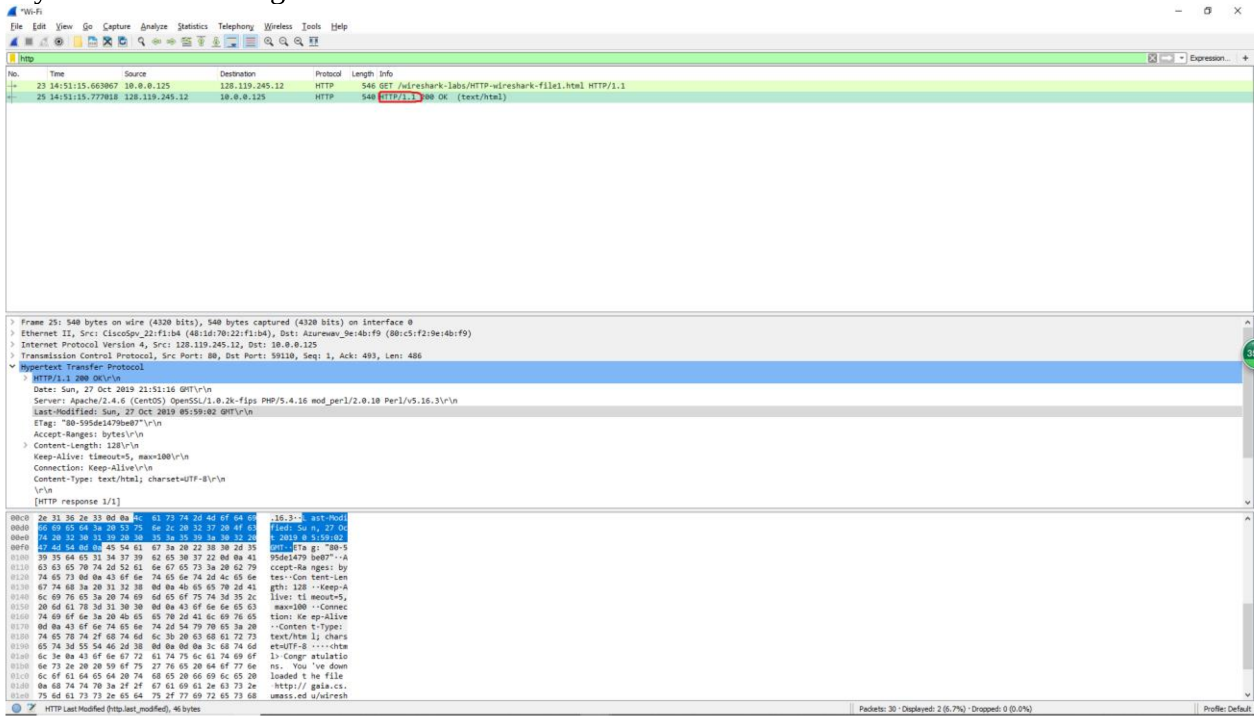
Hao (Jeff) Deng
ID: 932912420

CS 372 – Lab 2

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



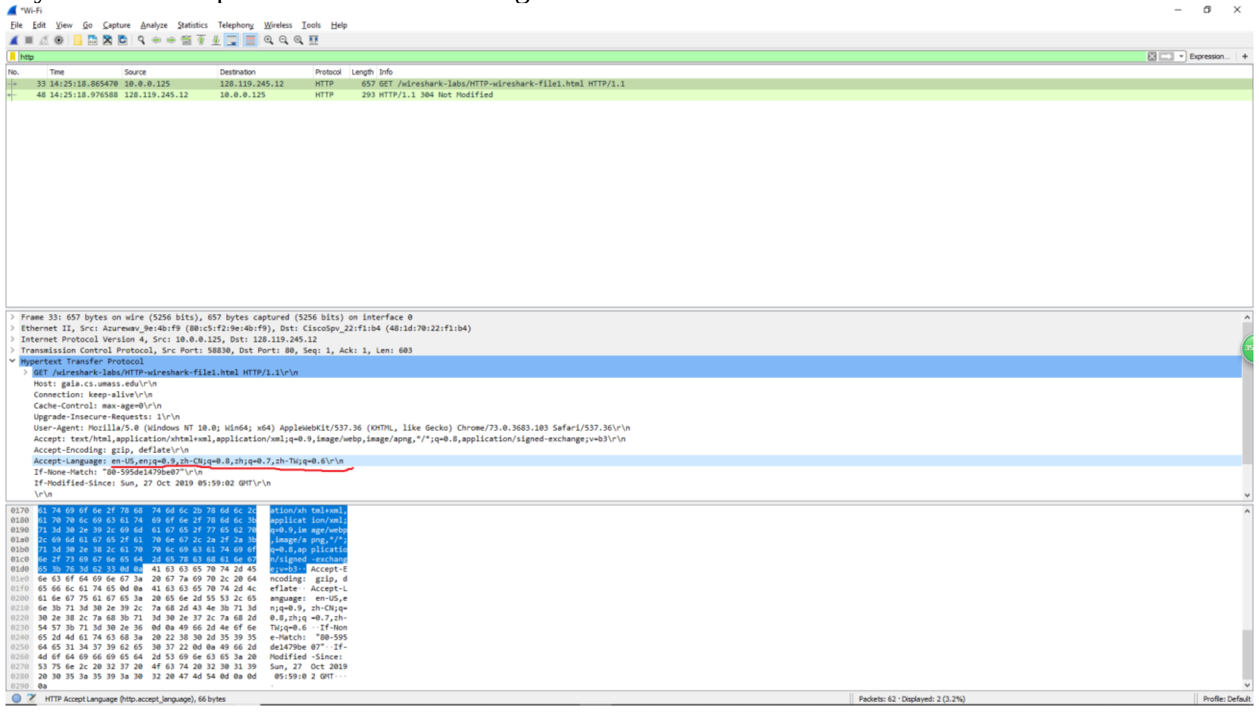
```
No.  Time             Source          Destination     Protocol  Length  Info
  23 14:51:15.663067  10.0.0.125      128.119.245.12  HTTP         546  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  25 14:51:15.777018  128.119.245.12  10.0.0.125      HTTP         540  HTTP/1.1 200 OK  (text/html)
```

```
> Frame 25: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 59110, Seq: 1, Ack: 493, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 27 Oct 2019 21:51:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "80-595de1479be07"\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]
```

```
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 37 20 4f 63   fied: Su n, 27 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 32 20   t 2019 0 5:59:02 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 35 64 65 31 34 37 39  62 65 30 37 22 0d 0a 41   95de1479 be07"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh
```

```
HTTP Last Modified (http.last_modified), 46 bytes    Packets: 30 · Displayed: 2 (6.7%) · Dropped: 0 (0.0%)    Profile: Default
```

2. What languages (if any) does your browser indicate that it can accept to the server?
   My browser accepts both Chinese and English



```
No.  Time             Source          Destination     Protocol  Length  Info
  33 14:25:18.865470  10.0.0.125      128.119.245.12  HTTP         657  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  48 14:25:18.976588  128.119.245.12  10.0.0.125      HTTP         293  HTTP/1.1 304 Not Modified
```

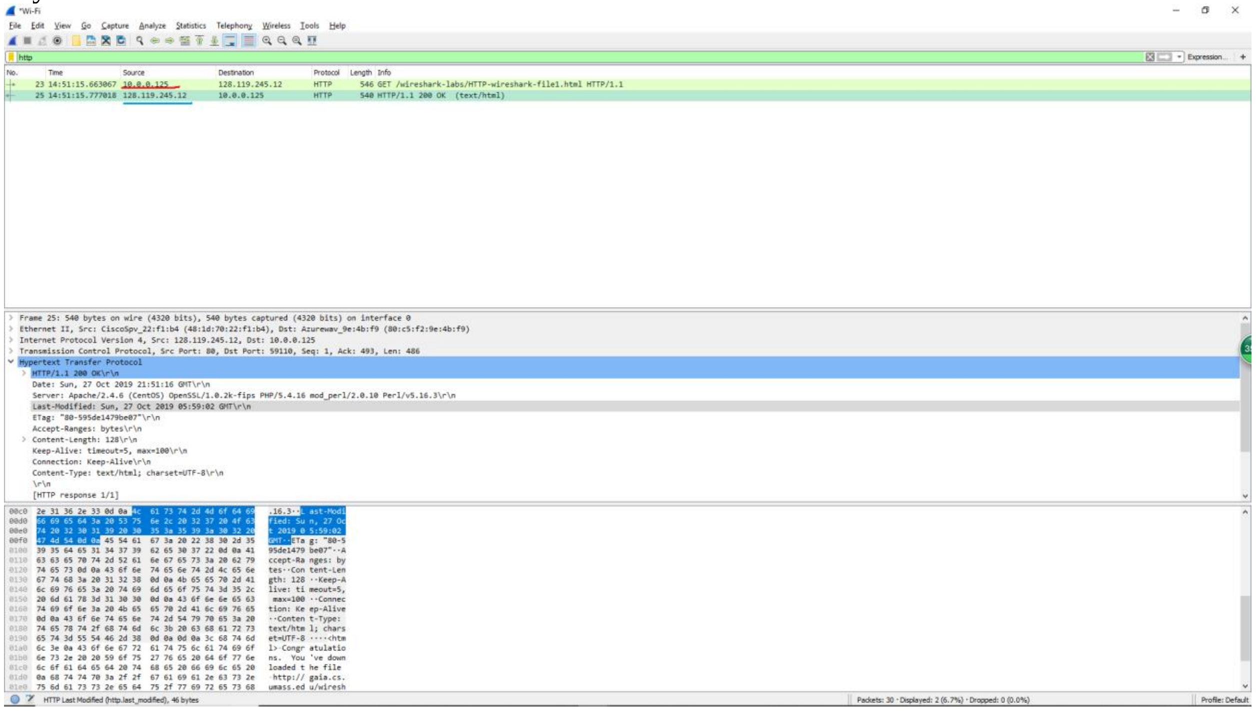
```
> Frame 33: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits) on interface 0
> Ethernet II, Src: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9), Dst: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4)
> Internet Protocol Version 4, Src: 10.0.0.125, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58830, Dst Port: 80, Seq: 1, Ack: 1, Len: 603
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.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
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.6\r\n
    If-None-Match: "80-595de1479be07"\r\n
    If-Modified-Since: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    \r\n
```

```
0170  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0180  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0190  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 77 65 62 70   q=0.9,im age/webp
01a0  2c 69 6d 61 67 65 2f 61  70 6e 67 2c 2a 2f 2a 3b   ,image/a png,*/*;
01b0  71 3d 30 2e 38 2c 61 70  70 6c 69 63 61 74 69 6f   q=0.8,ap plicatio
01c0  6e 2f 73 69 67 6e 65 64  2d 65 78 63 68 61 6e 67   n/signed -exchang
01d0  65 3b 76 3d 62 33 0d 0a  41 63 63 65 70 74 2d 45   e;v=b3·· Accept-E
01e0  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 2c 20 64   ncoding:  gzip, d
01f0  65 66 6c 61 74 65 0d 0a  41 63 63 65 70 74 2d 4c   eflate·· Accept-L
0200  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
0210  6e 3b 71 3d 30 2e 39 2c  7a 68 2d 43 4e 3b 71 3d   n;q=0.9, zh-CN;q=
0220  30 2e 38 2c 7a 68 3b 71  3d 30 2e 37 2c 7a 68 2d   0.8,zh;q =0.7,zh-
0230  54 57 3b 71 3d 30 2e 36  0d 0a 49 66 2d 4e 6f 6e   TW;q=0.6 ··If-Non
0240  65 2d 4d 61 74 63 68 3a  20 22 38 30 2d 35 39 35   e-Match:  "80-595
0250  64 65 31 34 37 39 62 65  30 37 22 0d 0a 49 66 2d   de1479be 07"··If-
0260  4d 6f 64 69 66 69 65 64  2d 53 69 6e 63 65 3a 20   Modified -Since: 
0270  53 75 6e 2c 20 32 37 20  4f 63 74 20 32 30 31 39   Sun, 27  Oct 2019
0280  20 30 35 3a 35 39 3a 30  32 20 47 4d 54 0d 0a 0d    05:59:0 2 GMT···
0290  0a                                                 ·
```

```
HTTP Accept Language (http.accept_language), 66 bytes    Packets: 62 · Displayed: 2 (3.2%)    Profile: Default
```

