Laboratory 1 – HTTP

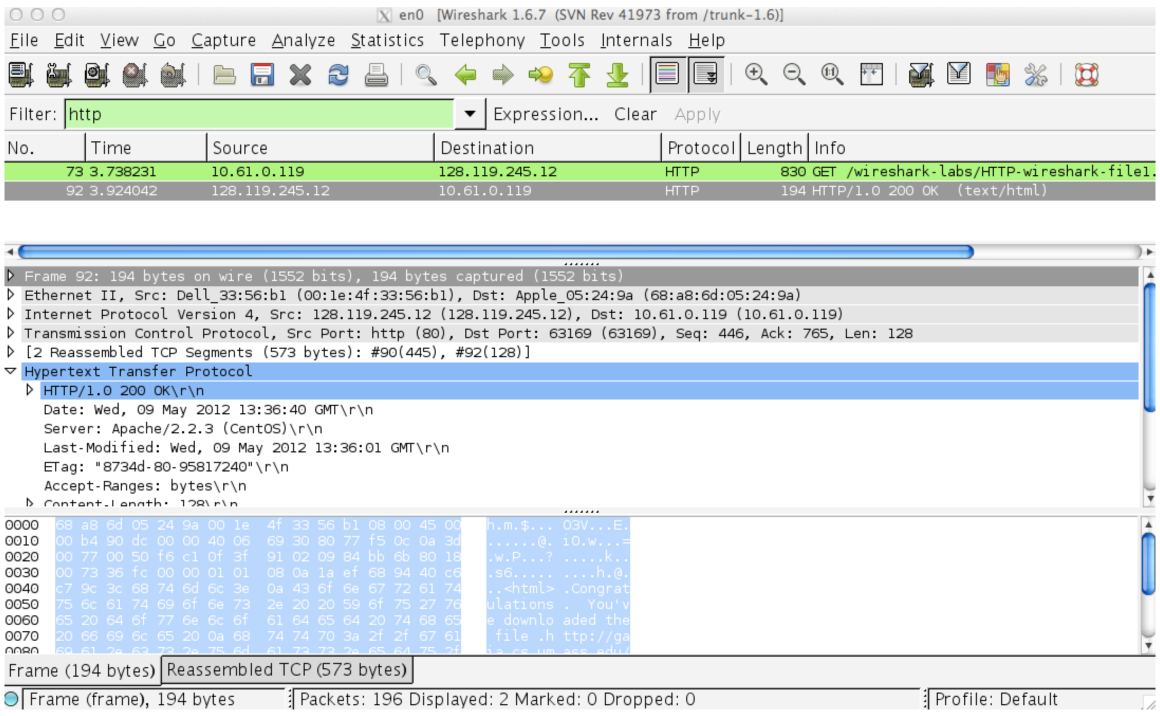
Student name: Phan Phương Duy. **Student ID**: ITITIU16010

1. THE BASIC HTTP GET/RESPONSE INTERACTION

Let's begin our exploration of HTTP by downloading a very simple HTML file - one that is very short, and contains no embedded objects. Do the following:

- Start up your web browser.
- Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).
- Wait a bit more than one minute (we'll see why shortly), and then begin Wireshark packet capture.
- Enter the following to your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html , your browser should display the very simple, one-line HTML file.
- Stop Wireshark packet capture.

Your Wireshark window should look similar to the window shown in Figure 1. If you are unable to run Wireshark on a live network connection, you can download a packet trace that was created when the steps above were followed.


en0 [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: http
Expression... Clear Apply

```
No.  Time        Source           Destination      Protocol Length Info
  73 3.738231    10.61.0.119      128.119.245.12   HTTP       830 GET /wireshark-labs/HTTP-wireshark-file1.
  92 3.924042    128.119.245.12   10.61.0.119      HTTP       194 HTTP/1.0 200 OK  (text/html)

▷ Frame 92: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
▷ Ethernet II, Src: Dell_33:56:b1 (00:1e:4f:33:56:b1), Dst: Apple_05:24:9a (68:a8:6d:05:24:9a)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.61.0.119 (10.61.0.119)
▷ Transmission Control Protocol, Src Port: http (80), Dst Port: 63169 (63169), Seq: 446, Ack: 765, Len: 128
▷ [2 Reassembled TCP Segments (573 bytes): #90(445), #92(128)]
▽ Hypertext Transfer Protocol
  ▷ HTTP/1.0 200 OK\r\n
    Date: Wed, 09 May 2012 13:36:40 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Wed, 09 May 2012 13:36:01 GMT\r\n
    ETag: "8734d-80-95817240"\r\n
    Accept-Ranges: bytes\r\n
  ▷ Content-Length: 128\r\n

0000  68 a8 6d 05 24 9a 00 1e  4f 33 56 b1 08 00 45 00   h.m.$... O3V...E.
0010  00 b4 90 dc 00 00 40 06  69 30 80 77 f5 0c 0a 3d   ......@. i0.w...=
0020  00 77 00 50 f6 c1 0f 3f  91 02 09 84 bb 6b 80 18   .w.P...? .....k..
0030  00 73 36 fc 00 00 01 01  08 0a 1a ef 68 94 40 c6   .s6..... ....h.@.
0040  c7 9c 3c 68 74 6d 6c 3e  0a 43 6f 6e 67 72 61 74   ..<html> .Congrat
0050  75 6c 61 74 69 6f 6e 73  2e 20 20 59 6f 75 27 76   ulations .  You'v
0060  65 20 64 6f 77 6e 6c 6f  61 64 65 64 20 74 68 65   e downlo aded the
0070  20 66 69 6c 65 20 0a 68  74 74 70 3a 2f 2f 67 61    file .h ttp://ga
0080  69 61 2e 63 73 2e 75 6d  61 73 73 2e 65 64 75 2f   ia.cs.um ass.edu/

Frame (194 bytes) | Reassembled TCP (573 bytes)
Frame (frame), 194 bytes | Packets: 196 Displayed: 2 Marked: 0 Dropped: 0 | Profile: Default
```

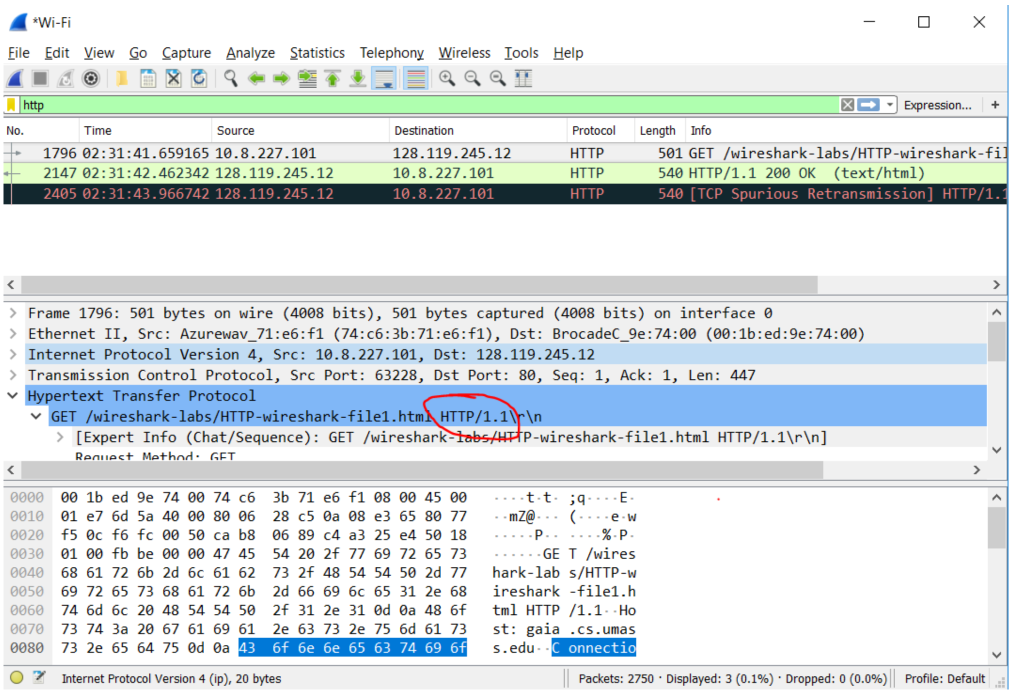
Figure 1: Wireshark Display after http://gaia.cs.umass.edu/wireshark-labs/ HTTP-wireshark-file1.html has been retrieved by your browser

The example in Figure 1 shows in the packet-listing window that two HTTP messages were captured: the GET message (from your browser to the gaia.cs.umass.edu web server) and the response message from the server to your browser. The packet-contents window shows details of the selected message (in this case the HTTP OK message, which is highlighted in the packet-listing window). Recall that since the HTTP message was carried inside a TCP segment, which was carried inside an IP datagram, which was carried within an Ethernet frame, Wireshark displays the Frame, Ethernet, IP, and TCP packet information as well. We want to minimize the amount of non-HTTP data displayed (we're interested in HTTP here, and will be investigating these other protocols is later labs), so make sure the boxes at the far left of the Frame, Ethernet, IP and TCP information have a plus sign or a right-pointing triangle (which means there is hidden, undisplayed information), and the HTTP line has a minus sign or a down-pointing triangle (which means that all information about the HTTP message is displayed).

By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the message you've found the information that answers the following questions. When you hand in your assignment, annotate the output so that it's clear where in the output you're getting the information for your answer (e.g., for our classes, we ask that students markup paper copies with a pen, or annotate electronic copies with text in a colored font).

