
GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1 650   HTTP  128.119.245.12    192.168.1.6  21:14:52.500523 2025-03-03 2730
                              HTTP/1.1 200 OK  (text/html) 544           HTTP     192.168.1.6 128.119.245.12  21:14:53.692165 2025-03-03 2742
                                GET /favicon.ico HTTP/1.1 511            HTTP  128.119.245.12    192.168.1.6  21:14:53.904043 2025-03-03 2748
                        HTTP/1.1 404 Not Found  (text/html) 538          HTTP     192.168.1.6 128.119.245.12  21:14:54.208270 2025-03-03 2749

0000  54 b8 0a 80 c1      Ethernet II, Src: HonHaiPrecis_62:34:71 (a8:6b:ad:62:34:71), Dst: DLinkInterna_80:c1:d0 (54:b8:0a:80:c1:d0)
0010  02 7c 7f 07 40      Internet Protocol Version 4, Src: 192.168.1.6, Dst: 128.119.245.12
0020  f5 0c c8 14 00      Transmission Control Protocol, Src Port: 51220, Dst Port: 80, Seq: 1, Ack: 1, Len: 596
0030  01 01 32 36 00      Hypertext Transfer Protocol
0040  68 61 72 6b 2d      GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
0050  74 65 64 5f 70      Host: gaia.cs.umass.edu\r\n
0060  69 72 65 73 68      Connection: keep-alive\r\n
0070  74 6d 6c 20 48      Cache-Control: max-age=0\r\n
0080  73 74 3a 20 67      Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
0090  73 2e 65 64 75      Upgrade-Insecure-Requests: 1\r\n
00a0  6e 3a 20 6b 65      er-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 Edg/133.0.0.0\r\n
00b0  61 63 68 65 2d      text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
00c0  78 2d 61 67 65      Accept-Encoding: gzip, deflate\r\n
00d0  7a 61 74 69 6f      Accept-Language: en-US,en;q=0.9,ar;q=0.8\r\n
                          r\n\
                          [Response in frame: 2742]
```