Hao (Jeff) Deng
ID: 932912420

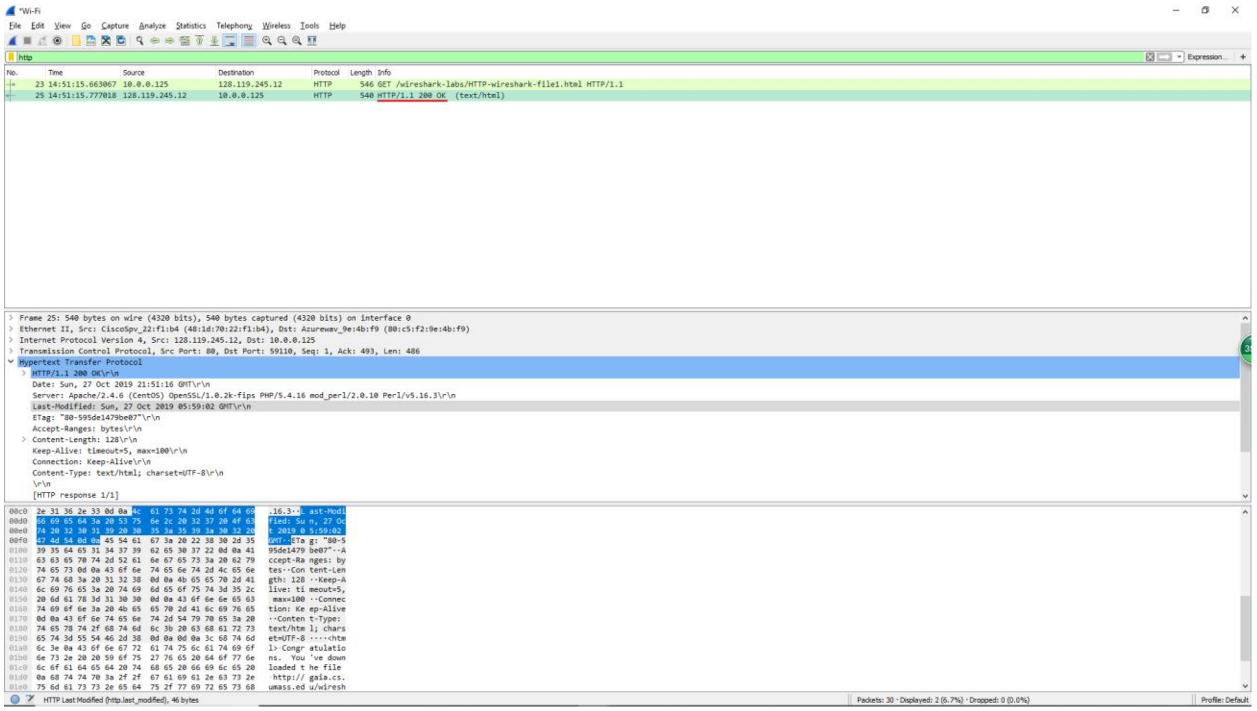
3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?
   My IP address is 10.0.0.125 and the server is 128.119.245.12



```
No.   Time              Source          Destination     Protocol Length Info
   23 14:51:15.663067   10.0.0.125      128.119.245.12  HTTP     546 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   25 14:51:15.777018   128.119.245.12  10.0.0.125      HTTP     540 HTTP/1.1 200 OK  (text/html)

> Frame 25: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 59110, Seq: 1, Ack: 493, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 27 Oct 2019 21:51:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "80-595de1479be07"\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]

00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 37 20 4f 63   fied: Su n, 27 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 32 20   t 2019 0 5:59:02 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 35 64 65 31 34 37 39  62 65 30 37 22 0d 0a 41   95de1479 be07"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh

HTTP Last Modified (http.last_modified), 46 bytes    Packets: 30 · Displayed: 2 (6.7%) · Dropped: 0 (0.0%)    Profile: Default
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

4. What is the status code returned from the server to your browser?
   The status code is 200 OK

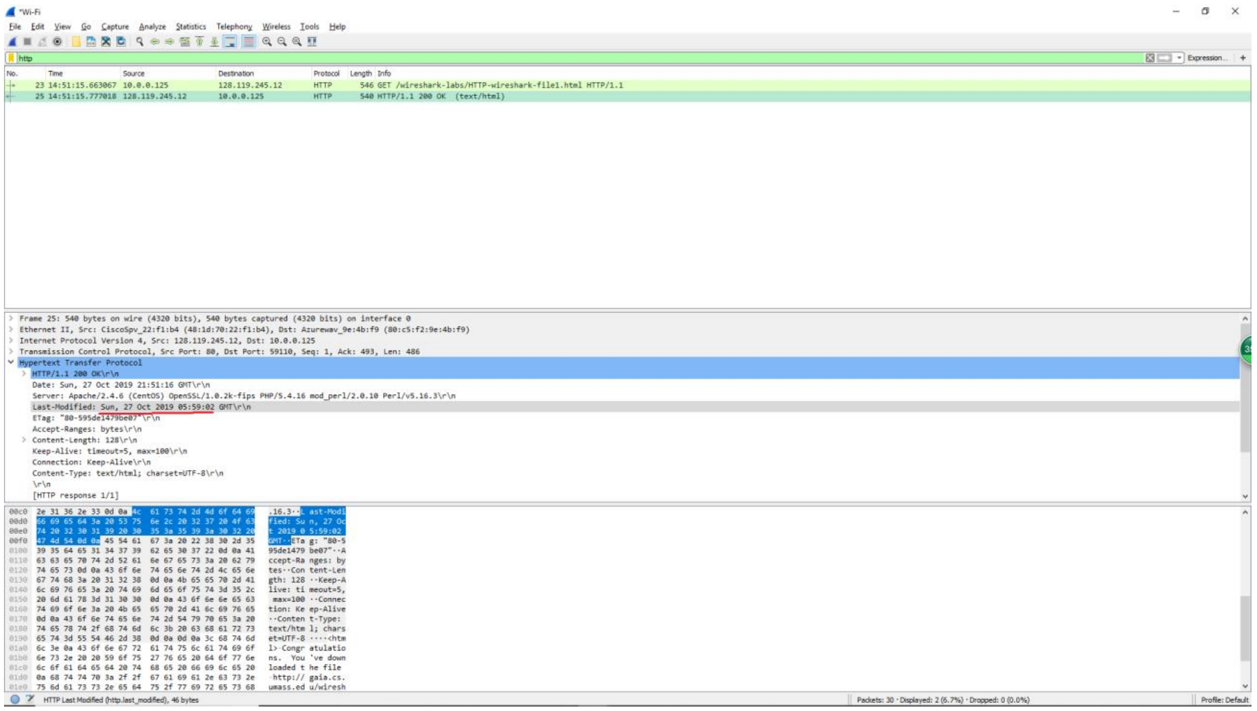


```
No.   Time              Source          Destination     Protocol Length Info
   23 14:51:15.663067   10.0.0.125      128.119.245.12  HTTP     546 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   25 14:51:15.777018   128.119.245.12  10.0.0.125      HTTP     540 HTTP/1.1 200 OK  (text/html)

> Frame 25: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 59110, Seq: 1, Ack: 493, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 27 Oct 2019 21:51:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "80-595de1479be07"\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]

00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 37 20 4f 63   fied: Su n, 27 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 32 20   t 2019 0 5:59:02 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 35 64 65 31 34 37 39  62 65 30 37 22 0d 0a 41   95de1479 be07"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh

HTTP Last Modified (http.last_modified), 46 bytes    Packets: 30 · Displayed: 2 (6.7%) · Dropped: 0 (0.0%)    Profile: Default
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

5. When was the HTML file that you are retrieving last modified at the server?
   Last modified was on Sunday October 27th, 2019 at 5:59:02 GMT.