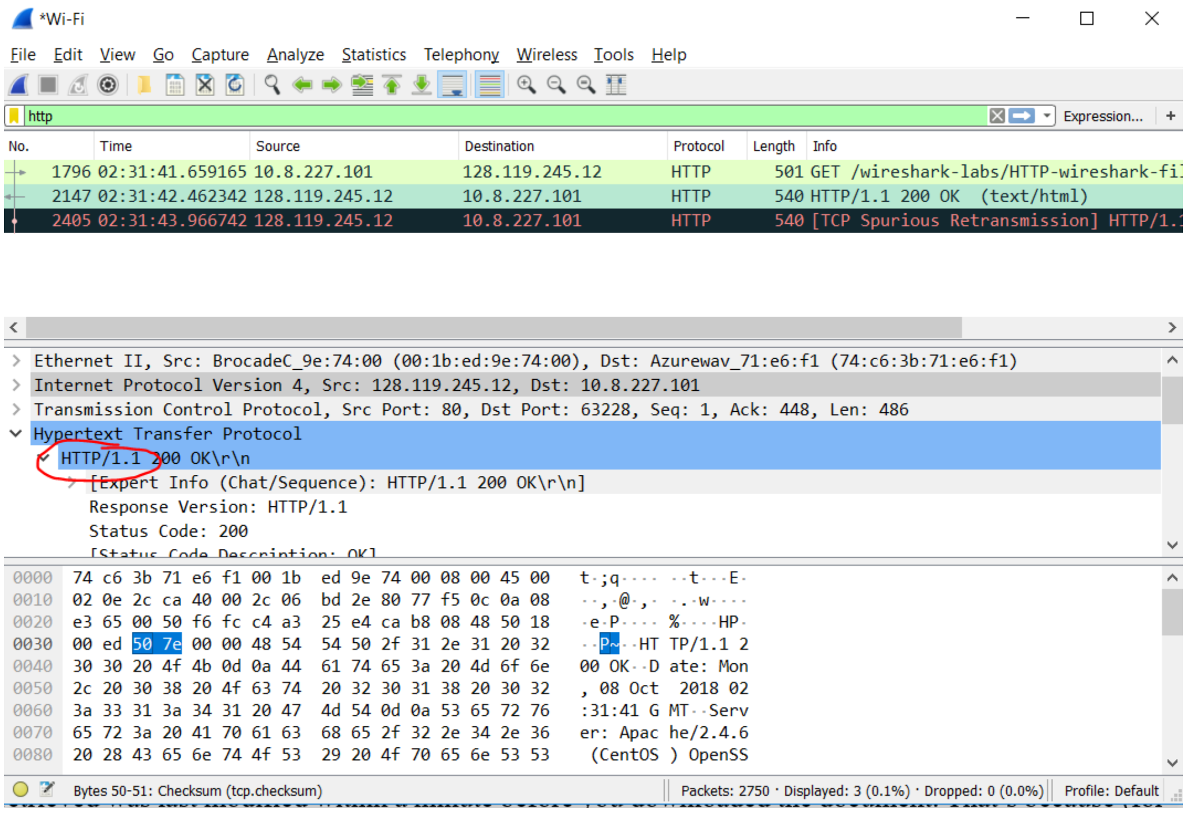
Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

My browser is running HTTP 1.1


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

```
No.   Time            Source          Destination     Protocol Length Info
1796 02:31:41.659165 10.8.227.101    128.119.245.12  HTTP     501 GET /wireshark-labs/HTTP-wireshark-fil
2147 02:31:42.462342 128.119.245.12  10.8.227.101    HTTP     540 HTTP/1.1 200 OK  (text/html)
2405 02:31:43.966742 128.119.245.12  10.8.227.101    HTTP     540 [TCP Spurious Retransmission] HTTP/1.1

> Frame 1796: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
> Ethernet II, Src: Azurewav_71:e6:f1 (74:c6:3b:71:e6:f1), Dst: BrocadeC_9e:74:00 (00:1b:ed:9e:74:00)
> Internet Protocol Version 4, Src: 10.8.227.101, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63228, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET

0000  00 1b ed 9e 74 00 74 c6  3b 71 e6 f1 08 00 45 00   ····t·t· ;q····E·
0010  01 e7 6d 5a 40 00 80 06  28 c5 0a 08 e3 65 80 77   ··mZ@··· (····e·w
0020  f5 0c f6 fc 00 50 ca b8  06 89 c4 a3 25 e4 50 18   ·····P·· ····%·P·
0030  01 00 fb be 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio

Internet Protocol Version 4 (ip), 20 bytes   Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%)   Profile: Default
```

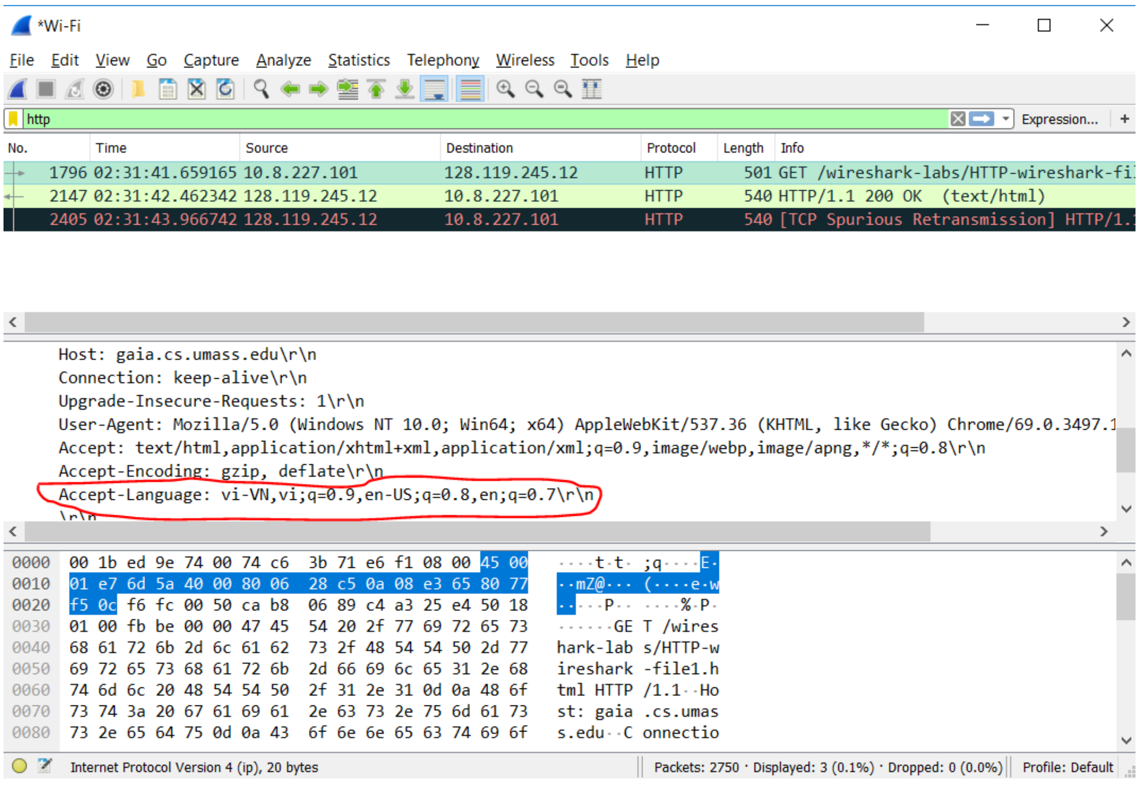
Server is running HTTP 1.1



```
http

No.   Time            Source          Destination     Protocol Length Info
 1796 02:31:41.659165 10.8.227.101    128.119.245.12  HTTP     501 GET /wireshark-labs/HTTP-wireshark-fi
 2147 02:31:42.462342 128.119.245.12  10.8.227.101    HTTP     540 HTTP/1.1 200 OK  (text/html)
 2405 02:31:43.966742 128.119.245.12  10.8.227.101    HTTP     540 [TCP Spurious Retransmission] HTTP/1.

> Ethernet II, Src: BrocadeC_9e:74:00 (00:1b:ed:9e:74:00), Dst: Azurewav_71:e6:f1 (74:c6:3b:71:e6:f1)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.227.101
> Transmission Control Protocol, Src Port: 80, Dst Port: 63228, Seq: 1, Ack: 448, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]

0000  74 c6 3b 71 e6 f1 00 1b  ed 9e 74 00 08 00 45 00   t·;q···· ··t···E·
0010  02 0e 2c ca 40 00 2c 06  bd 2e 80 77 f5 0c 0a 08   ··,·@·,· ·.·w····
0020  e3 65 00 50 f6 fc c4 a3  25 e4 ca b8 08 48 50 18   ·e·P···· %····HP·
0030  00 ed 50 7e 00 00 48 54  54 50 2f 31 2e 31 20 32   ··P~··HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D ate: Mon
0050  2c 20 30 38 20 4f 63 74  20 32 30 31 38 20 30 32   , 08 Oct  2018 02
0060  3a 33 31 3a 34 31 20 47  4d 54 0d 0a 53 65 72 76   :31:41 G MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS

Bytes 50-51: Checksum (tcp.checksum)   Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%)   Profile: Default
```

Q2. What languages (if any) does your browser indicate that it can accept to the server?

