Project 1: CMPT 371 **Alan Ou**
301320642

Question 1

a) **Traceroute to www.microsoft.com**

```
Tracing route to e13678.dspb.akamaiedge.net [23.59.156.241]
over a maximum of 30 hops:

  1     2 ms     2 ms     1 ms  192.168.1.254
  2     3 ms     4 ms     3 ms  96.1.208.76
  3     4 ms     4 ms     3 ms  154.11.12.196
  4     *        *        *     Request timed out.
  5     6 ms     6 ms     4 ms  a23-59-156-241.deploy.static.akamaitechnologies.com [23.59.156.241]

Trace complete.
```

b) The ISP networks passed through are:

192.186.1.254 which I assume is my router IP address,
96.1.208.76 which I assume would be my ISP's IP address,
154.11.12.196 is another IP address from my ISP,
the fourth hop was a no response signal because the router did not respond, and
23.59.156.241 which would be the destination IP address hosted by Akamai.

c) Since the destination roundtrip delays are a bit longer than the roundtrip delays of the first three hops, which I assumed to be local router IPs, and since Seattle is quite close to Vancouver, I would assume that Microsoft's server is in Seattle.

a) **Traceroute to www.apple.com**

```
Tracing route to e6858.dsce9.akamaiedge.net [173.222.233.107]
over a maximum of 30 hops:

  1     3 ms     7 ms     2 ms  192.168.1.254
  2     3 ms     2 ms    12 ms  96.1.208.76
  3     7 ms     7 ms    17 ms  154.11.12.201
  4     6 ms     6 ms    13 ms  ix-ae-27-0.tcore1.00s-seattle.as6453.net [64.86.123.208]
  5     9 ms    10 ms     8 ms  if-ae-2-2.tcore2.00s-seattle.as6453.net [64.86.123.93]
  6    34 ms    27 ms    25 ms  207.45.206.78
  7    16 ms    12 ms    12 ms  ae2.digfort-sea3.netarch.akamai.com [23.203.145.152]
  8     6 ms    10 ms     7 ms  a173-222-233-107.deploy.static.akamaitechnologies.com [173.222.233.107]

Trace complete.
```

b) The ISP networks passed through are 192.186.1.254 which I assume is my router IP address,
96.1.208.76 which I assume would be the ISP's IP address,
154.11.12.196 is another IP address from my ISP,
64.86.123.208 and 64.86.123.93 would be the same ISP (TATA COMMUNICATIONS (AMERICA) INC) because they have very similar IP's,
207.45.206.78 is another IP held by TATA COMMUNICATIONS (AMERICA) INC, however, the server is likely in a different part of the US,
23.203.145.152, and
173.222.233.107 which would be the destination IP address; both 23.203.145.152, and 173.222.233.107 are IP addresses held by Akamai, but servers are likely in different locations.

c) Apple's headquarters is in Cupertino, California; however, the traceroute result does not seem to reflect that. The roundtrip times for the destination hop is 6ms 10ms 7ms, which is only a bit longer than 6 ms 6 ms 4 ms, the roundtrip delays for the destination hop for www.microsoft.com, which I assumed the server was in Seattle. As a result, I assume that the sever for www.apple.com would be hosted somewhere a bit further than Seattle like Portland, but not as far as in California.

a) Traceroute to www.google.com

```
Tracing route to www.google.com [172.217.14.228]
over a maximum of 30 hops:

  1    24 ms     1 ms     1 ms  192.168.1.254
  2     4 ms     3 ms     6 ms  96.1.208.76
  3     *        *        *     Request timed out.
  4     9 ms    10 ms     6 ms  74.125.50.110
  5    13 ms     7 ms     9 ms  74.125.243.177
  6     9 ms     7 ms     7 ms  209.85.254.247
  7     6 ms     7 ms     7 ms  sea30s02-in-f4.1e100.net [172.217.14.228]

Trace complete.
```

b) The ISP networks passed through are 192.186.1.254 which I assume is my router IP address, 96.1.208.76 which I assume would be the ISP's IP address. Oddly, the route to www.google.com did not pass through the router 154.11.12.196, instead there was a no response signal for hop 3.

The other ISP routers passed through are 74.125.50.110 and 74.125.243.177 which I assume would be the same ISP provider (Google LLC) because of the similar IP addresses,
209.85.254.247,
and 172.217.14.228 which would be the destination IP address

The last four hops pass through routers held by Google LLC, however, the first two servers, server at hop 6, and sever at hop 7 are likely in different locations because of the difference in IP addresses.

c) Google's headquarters is in Mountain View, California; however, the traceroute result does not appear to show that. The roundtrip times for the destination hop is 6ms 7ms 7ms, which is only a bit longer than the roundtrip delay of the destination hop for www.microsoft.com at 6 ms 6 ms 4 ms, which I assumed the server would be in Seattle. As a result, I assume that the server for www.google.com would be hosted somewhere near Seattle or somewhere around the same distance from Vancouver.

Question 2

a) Persistent http: section 8.1

Caching: section 13

Commands (GET, etc.): If we include all the commands (OPTIONS to CONNECT) then it would be from sections 9.2 to 9.9; if we only include the common HTTP commands (GET, HEAD, POST, PUT, DELETE, TRACE, and CONNECT) then it would be from sections 9.3 to 9.9. Below is a section of the table of contents regarding HTTP commands from RFC 2616 for HTTP 1.1:

```
9.2   OPTIONS ...................................................52
9.3   GET .......................................................53
9.4   HEAD ......................................................54
9.5   POST ......................................................54
9.6   PUT .......................................................55
9.7   DELETE ....................................................56
9.8   TRACE .....................................................56
9.9   CONNECT ...................................................57
```

Transport layer protocol: section 1.4

b) A persistent connection with pipelining is when the sever keeps its connection open after its initial response and allowing the client to send as many requests as wanted and as soon as they are encountered, in other words, the client can send requests without waiting for an OK response.