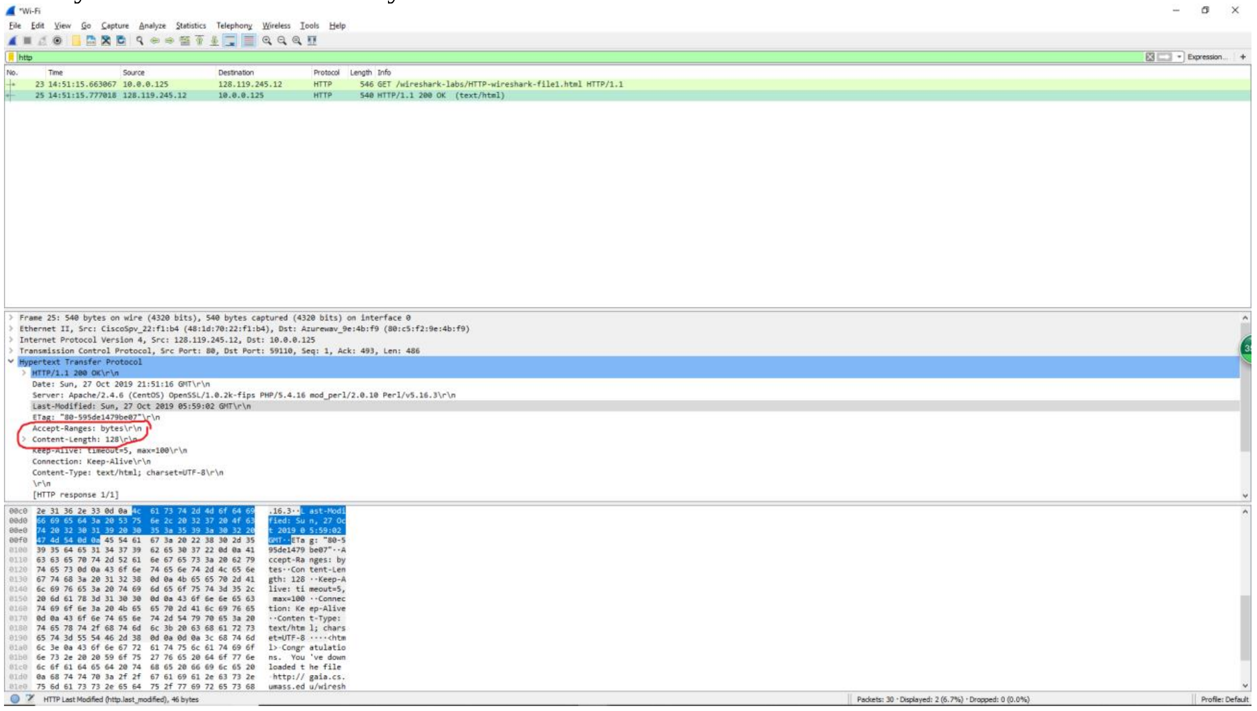
Hao (Jeff) Deng
ID: 932912420



```
http

No.  Time             Source          Destination     Protocol Length Info
  23 14:51:15.663067  10.0.0.125      128.119.245.12  HTTP     546 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  25 14:51:15.777018  128.119.245.12  10.0.0.125      HTTP     540 HTTP/1.1 200 OK  (text/html)

> Frame 25: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 59110, Seq: 1, Ack: 493, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 27 Oct 2019 21:51:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "80-595de1479be07"\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]

00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 37 20 4f 63   fied: Su n, 27 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 32 20   t 2019 0 5:59:02 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 35 64 65 31 34 37 39  62 65 30 37 22 0d 0a 41   95de1479 be07"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh

HTTP Last Modified (http.last_modified), 46 bytes    Packets: 30 · Displayed: 2 (6.7%) · Dropped: 0 (0.0%)    Profile: Default
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

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



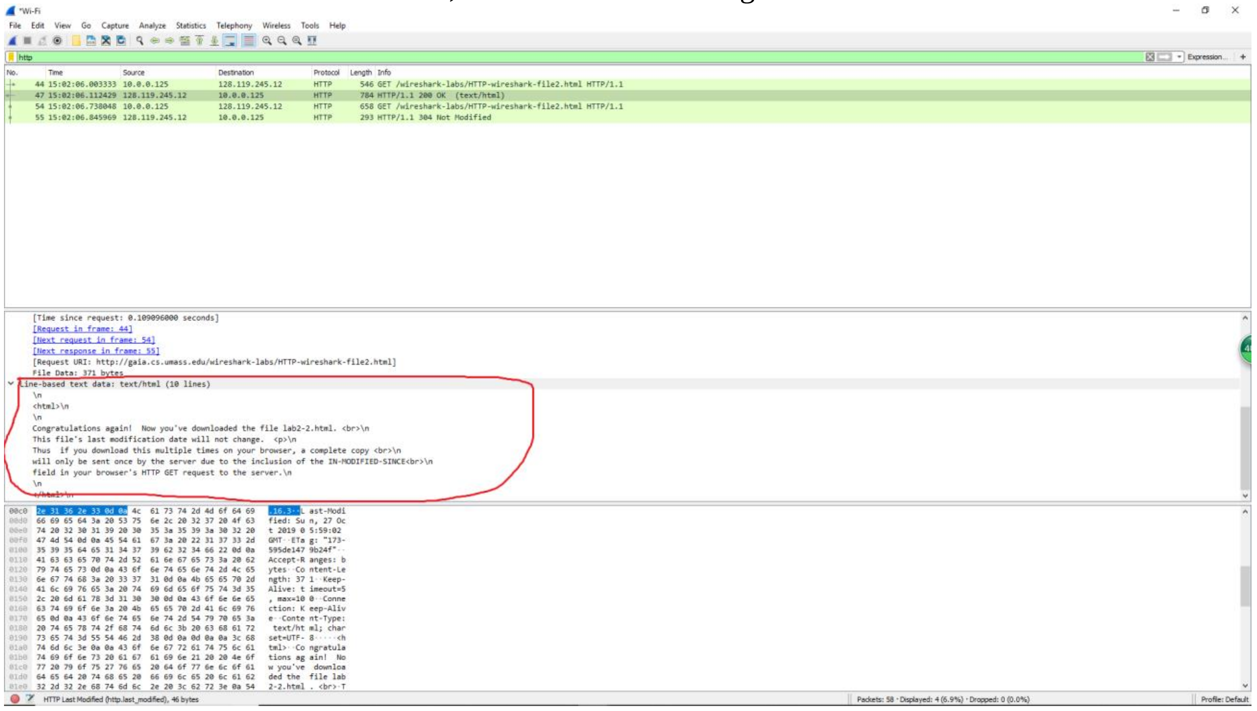
```
http

No.  Time             Source          Destination     Protocol Length Info
  23 14:51:15.663067  10.0.0.125      128.119.245.12  HTTP     546 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  25 14:51:15.777018  128.119.245.12  10.0.0.125      HTTP     540 HTTP/1.1 200 OK  (text/html)

> Frame 25: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 59110, Seq: 1, Ack: 493, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Sun, 27 Oct 2019 21:51:16 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "80-595de1479be07"\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]

00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 37 20 4f 63   fied: Su n, 27 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 32 20   t 2019 0 5:59:02 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 38 30 2d 35   GMT··ETa g: "80-5
0100  39 35 64 65 31 34 37 39  62 65 30 37 22 0d 0a 41   95de1479 be07"··A
0110  63 63 65 70 74 2d 52 61  6e 67 65 73 3a 20 62 79   ccept-Ra nges: by
0120  74 65 73 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   tes··Con tent-Len
0130  67 74 68 3a 20 31 32 38  0d 0a 4b 65 65 70 2d 41   gth: 128 ··Keep-A
0140  6c 69 76 65 3a 20 74 69  6d 65 6f 75 74 3d 35 2c   live: ti meout=5,
0150  20 6d 61 78 3d 31 30 30  0d 0a 43 6f 6e 6e 65 63    max=100 ··Connec
0160  74 69 6f 6e 3a 20 4b 65  65 70 2d 41 6c 69 76 65   tion: Ke ep-Alive
0170  0d 0a 43 6f 6e 74 65 6e  74 2d 54 79 70 65 3a 20   ··Conten t-Type: 
0180  74 65 78 74 2f 68 74 6d  6c 3b 20 63 68 61 72 73   text/htm l; chars
0190  65 74 3d 55 54 46 2d 38  0d 0a 0d 0a 3c 68 74 6d   et=UTF-8 ····<htm
01a0  6c 3e 0a 43 6f 6e 67 72  61 74 75 6c 61 74 69 6f   l>·Congr atulatio
01b0  6e 73 2e 20 20 59 6f 75  27 76 65 20 64 6f 77 6e   ns.  You 've down
01c0  6c 6f 61 64 65 64 20 74  68 65 20 66 69 6c 65 20   loaded t he file 
01d0  0a 68 74 74 70 3a 2f 2f  67 61 69 61 2e 63 73 2e   ·http:// gaia.cs.
01e0  75 6d 61 73 73 2e 65 64  75 2f 77 69 72 65 73 68   umass.ed u/wiresh