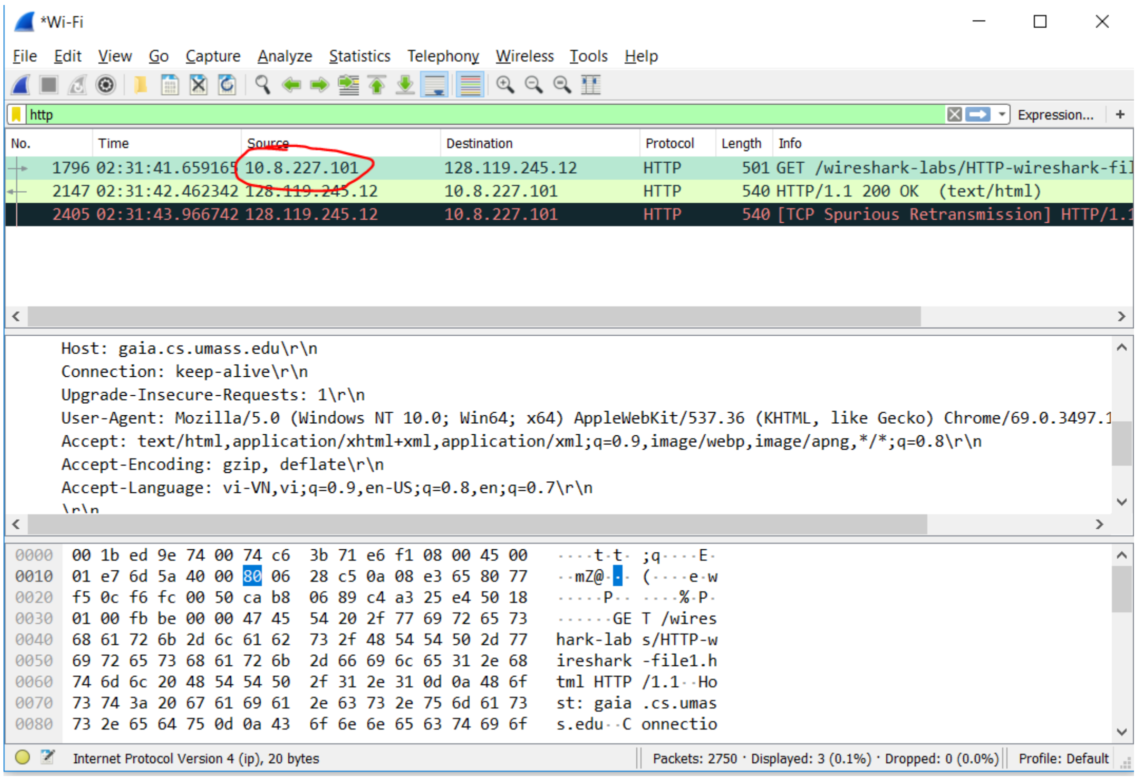
My browser indicates that it can accept Vietnamese (vi-VN) and English (en-US)



```
http

No.   Time            Source          Destination     Protocol Length Info
 1796 02:31:41.659165 10.8.227.101    128.119.245.12  HTTP     501 GET /wireshark-labs/HTTP-wireshark-fi
 2147 02:31:42.462342 128.119.245.12  10.8.227.101    HTTP     540 HTTP/1.1 200 OK  (text/html)
 2405 02:31:43.966742 128.119.245.12  10.8.227.101    HTTP     540 [TCP Spurious Retransmission] HTTP/1.

    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/69.0.3497.1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n

0000  00 1b ed 9e 74 00 74 c6  3b 71 e6 f1 08 00 45 00   ····t·t· ;q····E·
0010  01 e7 6d 5a 40 00 80 06  28 c5 0a 08 e3 65 80 77   ··mZ@··· (····e·w
0020  f5 0c f6 fc 00 50 ca b8  06 89 c4 a3 25 e4 50 18   ·····P·· ····%·P·
0030  01 00 fb be 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio

Internet Protocol Version 4 (ip), 20 bytes   Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%)   Profile: Default
```

Q3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

IP address of my computer: 10.8.227.101



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

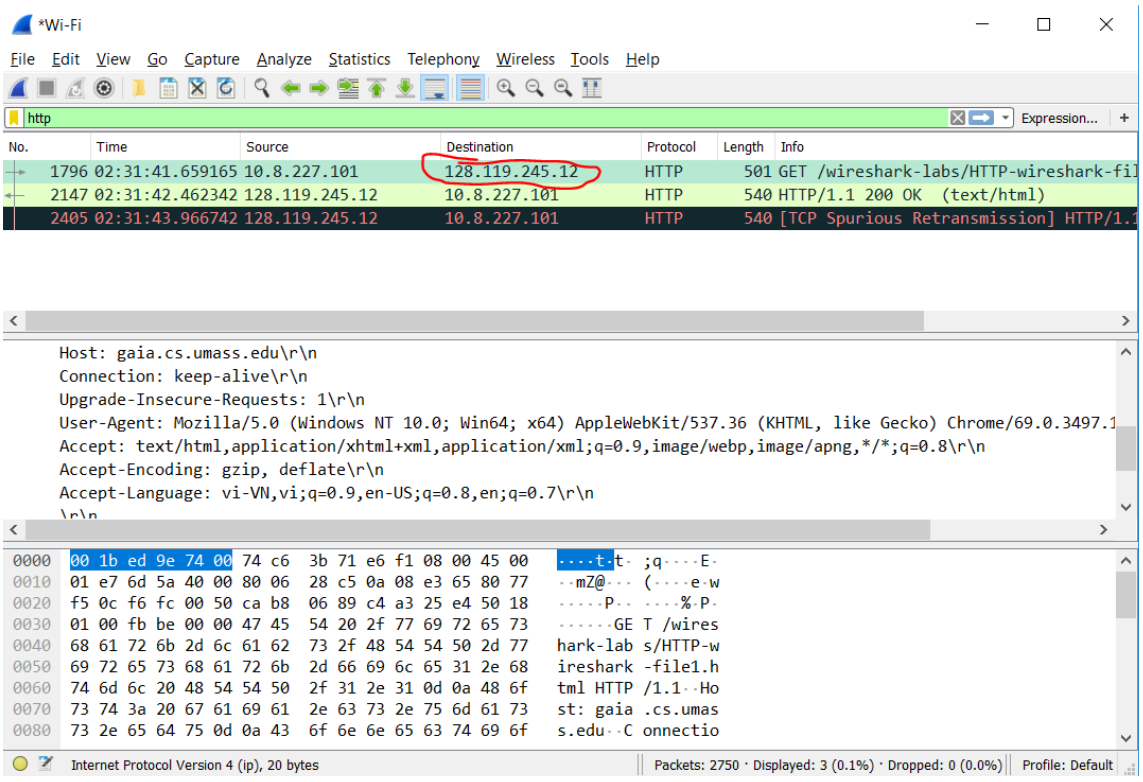
```
No.  Time            Source         Destination    Protocol Length Info
1796 02:31:41.659165 10.8.227.101   128.119.245.12 HTTP     501 GET /wireshark-labs/HTTP-wireshark-fil
2147 02:31:42.462342 128.119.245.12 10.8.227.101   HTTP     540 HTTP/1.1 200 OK  (text/html)
2405 02:31:43.966742 128.119.245.12 10.8.227.101   HTTP     540 [TCP Spurious Retransmission] HTTP/1.1
```

```
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
```

```
0000  00 1b ed 9e 74 00 74 c6  3b 71 e6 f1 08 00 45 00   ····t·t· ;q····E·
0010  01 e7 6d 5a 40 00 80 06  28 c5 0a 08 e3 65 80 77   ··mZ@··· (····e·w
0020  f5 0c f6 fc 00 50 ca b8  06 89 c4 a3 25 e4 50 18   ·····P·· ····%·P·
0030  01 00 fb be 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Ip address of gaia.cs.umass.edu server:



*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.  Time            Source         Destination    Protocol Length Info
1796 02:31:41.659165 10.8.227.101   128.119.245.12 HTTP     501 GET /wireshark-labs/HTTP-wireshark-fil
2147 02:31:42.462342 128.119.245.12 10.8.227.101   HTTP     540 HTTP/1.1 200 OK  (text/html)
2405 02:31:43.966742 128.119.245.12 10.8.227.101   HTTP     540 [TCP Spurious Retransmission] HTTP/1.1
```