HTTP Last Modified (http.last_modified), 46 bytes    Packets: 30 · Displayed: 2 (6.7%) · Dropped: 0 (0.0%)    Profile: Default
```

7. By inspecting the raw data in the packet content window, do you see any headers within
   No, I don’t see any see any headers within.

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?
   From the first HTTP Get request, I am not able to see an IF-MODIFIED-SINCE line

Hao (Jeff) Deng
ID: 932912420

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
   The server did explicitly return the contents of the file. At the bottom of the window, there's a section called Line-based text data, and the content is being stored inside.



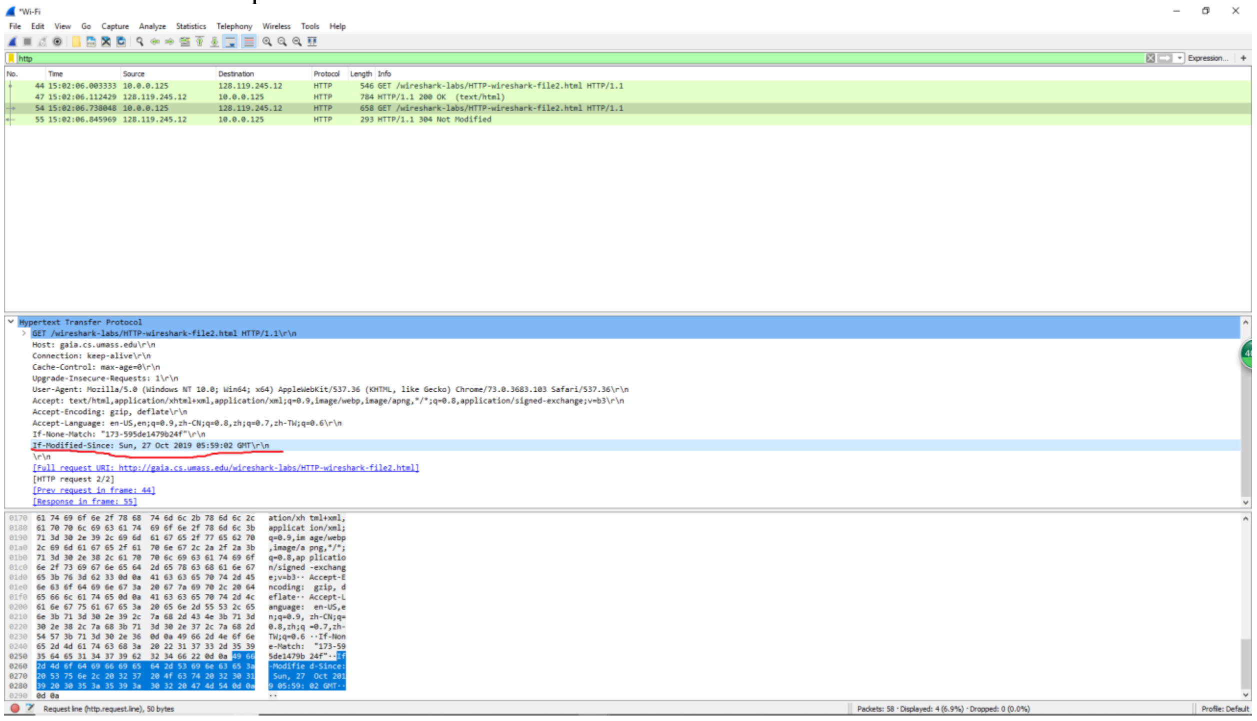
```
No.   Time            Source          Destination     Protocol Length Info
   44 15:02:06.003333 10.0.0.125      128.119.245.12  HTTP      546 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   47 15:02:06.112429 128.119.245.12  10.0.0.125      HTTP      784 HTTP/1.1 200 OK  (text/html)
   54 15:02:06.738048 10.0.0.125      128.119.245.12  HTTP      658 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   55 15:02:06.845969 128.119.245.12  10.0.0.125      HTTP      293 HTTP/1.1 304 Not Modified
```

```
    [Time since request: 0.109096000 seconds]
    [Request in frame: 44]
    [Next request in frame: 54]
    [Next response in frame: 55]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
v 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
```

```
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3··L ast-Modi
00d0  66 69 65 64 3a 20 53 75  6e 2c 20 32 37 20 4f 63   fied: Su n, 27 Oc
00e0  74 20 32 30 31 39 20 30  35 3a 35 39 3a 30 32 20   t 2019 0 5:59:02 
00f0  47 4d 54 0d 0a 45 54 61  67 3a 20 22 31 37 33 2d   GMT··ETa g: "173-
0100  35 39 35 64 65 31 34 37  39 62 32 34 66 22 0d 0a   595de147 9b24f"··
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
```

```
HTTP Last Modified (http.last_modified), 46 bytes    Packets: 58 · Displayed: 4 (6.9%) · Dropped: 0 (0.0%)    Profile: Default
```

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?
    The second GET request does contain the IF-MODIFIED-SINCE header.



```
No.   Time            Source          Destination     Protocol Length Info
   44 15:02:06.003333 10.0.0.125      128.119.245.12  HTTP      546 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   47 15:02:06.112429 128.119.245.12  10.0.0.125      HTTP      784 HTTP/1.1 200 OK  (text/html)
   54 15:02:06.738048 10.0.0.125      128.119.245.12  HTTP      658 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   55 15:02:06.845969 128.119.245.12  10.0.0.125      HTTP      293 HTTP/1.1 304 Not Modified
```

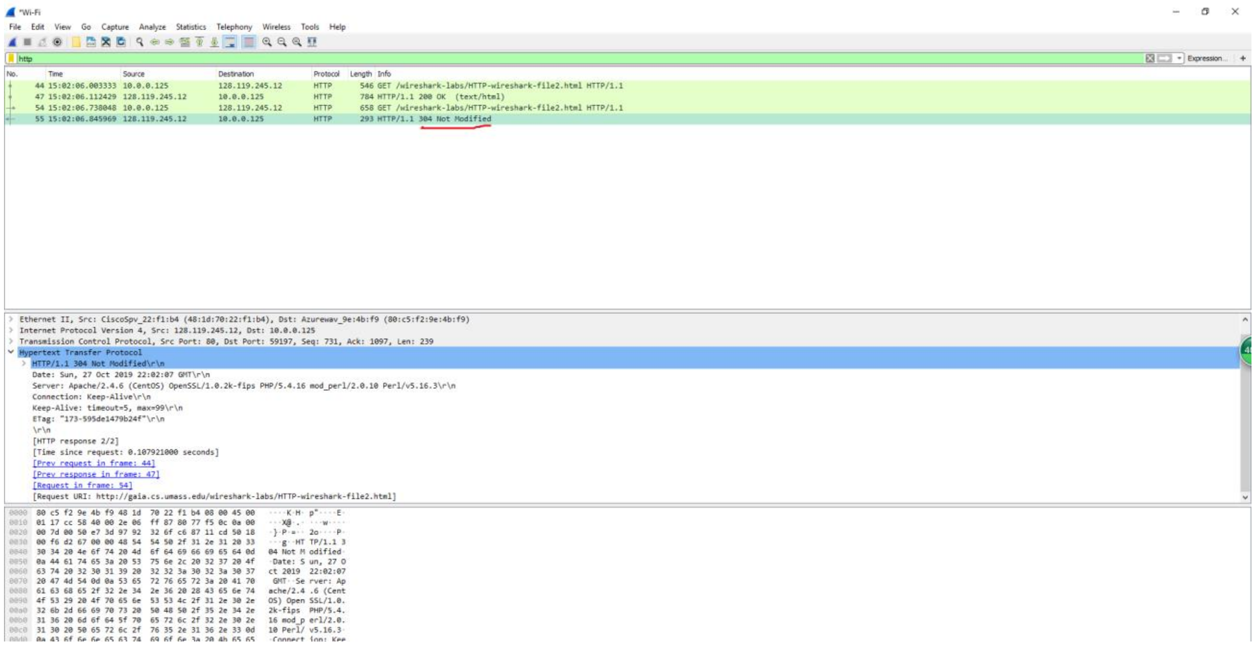
```
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.6\r\n
    If-None-Match: "173-595de1479b24f"\r\n
    If-Modified-Since: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 44]
    [Response in frame: 55]
```

```
0170  61 74 69 6f 6e 2f 78 68  74 6d 6c 2b 78 6d 6c 2c   ation/xh tml+xml,
0180  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 6d 6c 3b   applicat ion/xml;
0190  71 3d 30 2e 39 2c 69 6d  61 67 65 2f 77 65 62 70   q=0.9,im age/webp
01a0  2c 69 6d 61 67 65 2f 61  70 6e 67 2c 2a 2f 2a 3b   ,image/a png,*/*;
01b0  71 3d 30 2e 38 2c 61 70  70 6c 69 63 61 74 69 6f   q=0.8,ap plicatio
01c0  6e 2f 73 69 67 6e 65 64  2d 65 78 63 68 61 6e 67   n/signed -exchang
01d0  65 3b 76 3d 62 33 0d 0a  41 63 63 65 70 74 2d 45   e;v=b3·· Accept-E
01e0  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 2c 20 64   ncoding:  gzip, d
01f0  65 66 6c 61 74 65 0d 0a  41 63 63 65 70 74 2d 4c   eflate·· Accept-L
0200  61 6e 67 75 61 67 65 3a  20 65 6e 2d 55 53 2c 65   anguage:  en-US,e
0210  6e 3b 71 3d 30 2e 39 2c  7a 68 2d 43 4e 3b 71 3d   n;q=0.9, zh-CN;q=
0220  30 2e 38 2c 7a 68 3b 71  3d 30 2e 37 2c 7a 68 2d   0.8,zh;q =0.7,zh-
0230  54 57 3b 71 3d 30 2e 36  0d 0a 49 66 2d 4e 6f 6e   TW;q=0.6 ··If-Non
0240  65 2d 4d 61 74 63 68 3a  20 22 31 37 33 2d 35 39   e-Match:  "173-59
0250  35 64 65 31 34 37 39 62  32 34 66 22 0d 0a 49 66   5de1479b 24f"··If
0260  2d 4d 6f 64 69 66 69 65  64 2d 53 69 6e 63 65 3a   -Modifie d-Since:
0270  20 53 75 6e 2c 20 32 37  20 4f 63 74 20 32 30 31    Sun, 27  Oct 201
0280  39 20 30 35 3a 35 39 3a  30 32 20 47 4d 54 0d 0a   9 05:59: 02 GMT··
0290  0d 0a                                              ··
```