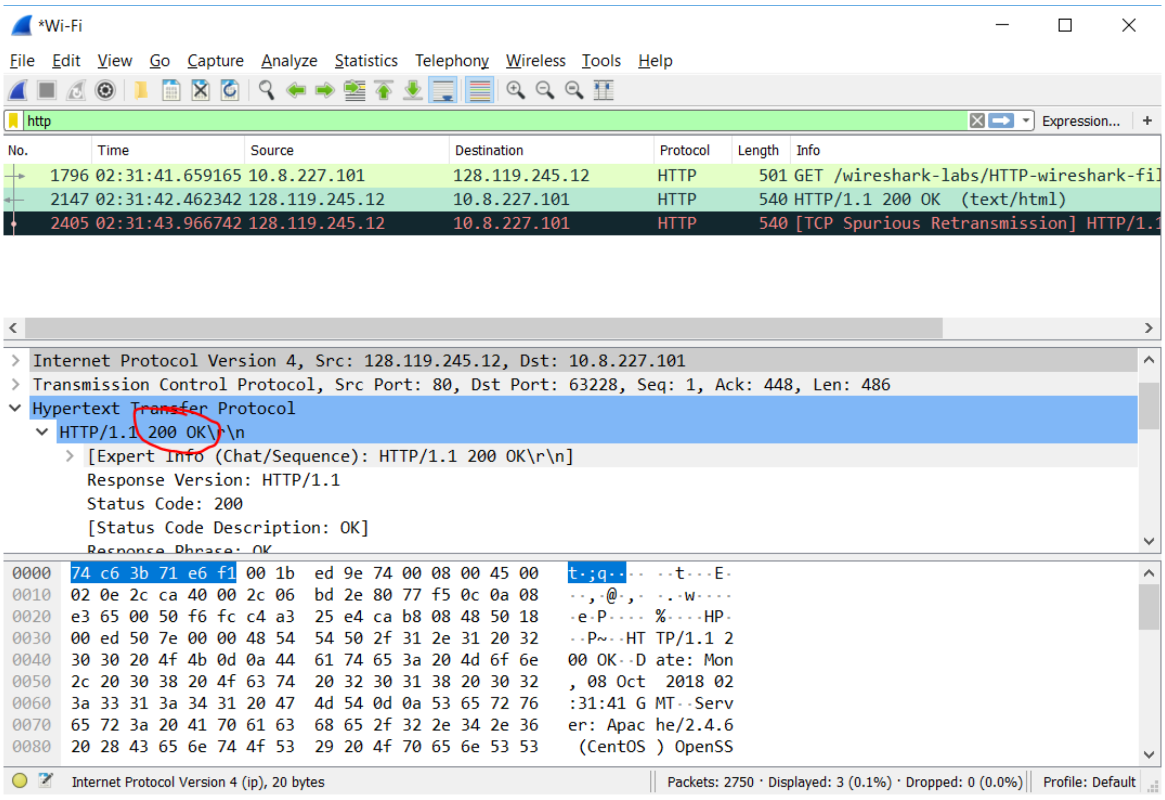
```
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n
\r\n
```

```
0000  00 1b ed 9e 74 00 74 c6  3b 71 e6 f1 08 00 45 00   ····t·t· ;q····E·
0010  01 e7 6d 5a 40 00 80 06  28 c5 0a 08 e3 65 80 77   ··mZ@··· (····e·w
0020  f5 0c f6 fc 00 50 ca b8  06 89 c4 a3 25 e4 50 18   ·····P·· ····%·P·
0030  01 00 fb be 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Q4. What is the status code returned from the server to your browser?

Status code: 200 OK


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

```
No.   Time             Source           Destination      Protocol  Length  Info
1796 02:31:41.659165 10.8.227.101     128.119.245.12   HTTP      501 GET /wireshark-labs/HTTP-wireshark-fil
2147 02:31:42.462342 128.119.245.12   10.8.227.101     HTTP      540 HTTP/1.1 200 OK  (text/html)
2405 02:31:43.966742 128.119.245.12   10.8.227.101     HTTP      540 [TCP Spurious Retransmission] HTTP/1.1
```

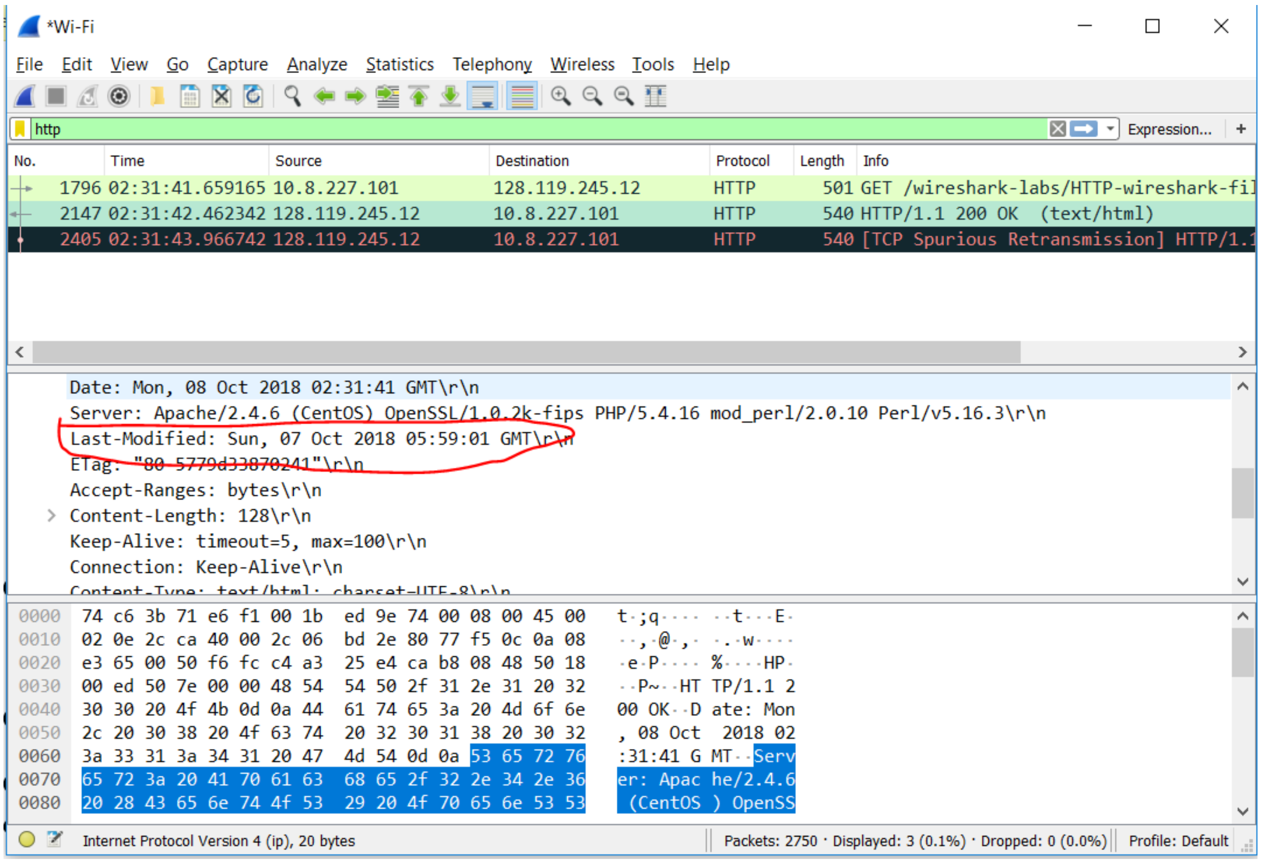
```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.227.101
> Transmission Control Protocol, Src Port: 80, Dst Port: 63228, Seq: 1, Ack: 448, Len: 486
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
```

```
0000  74 c6 3b 71 e6 f1 00 1b  ed 9e 74 00 08 00 45 00   t·;q····  ··t···E·
0010  02 0e 2c ca 40 00 2c 06  bd 2e 80 77 f5 0c 0a 08   ··,·@·,·  ·.·w····
0020  e3 65 00 50 f6 fc c4 a3  25 e4 ca b8 08 48 50 18   ·e·P····  %····HP·
0030  00 ed 50 7e 00 00 48 54  54 50 2f 31 2e 31 20 32   ··P~··HT  TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D  ate: Mon
0050  2c 20 30 38 20 4f 63 74  20 32 30 31 38 20 30 32   , 08 Oct   2018 02
0060  3a 33 31 3a 34 31 20 47  4d 54 0d 0a 53 65 72 76   :31:41 G  MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac  he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS  ) OpenSS
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Q5. When was the HTML file that you are retrieving last modified at the server?

The HTML file is last modified at Sun, 07 Oct 2018 5:59:01 GMT


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

```
No.   Time             Source           Destination      Protocol  Length  Info
1796 02:31:41.659165 10.8.227.101     128.119.245.12   HTTP      501 GET /wireshark-labs/HTTP-wireshark-fil
2147 02:31:42.462342 128.119.245.12   10.8.227.101     HTTP      540 HTTP/1.1 200 OK  (text/html)
2405 02:31:43.966742 128.119.245.12   10.8.227.101     HTTP      540 [TCP Spurious Retransmission] HTTP/1.1
```