```
Request line (http.request.line), 50 bytes    Packets: 58 · Displayed: 4 (6.9%) · Dropped: 0 (0.0%)    Profile: Default
```

Hao (Jeff) Deng
ID: 932912420

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.
The status code is 304 Not Modified and the server did not explicitly return the contents of the file. It is because the browser simply retrieved the file from its cache. It would have returned the contents of the file if the file has been modified since last time, but instead it simply told the browser to retrieve the old file from the cache.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...

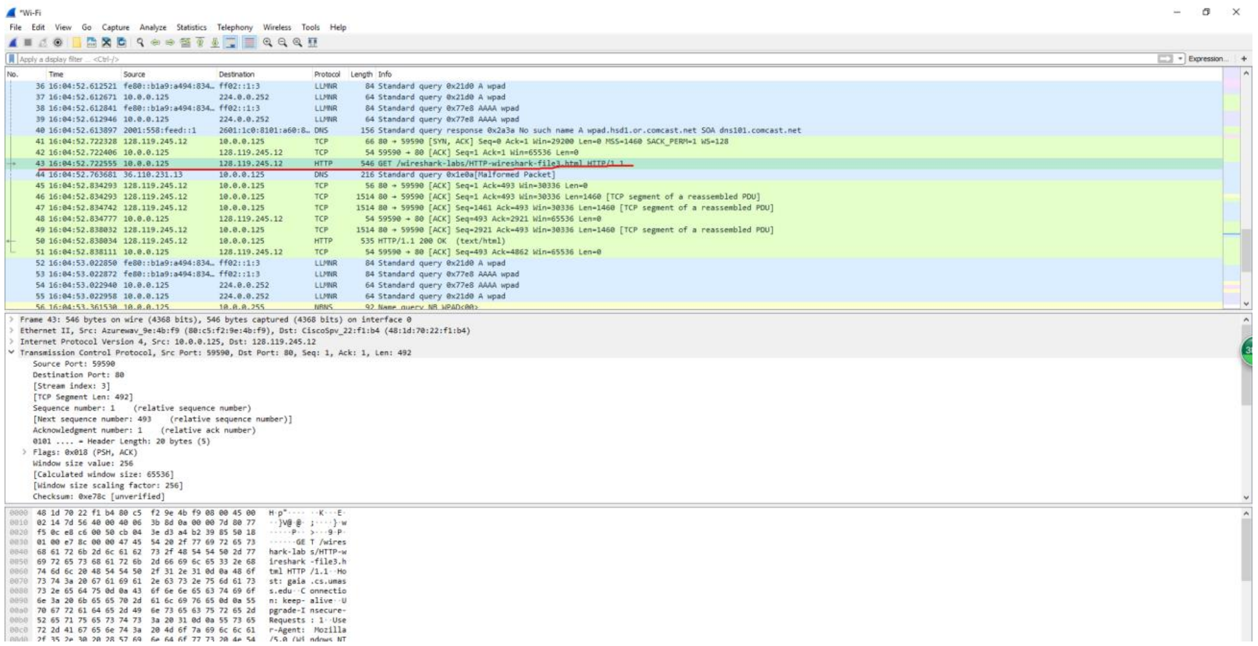
```
No.  Time             Source          Destination     Protocol Length Info
  44 15:02:06.003333  10.0.0.125      128.119.245.12  HTTP     546 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  47 15:02:06.112429  128.119.245.12  10.0.0.125      HTTP     784 HTTP/1.1 200 OK  (text/html)
  54 15:02:06.738048  10.0.0.125      128.119.245.12  HTTP     658 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  55 15:02:06.845969  128.119.245.12  10.0.0.125      HTTP     293 HTTP/1.1 304 Not Modified
```

```
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 59197, Seq: 731, Ack: 1097, Len: 239
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Sun, 27 Oct 2019 22:02:07 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-595de1479b24f"\r\n
    \r\n
    [HTTP response 2/2]
    [Time since request: 0.107921000 seconds]
    [Prev request in frame: 44]
    [Prev response in frame: 47]
    [Request in frame: 54]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

```
0000  80 c5 f2 9e 4b f9 48 1d  70 22 f1 b4 08 00 45 00   ····K·H· p"····E·
0010  01 17 cc 58 40 00 2e 06  ff 87 80 77 f5 0c 0a 00   ···X@·.· ···w····
0020  00 7d 00 50 e7 3d 97 92  32 6f c6 87 11 cd 50 18   ·}·P·=·· 2o····P·
0030  00 f6 d2 67 00 00 48 54  54 50 2f 31 2e 31 20 33   ···g··HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 53  75 6e 2c 20 32 37 20 4f   ·Date: S un, 27 O
0060  63 74 20 32 30 31 39 20  32 32 3a 30 32 3a 30 37   ct 2019  22:02:07
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
00b0  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
00c0  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3·
00d0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
```

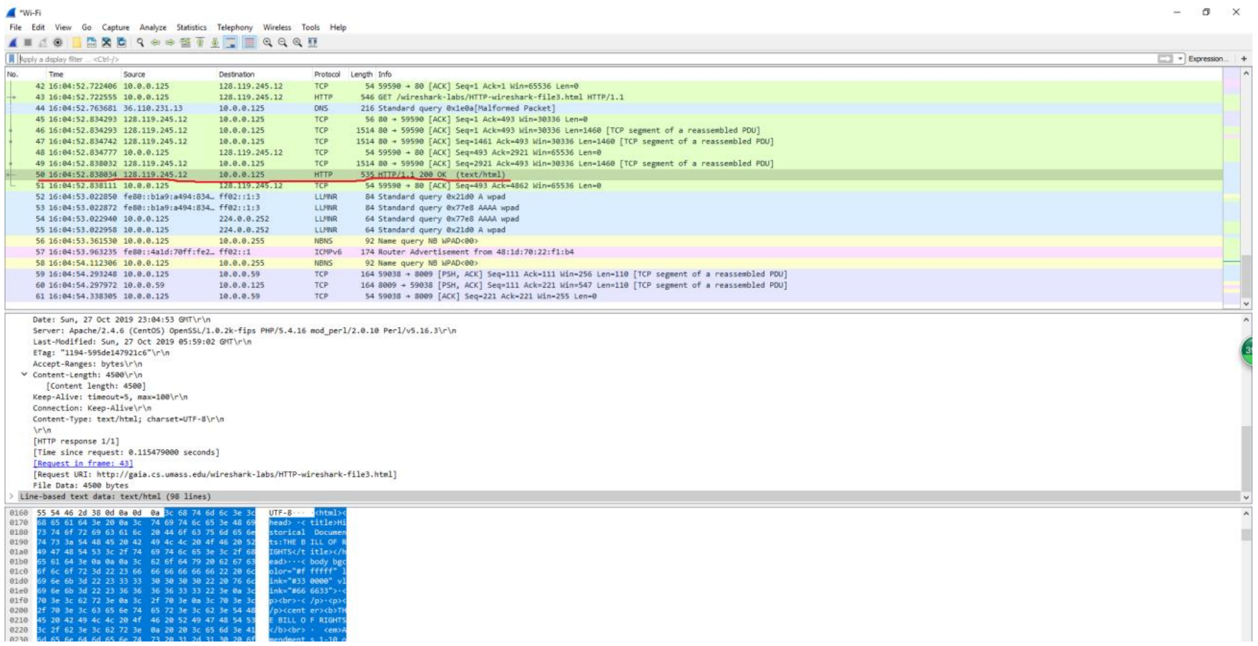
12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
My browser only sent 1 HTTP GET message and the packet number is 43

Hao (Jeff) Deng
ID: 932912420



```
No.  Time             Source                 Destination            Protocol Length Info
  36 16:04:52.612521  fe80::b1a9:a494:834…   ff02::1:3              LLMNR      84 Standard query 0x21d0 A wpad
  37 16:04:52.612671  10.0.0.125             224.0.0.252            LLMNR      64 Standard query 0x21d0 A wpad
  38 16:04:52.612841  fe80::b1a9:a494:834…   ff02::1:3              LLMNR      84 Standard query 0x77e8 AAAA wpad
  39 16:04:52.612946  10.0.0.125             224.0.0.252            LLMNR      64 Standard query 0x77e8 AAAA wpad
  40 16:04:52.613897  2001:558:feed::1       2601:1c0:8101:a60:8…   DNS       156 Standard query response 0x2a3a No such name A wpad.hsd1.or.comcast.net SOA dns101.comcast.net
  41 16:04:52.722328  128.119.245.12         10.0.0.125             TCP        66 80 → 59590 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
  42 16:04:52.722406  10.0.0.125             128.119.245.12         TCP        54 59590 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  43 16:04:52.722555  10.0.0.125             128.119.245.12         HTTP      546 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 16:04:52.763681  36.110.231.13          10.0.0.125             DNS       216 Standard query 0x1e0a[Malformed Packet]
  45 16:04:52.834293  128.119.245.12         10.0.0.125             TCP        56 80 → 59590 [ACK] Seq=1 Ack=493 Win=30336 Len=0
  46 16:04:52.834293  128.119.245.12         10.0.0.125             TCP      1514 80 → 59590 [ACK] Seq=1 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  47 16:04:52.834742  128.119.245.12         10.0.0.125             TCP      1514 80 → 59590 [ACK] Seq=1461 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  48 16:04:52.834777  10.0.0.125             128.119.245.12         TCP        54 59590 → 80 [ACK] Seq=493 Ack=2921 Win=65536 Len=0
  49 16:04:52.838032  128.119.245.12         10.0.0.125             TCP      1514 80 → 59590 [ACK] Seq=2921 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  50 16:04:52.838034  128.119.245.12         10.0.0.125             HTTP      535 HTTP/1.1 200 OK  (text/html)
  51 16:04:52.838111  10.0.0.125             128.119.245.12         TCP        54 59590 → 80 [ACK] Seq=493 Ack=4862 Win=65536 Len=0
  52 16:04:53.022850  fe80::b1a9:a494:834…   ff02::1:3              LLMNR      84 Standard query 0x21d0 A wpad
  53 16:04:53.022872  fe80::b1a9:a494:834…   ff02::1:3              LLMNR      84 Standard query 0x77e8 AAAA wpad
  54 16:04:53.022940  10.0.0.125             224.0.0.252            LLMNR      64 Standard query 0x77e8 AAAA wpad
  55 16:04:53.022958  10.0.0.125             224.0.0.252            LLMNR      64 Standard query 0x21d0 A wpad
  56 16:04:53.361530  10.0.0.125             10.0.0.255             NBNS       92 Name query NB WPAD<00>

> Frame 43: 546 bytes on wire (4368 bits), 546 bytes captured (4368 bits) on interface 0
> Ethernet II, Src: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9), Dst: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4)
> Internet Protocol Version 4, Src: 10.0.0.125, Dst: 128.119.245.12
v Transmission Control Protocol, Src Port: 59590, Dst Port: 80, Seq: 1, Ack: 1, Len: 492
    Source Port: 59590
    Destination Port: 80
    [Stream index: 3]
    [TCP Segment Len: 492]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 493    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0xe78c [unverified]

0000  48 1d 70 22 f1 b4 80 c5  f2 9e 4b f9 08 00 45 00   H·p"···· ··K···E·
0010  02 14 7d 56 40 00 40 06  3b 8d 0a 00 00 7d 80 77   ··}V@·@· ;····}·w
0020  f5 0c e8 c6 00 50 cb 04  3e d3 a4 b2 39 85 50 18   ·····P·· >···9·P·
0030  01 00 e7 8c 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 33 2e 68   ireshark -file3.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 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
```