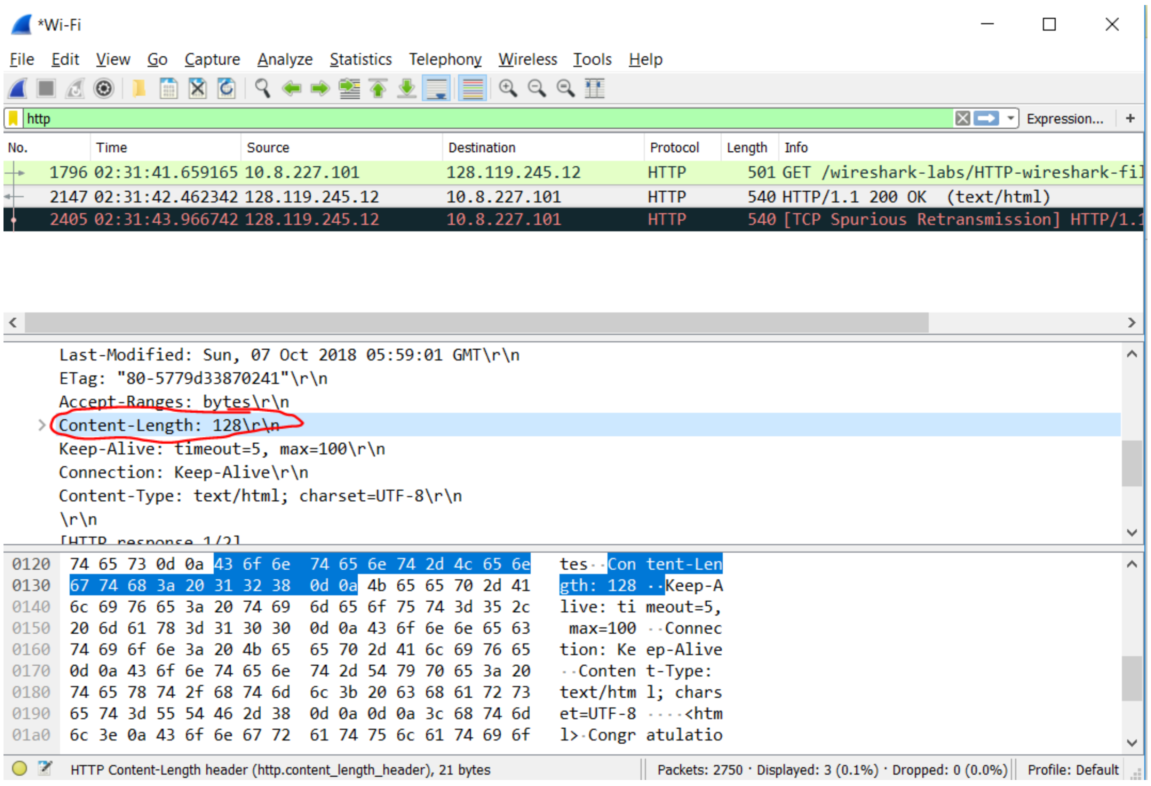
```
      Date: Mon, 08 Oct 2018 02:31:41 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
      Last-Modified: Sun, 07 Oct 2018 05:59:01 GMT\r\n
      ETag: "80-5779d33870241"\r\n
      Accept-Ranges: bytes\r\n
    > Content-Length: 128\r\n
      Keep-Alive: timeout=5, max=100\r\n
      Connection: Keep-Alive\r\n
      Content-Type: text/html; charset=UTF-8\r\n
```

```
0000  74 c6 3b 71 e6 f1 00 1b  ed 9e 74 00 08 00 45 00   t·;q····  ··t···E·
0010  02 0e 2c ca 40 00 2c 06  bd 2e 80 77 f5 0c 0a 08   ··,·@·,·  ·.·w····
0020  e3 65 00 50 f6 fc c4 a3  25 e4 ca b8 08 48 50 18   ·e·P····  %····HP·
0030  00 ed 50 7e 00 00 48 54  54 50 2f 31 2e 31 20 32   ··P~··HT  TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D  ate: Mon
0050  2c 20 30 38 20 4f 63 74  20 32 30 31 38 20 30 32   , 08 Oct   2018 02
0060  3a 33 31 3a 34 31 20 47  4d 54 0d 0a 53 65 72 76   :31:41 G  MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac  he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS  ) OpenSS
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

Q6. How many bytes of content are being returned to your browser?

128 bytes were returned to my browser


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

```
No.   Time              Source          Destination     Protocol  Length  Info
 1796 02:31:41.659165 10.8.227.101    128.119.245.12  HTTP       501 GET /wireshark-labs/HTTP-wireshark-fil
 2147 02:31:42.462342 128.119.245.12  10.8.227.101    HTTP       540 HTTP/1.1 200 OK  (text/html)
 2405 02:31:43.966742 128.119.245.12  10.8.227.101    HTTP       540 [TCP Spurious Retransmission] HTTP/1.1
```

```
    Last-Modified: Sun, 07 Oct 2018 05:59:01 GMT\r\n
    ETag: "80-5779d33870241"\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 1/2]
```

```
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
```

```
HTTP Content-Length header (http.content_length_header), 21 bytes | Packets: 2750 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%) | Profile: Default
```

Q7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

No, I do not see any headers that are missing.

In your answer to question 5 above, you might have been surprised to find that the document you just retrieved was last modified within a minute before you downloaded the document. That's because (for this particular file), the gaia.cs.umass.edu server is setting the file's last-modified time to be the current time, and is doing so once per minute. Thus, if you wait a minute between accesses, the file will appear to have been recently modified, and hence your browser will download a "new" copy of the document.

2. THE HTTP CONDITIONAL GET/RESPONSE INTERACTION

Recall from Section 2.2.6 of the text, that most web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object. Before performing the steps below, make sure your browser's cache is empty. (To do this under Firefox, select Tools->Clear Recent History and check the Cache box, or for Internet Explorer, select Tools->Internet Options->Delete File; these actions will remove cached files from your browser's cache.) Now do the following:

- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html, your browser should display a very simple five-line

HTML file.

- Quickly enter the same URL into your browser again (or simply select the refresh button on your browser)
- Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

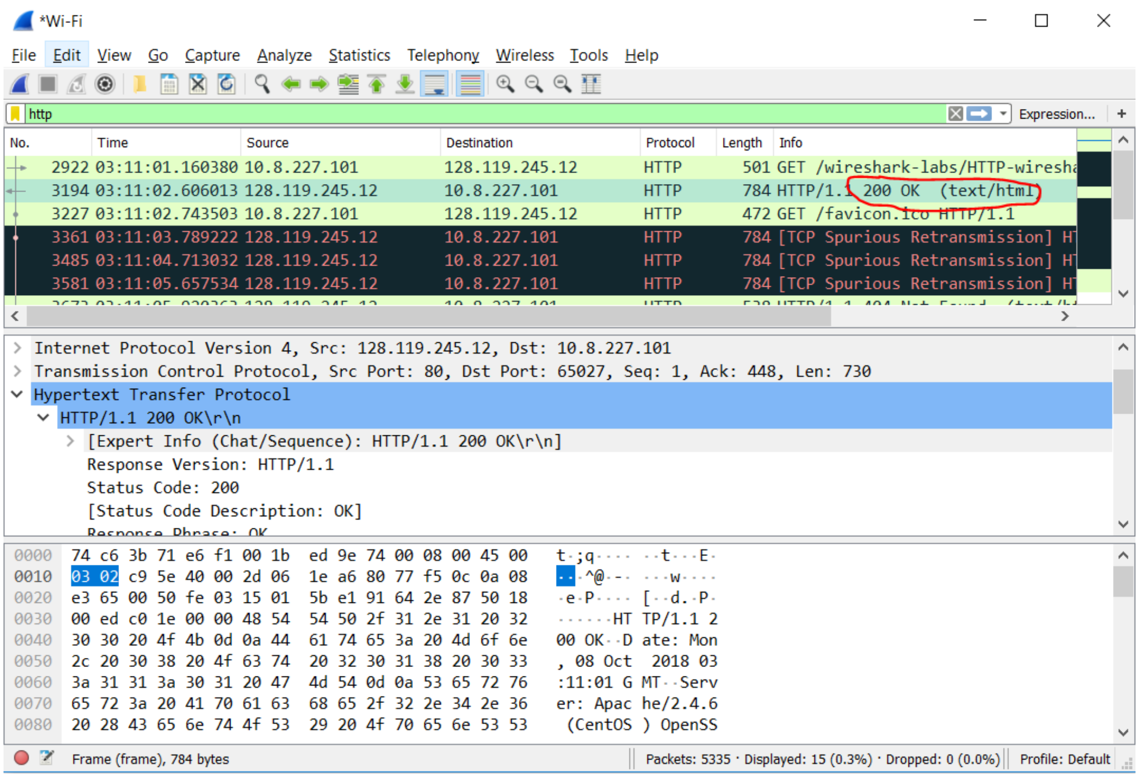
Answer the following questions:

Q 8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?

No, I do not see header "IF-MODIFIED-SINCE" in the HTTP GET

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

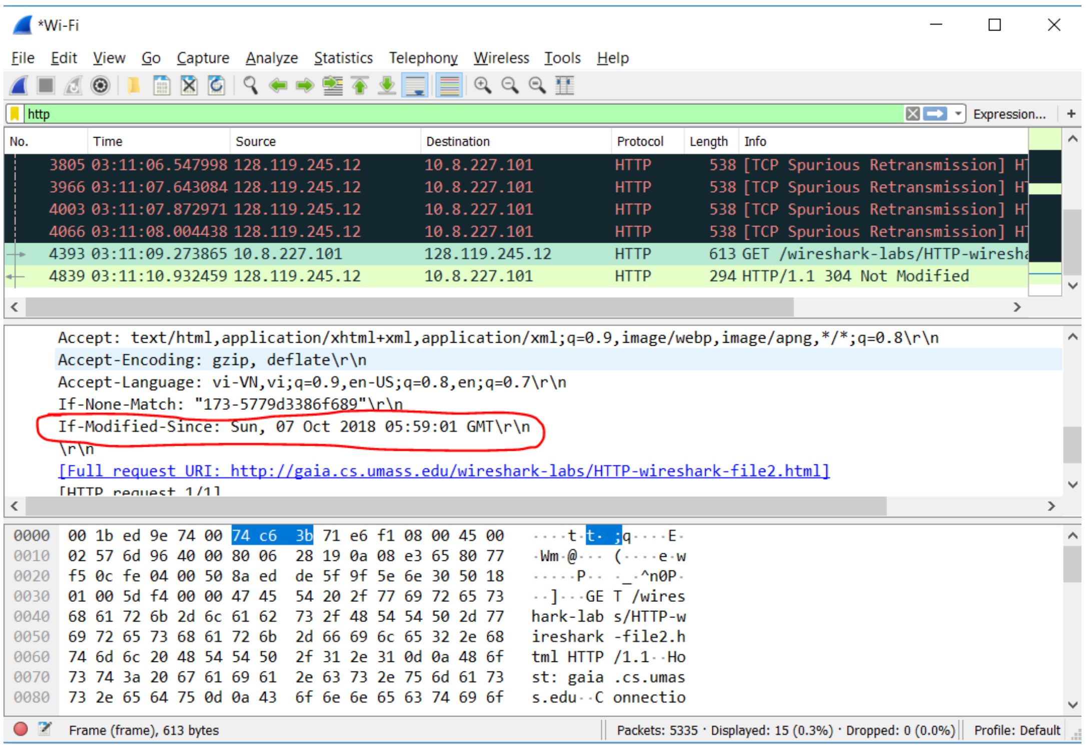
Yes, the server returned the contents of the file (text/html)


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