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?
The packet number that associate with the HTTP GET request is 50

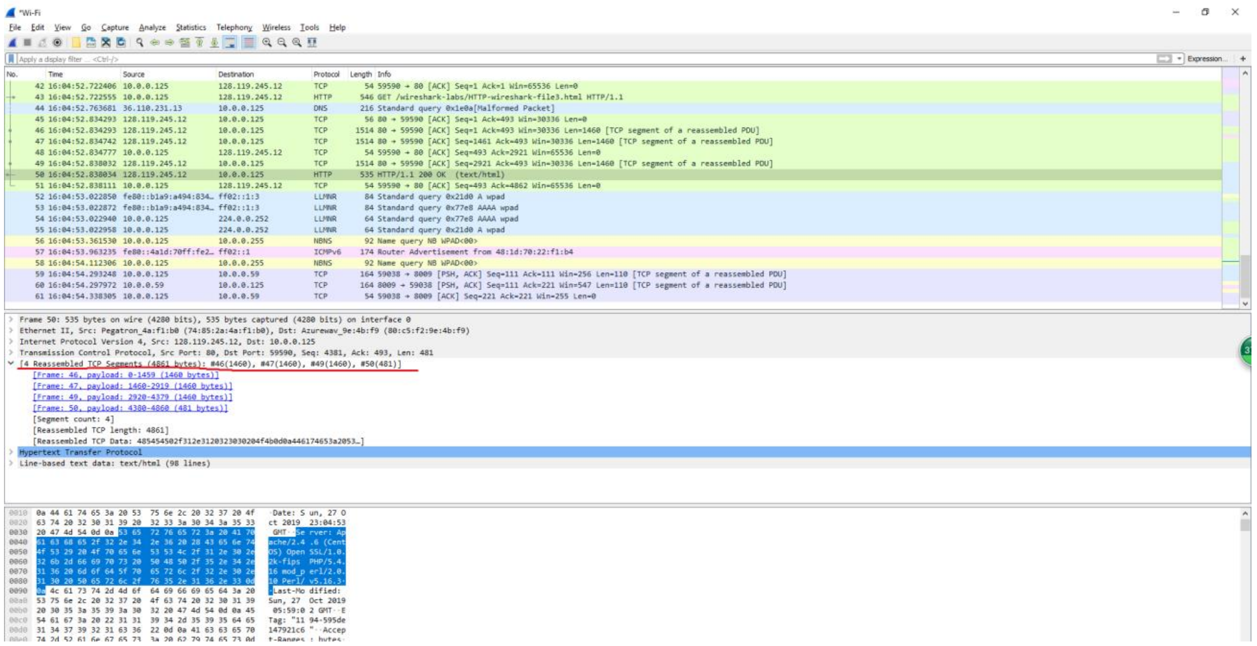


```
No.  Time             Source                 Destination            Protocol Length Info
  42 16:04:52.722406  10.0.0.125             128.119.245.12         TCP        54 59590 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  43 16:04:52.722555  10.0.0.125             128.119.245.12         HTTP      546 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 16:04:52.763681  36.110.231.13          10.0.0.125             DNS       216 Standard query 0x1e0a[Malformed Packet]
  45 16:04:52.834293  128.119.245.12         10.0.0.125             TCP        56 80 → 59590 [ACK] Seq=1 Ack=493 Win=30336 Len=0
  46 16:04:52.834293  128.119.245.12         10.0.0.125             TCP      1514 80 → 59590 [ACK] Seq=1 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  47 16:04:52.834742  128.119.245.12         10.0.0.125             TCP      1514 80 → 59590 [ACK] Seq=1461 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  48 16:04:52.834777  10.0.0.125             128.119.245.12         TCP        54 59590 → 80 [ACK] Seq=493 Ack=2921 Win=65536 Len=0
  49 16:04:52.838032  128.119.245.12         10.0.0.125             TCP      1514 80 → 59590 [ACK] Seq=2921 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  50 16:04:52.838034  128.119.245.12         10.0.0.125             HTTP      535 HTTP/1.1 200 OK  (text/html)
  51 16:04:52.838111  10.0.0.125             128.119.245.12         TCP        54 59590 → 80 [ACK] Seq=493 Ack=4862 Win=65536 Len=0
  52 16:04:53.022850  fe80::b1a9:a494:834…   ff02::1:3              LLMNR      84 Standard query 0x21d0 A wpad
  53 16:04:53.022872  fe80::b1a9:a494:834…   ff02::1:3              LLMNR      84 Standard query 0x77e8 AAAA wpad
  54 16:04:53.022940  10.0.0.125             224.0.0.252            LLMNR      64 Standard query 0x77e8 AAAA wpad
  55 16:04:53.022958  10.0.0.125             224.0.0.252            LLMNR      64 Standard query 0x21d0 A wpad
  56 16:04:53.361530  10.0.0.125             10.0.0.255             NBNS       92 Name query NB WPAD<00>
  57 16:04:53.963235  fe80::4a1d:70ff:fe2…   ff02::1                ICMPv6    174 Router Advertisement from 48:1d:70:22:f1:b4
  58 16:04:54.112306  10.0.0.125             10.0.0.255             NBNS       92 Name query NB WPAD<00>
  59 16:04:54.293248  10.0.0.125             10.0.0.59              TCP       164 59038 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=256 Len=110 [TCP segment of a reassembled PDU]
  60 16:04:54.297972  10.0.0.59              10.0.0.125             TCP       164 8009 → 59038 [PSH, ACK] Seq=111 Ack=221 Win=547 Len=110 [TCP segment of a reassembled PDU]
  61 16:04:54.338305  10.0.0.125             10.0.0.59              TCP        54 59038 → 8009 [ACK] Seq=221 Ack=221 Win=255 Len=0

    Date: Sun, 27 Oct 2019 23:04:53 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    Last-Modified: Sun, 27 Oct 2019 05:59:02 GMT\r\n
    ETag: "1194-595de147921c6"\r\n
    Accept-Ranges: bytes\r\n
  v Content-Length: 4500\r\n
        [Content length: 4500]
    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: 0.115479000 seconds]
    [Request in frame: 43]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
> Line-based text data: text/html (98 lines)

0160  55 54 46 2d 38 0d 0a 0d  0a 3c 68 74 6d 6c 3e 3c   UTF-8··· ·<html><
0170  68 65 61 64 3e 20 0a 3c  74 69 74 6c 65 3e 48 69   head> ·< title>Hi
0180  73 74 6f 72 69 63 61 6c  20 44 6f 63 75 6d 65 6e   storical  Documen
0190  74 73 3a 54 48 45 20 42  49 4c 4c 20 4f 46 20 52   ts:THE B ILL OF R
01a0  49 47 48 54 53 3c 2f 74  69 74 6c 65 3e 3c 2f 68   IGHTS</t itle></h
01b0  65 61 64 3e 0a 0a 0a 3c  62 6f 64 79 20 62 67 63   ead>···< body bgc
01c0  6f 6c 6f 72 3d 22 23 66  66 66 66 66 66 22 20 6c   olor="#f fffff" l
01d0  69 6e 6b 3d 22 23 33 33  30 30 30 30 22 20 76 6c   ink="#33 0000" vl
01e0  69 6e 6b 3d 22 23 36 36  36 36 33 33 22 3e 0a 3c   ink="#66 6633">·<
01f0  70 3e 3c 62 72 3e 0a 3c  2f 70 3e 0a 3c 70 3e 3c   p><br>·< /p>·<p><
0200  2f 70 3e 3c 63 65 6e 74  65 72 3e 3c 62 3e 54 48   /p><cent er><b>TH
0210  45 20 42 49 4c 4c 20 4f  46 20 52 49 47 48 54 53   E BILL O F RIGHTS
0220  3c 2f 62 3e 3c 62 72 3e  0a 20 20 3c 65 6d 3e 41   </b><br> ·  <em>A
0230  6d 65 6e 64 6d 65 6e 74  73 20 31 2d 31 30 20 6f   mendment s 1-10 o
```

14. What is the status code and phrase in the response?
The status code and phrase in the response was 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?
The data was sent in 4 TCP segments and then reassembled