```
http

No.  Time            Source          Destination     Protocol Length Info
2922 03:11:01.160380 10.8.227.101    128.119.245.12  HTTP     501 GET /wireshark-labs/HTTP-wiresha
3194 03:11:02.606013 128.119.245.12  10.8.227.101    HTTP     784 HTTP/1.1 200 OK  (text/html)
3227 03:11:02.743503 10.8.227.101    128.119.245.12  HTTP     472 GET /favicon.ico HTTP/1.1
3361 03:11:03.789222 128.119.245.12  10.8.227.101    HTTP     784 [TCP Spurious Retransmission] H
3485 03:11:04.713032 128.119.245.12  10.8.227.101    HTTP     784 [TCP Spurious Retransmission] H
3581 03:11:05.657534 128.119.245.12  10.8.227.101    HTTP     784 [TCP Spurious Retransmission] H

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.8.227.101
> Transmission Control Protocol, Src Port: 80, Dst Port: 65027, Seq: 1, Ack: 448, Len: 730
v Hypertext Transfer Protocol
  v HTTP/1.1 200 OK\r\n
    > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK

0000  74 c6 3b 71 e6 f1 00 1b  ed 9e 74 00 08 00 45 00   t·;q····  ··t···E·
0010  03 02 c9 5e 40 00 2d 06  1e a6 80 77 f5 0c 0a 08   ···^@·-·  ···w····
0020  e3 65 00 50 fe 03 15 01  5b e1 91 64 2e 87 50 18   ·e·P····  [··d.·P·
0030  00 ed c0 1e 00 00 48 54  54 50 2f 31 2e 31 20 32   ······HT  TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 4d 6f 6e   00 OK··D  ate: Mon
0050  2c 20 30 38 20 4f 63 74  20 32 30 31 38 20 30 33   , 08 Oct   2018 03
0060  3a 31 31 3a 30 31 20 47  4d 54 0d 0a 53 65 72 76   :11:01 G  MT··Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac  he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS  ) OpenSS

Frame (frame), 784 bytes    Packets: 5335 · Displayed: 15 (0.3%) · Dropped: 0 (0.0%)    Profile: Default
```

Q 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 header "IF-MODIFIED-SINCE" appeared in second HTTP GET request. The information followed was Sun, 07 Oct 2018 05:59:01 GMT.


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

```
No.   Time                Source          Destination     Protocol Length Info
 3805 03:11:06.547998 128.119.245.12  10.8.227.101    HTTP     538 [TCP Spurious Retransmission] H
 3966 03:11:07.643084 128.119.245.12  10.8.227.101    HTTP     538 [TCP Spurious Retransmission] H
 4003 03:11:07.872971 128.119.245.12  10.8.227.101    HTTP     538 [TCP Spurious Retransmission] H
 4066 03:11:08.004438 128.119.245.12  10.8.227.101    HTTP     538 [TCP Spurious Retransmission] H
 4393 03:11:09.273865 10.8.227.101    128.119.245.12  HTTP     613 GET /wireshark-labs/HTTP-wiresha
 4839 03:11:10.932459 128.119.245.12  10.8.227.101    HTTP     294 HTTP/1.1 304 Not Modified
```

```
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: vi-VN,vi;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    If-None-Match: "173-5779d3386f689"\r\n
    If-Modified-Since: Sun, 07 Oct 2018 05:59:01 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
```

```
0000  00 1b ed 9e 74 00 74 c6  3b 71 e6 f1 08 00 45 00   ····t·t· ;q····E·
0010  02 57 6d 96 40 00 80 06  28 19 0a 08 e3 65 80 77   ·Wm·@··· (····e·w
0020  f5 0c fe 04 00 50 8a ed  de 5f 9f 5e 6e 30 50 18   ·····P·· ·_·^n0P·
0030  01 00 5d f4 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 32 2e 68   ireshark -file2.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
```

Frame (frame), 613 bytes | Packets: 5335 · Displayed: 15 (0.3%) · Dropped: 0 (0.0%) | Profile: Default

Q 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.

HTTP status code and phrase: 304 Not Modified

The server did not return the contents of the file. Because the header "IF-MODIFIED-SINCE" of the second HTTP GET request was Sun, 07 Oct 2018 05:59:01 GMT and the header "LAST-MODIFIED" of the first HTTP GET response was Sun, 07 Oct 2018 05:59:01 GMT. It means that if the file cached was modified (updated) since Sun, 07 Oct 2018 05:59:01 GMT, then it returned to client directly (not making request to the origin server anymore).

3. RETRIEVING LONG DOCUMENTS

In our examples thus far, the documents retrieved have been simple and short HTML files. Let's next see what happens when we download a long HTML file. Do the following:

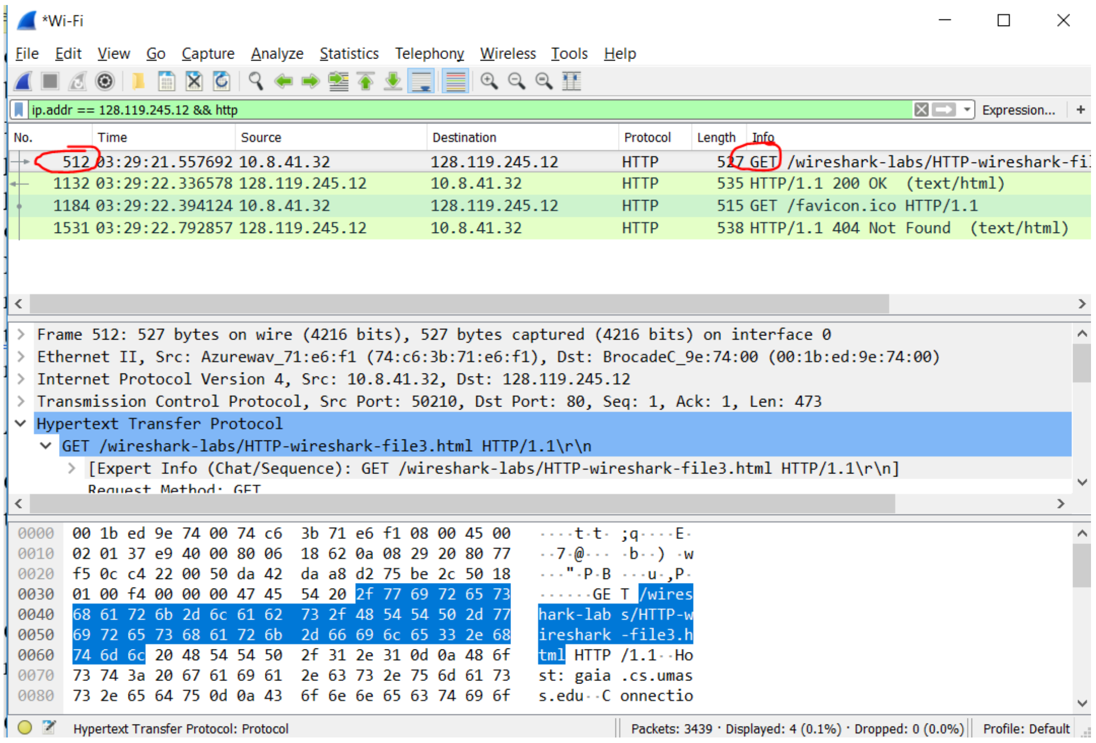
- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html, your browser should display the rather lengthy US Bill of Rights.
- Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

In the packet-listing window, you should see your HTTP GET message, followed by a multiple-packet TCP response to your HTTP GET request. This multiple-packet response deserves a bit of explanation. Recall from Section 2.2 (see Figure 2.9 in the text) that the HTTP response message consists of a status line, followed by header lines, followed by a blank line, followed by the entity body. In the case of our HTTP GET, the entity body in the response is the entire requested HTML file. In our case here, the HTML file is rather long, and at 4500 bytes is too large to fit in one TCP packet. The single HTTP response message is thus broken into several pieces by TCP, with each piece being contained within a separate TCP segment (see Figure 1.24 in the text). In recent versions of Wireshark, Wireshark indicates each TCP segment as a separate packet, and the fact that the single HTTP response was fragmented across multiple TCP packets is indicated by the "TCP segment of a reassembled PDU" in the Info column of the Wireshark display. Earlier versions of Wireshark used the "Continuation" phrase to indicated that the entire content of an HTTP message was broken across multiple TCP segments.. We stress here that there is no "Continuation" message in HTTP!

Answer the following questions:

Q 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?

Only 1 HTTP GET request message that my browser sent (packet number: 512)


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

ip.addr == 128.119.245.12 && http

```
No.   Time            Source          Destination     Protocol  Length Info
 512 03:29:21.557692 10.8.41.32      128.119.245.12  HTTP       527 GET /wireshark-labs/HTTP-wireshark-fi
1132 03:29:22.336578 128.119.245.12  10.8.41.32      HTTP       535 HTTP/1.1 200 OK  (text/html)
1184 03:29:22.394124 10.8.41.32      128.119.245.12  HTTP       515 GET /favicon.ico HTTP/1.1
1531 03:29:22.792857 128.119.245.12  10.8.41.32      HTTP       538 HTTP/1.1 404 Not Found  (text/html)
```

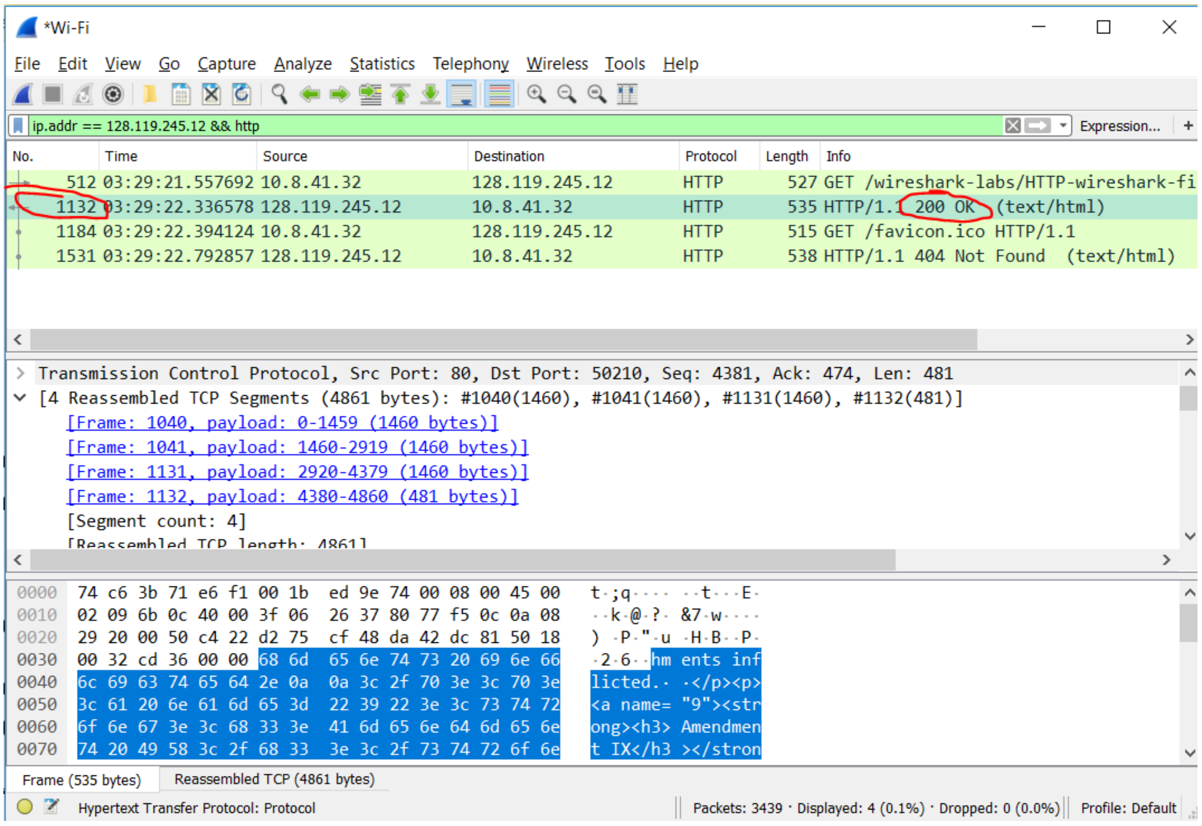
```
> Frame 512: 527 bytes on wire (4216 bits), 527 bytes captured (4216 bits) on interface 0
> Ethernet II, Src: Azurewav_71:e6:f1 (74:c6:3b:71:e6:f1), Dst: BrocadeC_9e:74:00 (00:1b:ed:9e:74:00)
> Internet Protocol Version 4, Src: 10.8.41.32, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50210, Dst Port: 80, Seq: 1, Ack: 1, Len: 473
v Hypertext Transfer Protocol
  v GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
```

```
0000  00 1b ed 9e 74 00 74 c6  3b 71 e6 f1 08 00 45 00   ····t·t· ;q····E·
0010  02 01 37 e9 40 00 80 06  18 62 0a 08 29 20 80 77   ··7·@··· ·b··) ·w
0020  f5 0c c4 22 00 50 da 42  da a8 d2 75 be 2c 50 18   ···"·P·B ···u·,P·
0030  01 00 f4 00 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
```

Hypertext Transfer Protocol: Protocol | Packets: 3439 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

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

Packet number: 1132


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

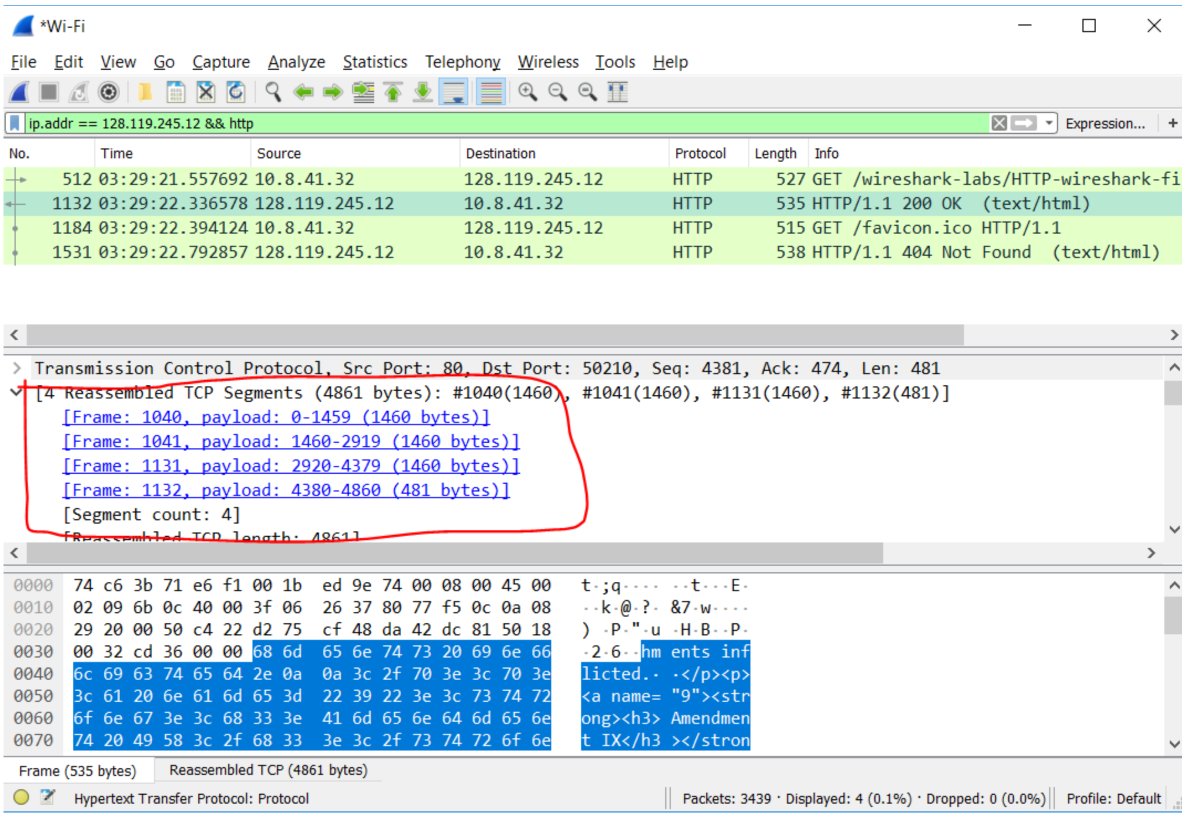
```
ip.addr == 128.119.245.12 && http

No.   Time            Source          Destination     Protocol Length Info
 512 03:29:21.557692 10.8.41.32      128.119.245.12  HTTP     527 GET /wireshark-labs/HTTP-wireshark-fi
1132 03:29:22.336578 128.119.245.12  10.8.41.32      HTTP     535 HTTP/1.1 200 OK  (text/html)
1184 03:29:22.394124 10.8.41.32      128.119.245.12  HTTP     515 GET /favicon.ico HTTP/1.1
1531 03:29:22.792857 128.119.245.12  10.8.41.32      HTTP     538 HTTP/1.1 404 Not Found  (text/html)

> Transmission Control Protocol, Src Port: 80, Dst Port: 50210, Seq: 4381, Ack: 474, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #1040(1460), #1041(1460), #1131(1460), #1132(481)]
    [Frame: 1040, payload: 0-1459 (1460 bytes)]
    [Frame: 1041, payload: 1460-2919 (1460 bytes)]
    [Frame: 1131, payload: 2920-4379 (1460 bytes)]
    [Frame: 1132, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]