Hao (Jeff) Deng
ID: 932912420



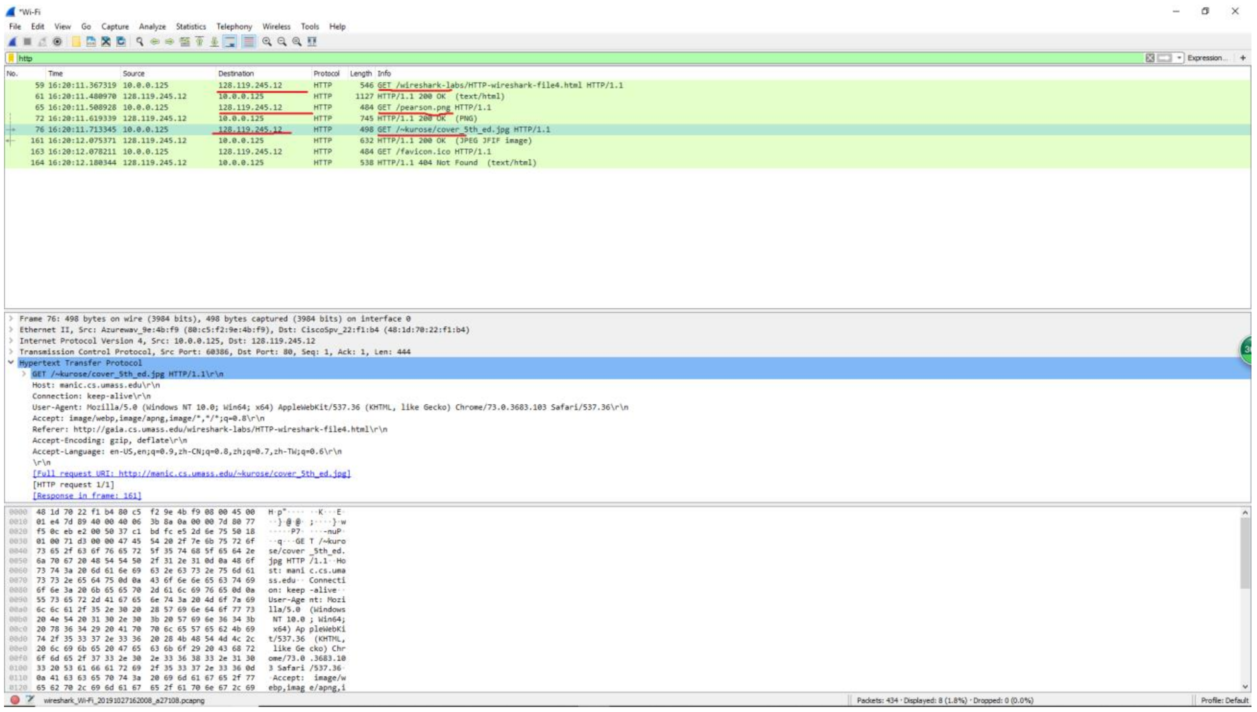
*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…

```
No.  Time             Source                Destination      Protocol Length Info
  42 16:04:52.722406  10.0.0.125            128.119.245.12   TCP        54 59590 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
  43 16:04:52.722555  10.0.0.125            128.119.245.12   HTTP      546 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
  44 16:04:52.763681  36.110.231.13         10.0.0.125       DNS       216 Standard query 0x1e0a[Malformed Packet]
  45 16:04:52.834293  128.119.245.12        10.0.0.125       TCP        56 80 → 59590 [ACK] Seq=1 Ack=493 Win=30336 Len=0
  46 16:04:52.834293  128.119.245.12        10.0.0.125       TCP      1514 80 → 59590 [ACK] Seq=1 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  47 16:04:52.834742  128.119.245.12        10.0.0.125       TCP      1514 80 → 59590 [ACK] Seq=1461 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  48 16:04:52.834777  10.0.0.125            128.119.245.12   TCP        54 59590 → 80 [ACK] Seq=493 Ack=2921 Win=65536 Len=0
  49 16:04:52.838032  128.119.245.12        10.0.0.125       TCP      1514 80 → 59590 [ACK] Seq=2921 Ack=493 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
  50 16:04:52.838034  128.119.245.12        10.0.0.125       HTTP      535 HTTP/1.1 200 OK  (text/html)
  51 16:04:52.838111  10.0.0.125            128.119.245.12   TCP        54 59590 → 80 [ACK] Seq=493 Ack=4862 Win=65536 Len=0
  52 16:04:53.022850  fe80::b1a9:a494:834…  ff02::1:3        LLMNR      84 Standard query 0x21d0 A wpad
  53 16:04:53.022872  fe80::b1a9:a494:834…  ff02::1:3        LLMNR      84 Standard query 0x77e8 AAAA wpad
  54 16:04:53.022940  10.0.0.125            224.0.0.252      LLMNR      64 Standard query 0x77e8 AAAA wpad
  55 16:04:53.022958  10.0.0.125            224.0.0.252      LLMNR      64 Standard query 0x21d0 A wpad
  56 16:04:53.361530  10.0.0.125            10.0.0.255       NBNS       92 Name query NB WPAD<00>
  57 16:04:53.963235  fe80::4a1d:70ff:fe2…  ff02::1          ICMPv6    174 Router Advertisement from 48:1d:70:22:f1:b4
  58 16:04:54.112306  10.0.0.125            10.0.0.255       NBNS       92 Name query NB WPAD<00>
  59 16:04:54.293248  10.0.0.125            10.0.0.59        TCP       164 59038 → 8009 [PSH, ACK] Seq=111 Ack=111 Win=256 Len=110 [TCP segment of a reassembled PDU]
  60 16:04:54.297972  10.0.0.59             10.0.0.125       TCP       164 8009 → 59038 [PSH, ACK] Seq=111 Ack=221 Win=547 Len=110 [TCP segment of a reassembled PDU]
  61 16:04:54.338305  10.0.0.125            10.0.0.59        TCP        54 59038 → 8009 [ACK] Seq=221 Ack=221 Win=255 Len=0
```

```
> Frame 50: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0
> Ethernet II, Src: Pegatron_4a:f1:b0 (74:85:2a:4a:f1:b0), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 59590, Seq: 4381, Ack: 493, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #46(1460), #47(1460), #49(1460), #50(481)]
    [Frame: 46, payload: 0-1459 (1460 bytes)]
    [Frame: 47, payload: 1460-2919 (1460 bytes)]
    [Frame: 49, payload: 2920-4379 (1460 bytes)]
    [Frame: 50, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053…]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

```
0010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 32 37 20 4f   ·Date: S un, 27 O
0020  63 74 20 32 30 31 39 20  32 33 3a 30 34 3a 35 33   ct 2019  23:04:53
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
0070  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
0080  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified: 
00a0  53 75 6e 2c 20 32 37 20  4f 63 74 20 32 30 31 39   Sun, 27  Oct 2019
00b0  20 30 35 3a 35 39 3a 30  32 20 47 4d 54 0d 0a 45    05:59:0 2 GMT··E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 35 39 35 64 65   Tag: "11 94-595de
00d0  31 34 37 39 32 31 63 36  22 0d 0a 41 63 63 65 70   147921c6 "··Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
```

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?
    My browser sent 3 HTTP GET request messages and they are:
        Initial website: 128.119.245.12
        Pearson logo: 128.119.245.12
        Textbook: 128.119.245.12
    Seems to me that all of these IP addresses are the same



*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…

```
No.  Time             Source           Destination      Protocol Length Info
  59 16:20:11.367319  10.0.0.125       128.119.245.12   HTTP      546 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
  61 16:20:11.480970  128.119.245.12   10.0.0.125       HTTP     1127 HTTP/1.1 200 OK  (text/html)
  65 16:20:11.508928  10.0.0.125       128.119.245.12   HTTP      484 GET /pearson.png HTTP/1.1
  72 16:20:11.619339  128.119.245.12   10.0.0.125       HTTP      745 HTTP/1.1 200 OK  (PNG)
  76 16:20:11.713345  10.0.0.125       128.119.245.12   HTTP      498 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
 161 16:20:12.075371  128.119.245.12   10.0.0.125       HTTP      632 HTTP/1.1 200 OK  (JPEG JFIF image)
 163 16:20:12.078211  10.0.0.125       128.119.245.12   HTTP      484 GET /favicon.ico HTTP/1.1
 164 16:20:12.180344  128.119.245.12   10.0.0.125       HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Frame 76: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0
> Ethernet II, Src: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9), Dst: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4)
> Internet Protocol Version 4, Src: 10.0.0.125, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60386, Dst Port: 80, Seq: 1, Ack: 1, Len: 444
v Hypertext Transfer Protocol
  > GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\n
    Host: manic.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
    Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.6\r\n
    \r\n
    [Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]
    [HTTP request 1/1]
    [Response in frame: 161]
```

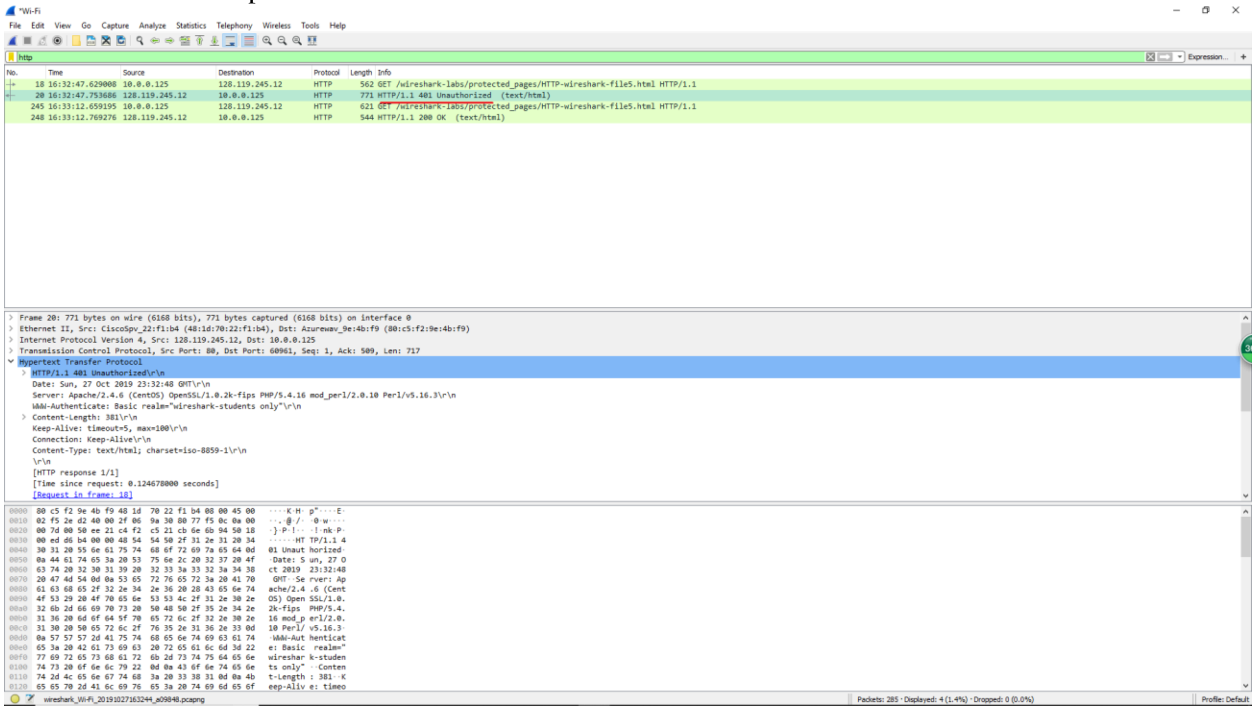
```
0000  48 1d 70 22 f1 b4 80 c5  f2 9e 4b f9 08 00 45 00   H·p"···· ··K···E·
0010  01 e4 7d 89 40 00 40 06  3b 8a 0a 00 00 7d 80 77   ··}·@·@· ;····}·w
0020  f5 0c eb e2 00 50 37 c1  bd fc e5 2d 6e 75 50 18   ·····P7· ···-nuP·
0030  01 00 71 d3 00 00 47 45  54 20 2f 7e 6b 75 72 6f   ··q···GE T /~kuro
0040  73 65 2f 63 6f 76 65 72  5f 35 74 68 5f 65 64 2e   se/cover _5th_ed.
0050  6a 70 67 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   jpg HTTP /1.1··Ho
0060  73 74 3a 20 6d 61 6e 69  63 2e 63 73 2e 75 6d 61   st: mani c.cs.uma
0070  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0080  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
0090  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00a0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
00b0  20 4e 54 20 31 30 2e 30  3b 20 57 69 6e 36 34 3b    NT 10.0 ; Win64;
00c0  20 78 36 34 29 20 41 70  70 6c 65 57 65 62 4b 69    x64) Ap pleWebKi
00d0  74 2f 35 33 37 2e 33 36  20 28 4b 48 54 4d 4c 2c   t/537.36  (KHTML,
00e0  20 6c 69 6b 65 20 47 65  63 6b 6f 29 20 43 68 72    like Ge cko) Chr
00f0  6f 6d 65 2f 37 33 2e 30  2e 33 36 38 33 2e 31 30   ome/73.0 .3683.10
0100  33 20 53 61 66 61 72 69  2f 35 33 37 2e 33 36 0d   3 Safari /537.36·
0110  0a 41 63 63 65 70 74 3a  20 69 6d 61 67 65 2f 77   ·Accept:  image/w
0120  65 62 70 2c 69 6d 61 67  65 2f 61 70 6e 67 2c 69   ebp,imag e/apng,i
```