0000  74 c6 3b 71 e6 f1 00 1b  ed 9e 74 00 08 00 45 00   t·;q····  ··t···E·
0010  02 09 6b 0c 40 00 3f 06  26 37 80 77 f5 0c 0a 08   ··k·@·?·  &7·w····
0020  29 20 00 50 c4 22 d2 75  cf 48 da 42 dc 81 50 18   ) ·P·"·u  ·H·B··P·
0030  00 32 cd 36 00 00 68 6d  65 6e 74 73 20 69 6e 66   ·2·6··hm ents inf
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.·  ·</p><p>
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73 74 72   <a name= "9"><str
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d 65 6e   ong><h3> Amendmen
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72 6f 6e   t IX</h3 ></stron

Frame (535 bytes)   Reassembled TCP (4861 bytes)
Hypertext Transfer Protocol: Protocol   Packets: 3439 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%)   Profile: Default
```

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

Status code and phrase: 200 OK

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

4 TCP segments that were needed to carry the single HTTP response and the text of the Bill of Rights.


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

```
ip.addr == 128.119.245.12 && http

No.   Time             Source         Destination    Protocol Length Info
 512 03:29:21.557692 10.8.41.32     128.119.245.12 HTTP     527 GET /wireshark-labs/HTTP-wireshark-fi
1132 03:29:22.336578 128.119.245.12 10.8.41.32     HTTP     535 HTTP/1.1 200 OK  (text/html)
1184 03:29:22.394124 10.8.41.32     128.119.245.12 HTTP     515 GET /favicon.ico HTTP/1.1
1531 03:29:22.792857 128.119.245.12 10.8.41.32     HTTP     538 HTTP/1.1 404 Not Found  (text/html)
```

```
> Transmission Control Protocol, Src Port: 80, Dst Port: 50210, Seq: 4381, Ack: 474, Len: 481
v [4 Reassembled TCP Segments (4861 bytes): #1040(1460), #1041(1460), #1131(1460), #1132(481)]
    [Frame: 1040, payload: 0-1459 (1460 bytes)]
    [Frame: 1041, payload: 1460-2919 (1460 bytes)]
    [Frame: 1131, payload: 2920-4379 (1460 bytes)]
    [Frame: 1132, payload: 4380-4860 (481 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
```

```
0000  74 c6 3b 71 e6 f1 00 1b  ed 9e 74 00 08 00 45 00   t·;q···· ··t···E·
0010  02 09 6b 0c 40 00 3f 06  26 37 80 77 f5 0c 0a 08   ··k·@·?· &7·w····
0020  29 20 00 50 c4 22 d2 75  cf 48 da 42 dc 81 50 18   ) ·P·"·u ·H·B··P·
0030  00 32 cd 36 00 00 68 6d  65 6e 74 73 20 69 6e 66   ·2·6··hm ents inf
0040  6c 69 63 74 65 64 2e 0a  0a 3c 2f 70 3e 3c 70 3e   licted.· ·</p><p>
0050  3c 61 20 6e 61 6d 65 3d  22 39 22 3e 3c 73 74 72   <a name= "9"><str
0060  6f 6e 67 3e 3c 68 33 3e  41 6d 65 6e 64 6d 65 6e   ong><h3> Amendmen
0070  74 20 49 58 3c 2f 68 33  3e 3c 2f 73 74 72 6f 6e   t IX</h3 ></stron
```

Frame (535 bytes) Reassembled TCP (4861 bytes)

Hypertext Transfer Protocol: Protocol | Packets: 3439 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

4. HTML DOCUMENTS WITH EMBEDDED OBJECTS

Now that we've seen how Wireshark displays the captured packet traffic for large HTML files, we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server(s).

Do the following:

- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html, your browser should display a short HTML file with two images. These two images are referenced in the base HTML file. That is, the images themselves are not contained in the HTML; instead the URLs for the images are contained in the downloaded HTML file. As discussed in the textbook, your browser will have to retrieve these logos from the indicated web sites. Our publisher's logo is retrieved from the www.aw-bc.com web site. The image of the cover for our 5th edition (one of our favorite covers) is stored at the manic.cs.umass.edu server.
- Stop Wireshark packet capture, and enter "http" in the display-filter-specification window, so that only captured HTTP messages will be displayed.

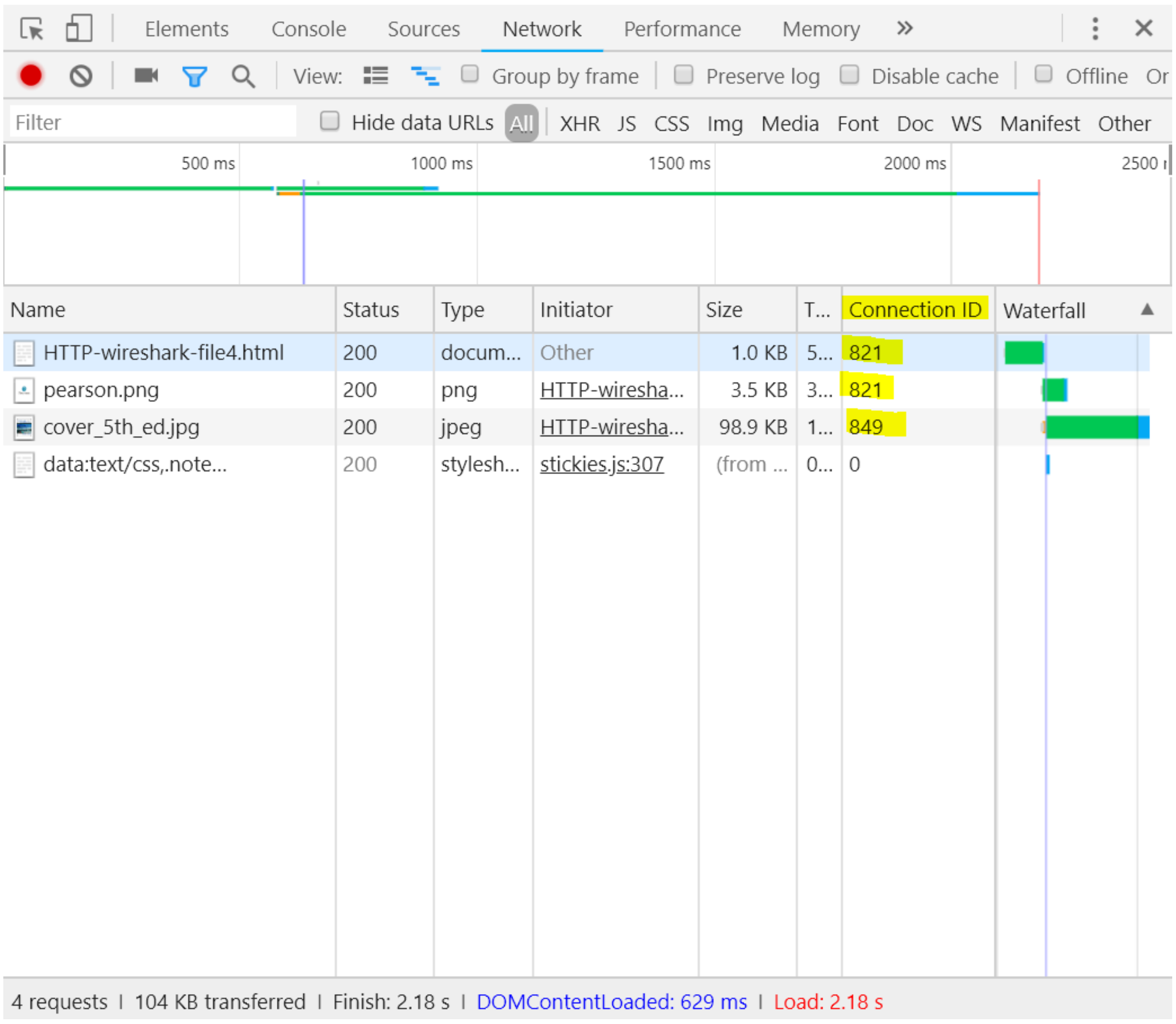
Answer the following questions:

Q16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

There were 3 HTTP GET requests that my browser sent. The destination IP address of 3 request was the same: 128.119.245.12 because all the objects and files were on the same host.

Q17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

My browser downloaded the 2 images in parallel.



Name	Status	Type	Initiator	Size	T...	Connection ID
HTTP-wireshark-file4.html	200	docum...	Other	1.0 KB	5...	821
pearson.png	200	png	HTTP-wiresha...	3.5 KB	3...	821
cover_5th_ed.jpg	200	jpeg	HTTP-wiresha...	98.9 KB	1...	849
data:text/css,.note...	200	stylesh...	stickies.js:307	(from ...	0...	0

4 requests | 104 KB transferred | Finish: 2.18 s | DOMContentLoaded: 629 ms | Load: 2.18 s

In chrome developer tools, we can see that after the first request to get html file, two different parrallel connection whose id 821 and 849, respectively, were opened to get the next two images. The reason the first image (pearson.png) connection id was same as the html connection id (821) because the first request the browser set header “connection: keep-alive” that means the browser wanted to keep persistent connection. After getting the html file, the browser still used the same connection (id=821) to get first image and simultaneously opened new TCP connection (id=849) to get the second image.

THE END.

This lab content is from the lab materials of the book “Computer Networking: a Top-Down Approach.”