```
wireshark_Wi-Fi_20191027162008_a27108.pcapng    Packets: 434 · Displayed: 8 (1.8%) · Dropped: 0 (0.0%)    Profile: Default
```

Hao (Jeff) Deng
ID: 932912420

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.
    Seems to me that both images were downloaded serially because the first image was requested and sent before the second image. If they were done in parallel, them both images would have been requested and returned at the same time period. In this case, the second image was only requested after the first image came back.

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?
    The server's response to the initial HTTP GET was 401 Unauthorized



```
No.  Time             Source          Destination     Protocol Length Info
  18 16:32:47.629008 10.0.0.125      128.119.245.12  HTTP      562 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  20 16:32:47.753686 128.119.245.12  10.0.0.125      HTTP      771 HTTP/1.1 401 Unauthorized  (text/html)
 245 16:33:12.659195 10.0.0.125      128.119.245.12  HTTP      621 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 248 16:33:12.769276 128.119.245.12  10.0.0.125      HTTP      544 HTTP/1.1 200 OK  (text/html)
```

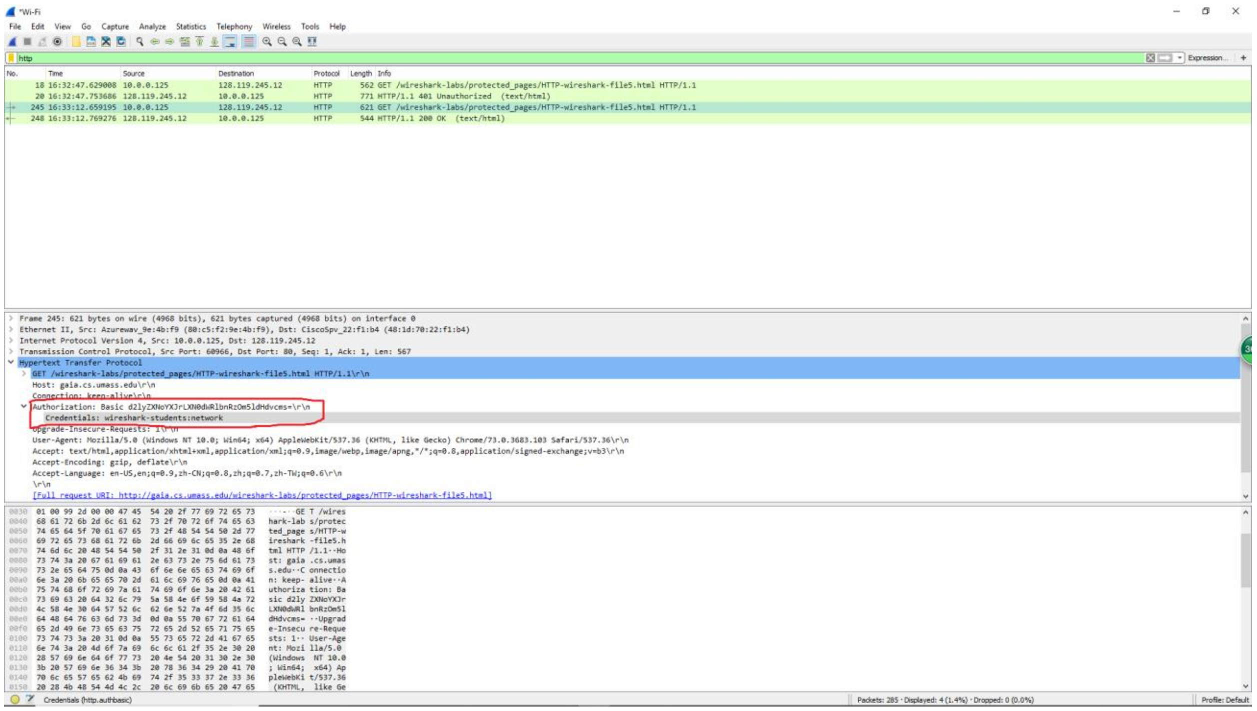
```
> Frame 20: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface 0
> Ethernet II, Src: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4), Dst: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.125
> Transmission Control Protocol, Src Port: 80, Dst Port: 60961, Seq: 1, Ack: 509, Len: 717
v Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Sun, 27 Oct 2019 23:32:48 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  > Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.124678000 seconds]
    [Request in frame: 18]
```

```
0000  80 c5 f2 9e 4b f9 48 1d  70 22 f1 b4 08 00 45 00   ····K·H· p"····E·
0010  02 f5 2e d2 40 00 2f 06  9a 30 80 77 f5 0c 0a 00   ··.·@·/· ·0·w····
0020  00 7d 00 50 ee 21 c4 f2  c5 21 cb 6e 6b 94 50 18   ·}·P·!·· ·!·nk·P·
0030  00 ed d6 b4 00 00 48 54  54 50 2f 31 2e 31 20 34   ······HT TP/1.1 4
0040  30 31 20 55 6e 61 75 74  68 6f 72 69 7a 65 64 0d   01 Unaut horized·
0050  0a 44 61 74 65 3a 20 53  75 6e 2c 20 32 37 20 4f   ·Date: S un, 27 O
0060  63 74 20 32 30 31 39 20  32 33 3a 33 32 3a 34 38   ct 2019  23:32:48
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   2k-fips  PHP/5.4.
00b0  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
00c0  31 30 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   10 Perl/ v5.16.3·
00d0  0a 57 57 57 2d 41 75 74  68 65 6e 74 69 63 61 74   ·WWW-Aut henticat
00e0  65 3a 20 42 61 73 69 63  20 72 65 61 6c 6d 3d 22   e: Basic  realm="
00f0  77 69 72 65 73 68 61 72  6b 2d 73 74 75 64 65 6e   wireshar k-studen
0100  74 73 20 6f 6e 6c 79 22  0d 0a 43 6f 6e 74 65 6e   ts only" ··Conten
0110  74 2d 4c 65 6e 67 74 68  3a 20 33 38 31 0d 0a 4b   t-Length : 381··K
0120  65 65 70 2d 41 6c 69 76  65 3a 20 74 69 6d 65 6f   eep-Aliv e: timeo
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
wireshark_Wi-Fi_20191027163244_a09848.pcapng
Packets: 285 · Displayed: 4 (1.4%) · Dropped: 0 (0.0%)
Profile: Default

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?
    For the second time, the new field included in the HTTP GET message was the Authorization field, which contains the credentials

Hao (Jeff) Deng
ID: 932912420



```
No.  Time               Source          Destination     Protocol Length Info
  18 16:32:47.629008    10.0.0.125      128.119.245.12  HTTP     562 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
  20 16:32:47.753686    128.119.245.12  10.0.0.125      HTTP     771 HTTP/1.1 401 Unauthorized  (text/html)
 245 16:33:12.659195    10.0.0.125      128.119.245.12  HTTP     621 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 248 16:33:12.769276    128.119.245.12  10.0.0.125      HTTP     544 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 245: 621 bytes on wire (4968 bits), 621 bytes captured (4968 bits) on interface 0
> Ethernet II, Src: Azurewav_9e:4b:f9 (80:c5:f2:9e:4b:f9), Dst: CiscoSpv_22:f1:b4 (48:1d:70:22:f1:b4)
> Internet Protocol Version 4, Src: 10.0.0.125, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60966, Dst Port: 80, Seq: 1, Ack: 1, Len: 567
v Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
  v Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
        Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,zh-TW;q=0.6\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
```

```
0030  01 00 99 2d 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 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 35 2e 68   ireshark -file5.h
0070  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0080  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0090  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
00a0  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 41   n: keep- alive··A
00b0  75 74 68 6f 72 69 7a 61  74 69 6f 6e 3a 20 42 61   uthoriza tion: Ba
00c0  73 69 63 20 64 32 6c 79  5a 58 4e 6f 59 58 4a 72   sic d2ly ZXNoYXJr
00d0  4c 58 4e 30 64 57 52 6c  62 6e 52 7a 4f 6d 35 6c   LXN0dWRl bnRzOm5l
00e0  64 48 64 76 63 6d 73 3d  0d 0a 55 70 67 72 61 64   dHdvcms= ··Upgrad
00f0  65 2d 49 6e 73 65 63 75  72 65 2d 52 65 71 75 65   e-Insecu re-Reque
0100  73 74 73 3a 20 31 0d 0a  55 73 65 72 2d 41 67 65   sts: 1·· User-Age
0110  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
0120  28 57 69 6e 64 6f 77 73  20 4e 54 20 31 30 2e 30   (Windows  NT 10.0
0130  3b 20 57 69 6e 36 34 3b  20 78 36 34 29 20 41 70   ; Win64;  x64) Ap
0140  70 6c 65 57 65 62 4b 69  74 2f 35 33 37 2e 33 36   pleWebKi t/537.36
0150  20 28 4b 48 54 4d 4c 2c  20 6c 69 6b 65 20 47 65    (KHTML,  like Ge
```

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
Credentials (http.authbasic)
Packets: 285 · Displayed: 4 (1.4%) · Dropped: 0 (0.0%)
Profile: Default