The RFC description of persistent connection is "Prior to persistent connections, a separate TCP connection was established to fetch each URL, increasing the load on HTTP servers and causing congestion on the Internet." The RFC connection of persistent connection with pipelining is "A client that supports persistent connections MAY "pipeline" its requests (i.e., send multiple requests without waiting for each response). A server MUST send its responses to those requests in the same order that the requests were received"

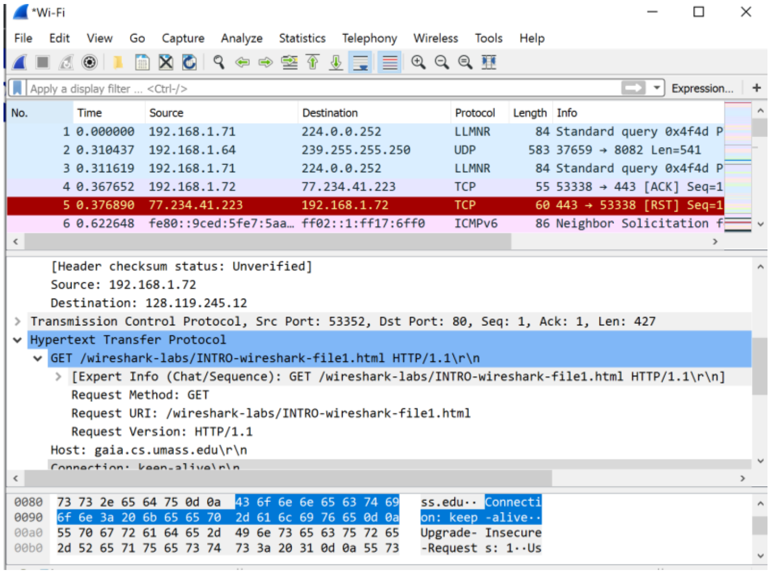
Overall, I found my definition and the definition from the RFC description to be similar.

Question 4

P78: "Packet sniffer"

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

LLMNR, UDP, TCP

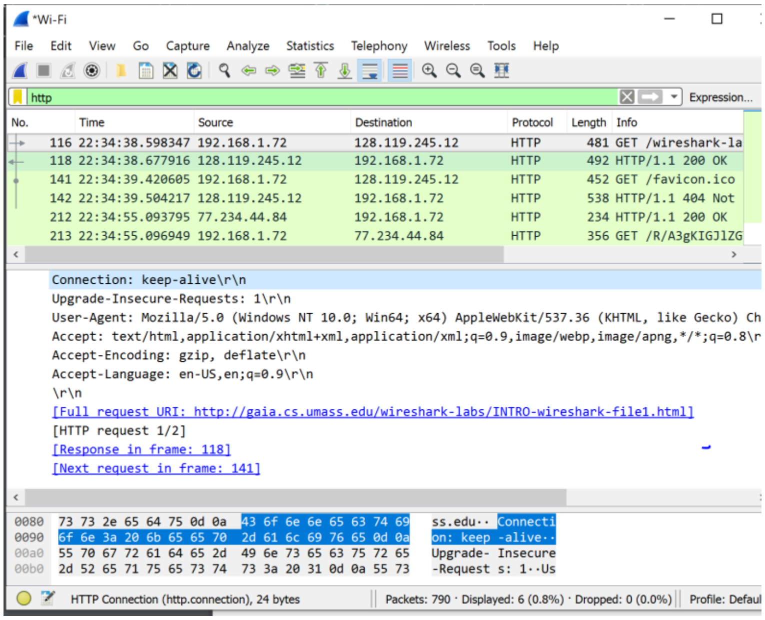


```
No.  Time      Source                Destination       Protocol Length Info
   1 0.000000  192.168.1.71          224.0.0.252       LLMNR        84 Standard query 0x4f4d P
   2 0.310437  192.168.1.64          239.255.255.250   UDP         583 37659 → 8082 Len=541
   3 0.311619  192.168.1.71          224.0.0.252       LLMNR        84 Standard query 0x4f4d P
   4 0.367652  192.168.1.72          77.234.41.223     TCP          55 53338 → 443 [ACK] Seq=1
   5 0.376890  77.234.41.223         192.168.1.72      TCP          60 443 → 53338 [RST] Seq=1
   6 0.622648  fe80::9ced:5fe7:5aa…  ff02::1:ff17:6ff0 ICMPv6       86 Neighbor Solicitation f
```

```
      [Header checksum status: Unverified]
      Source: 192.168.1.72
      Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 53352, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
v Hypertext Transfer Protocol
  v GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/INTRO-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
```

```
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
```

2) How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet listing window is the amount of time, in seconds, since Wireshark tracing began.



```
http
```

```
No.  Time             Source          Destination     Protocol Length Info
 116 22:34:38.598347 192.168.1.72    128.119.245.12  HTTP        481 GET /wireshark-la
 118 22:34:38.677916 128.119.245.12  192.168.1.72    HTTP        492 HTTP/1.1 200 OK
 141 22:34:39.420605 192.168.1.72    128.119.245.12  HTTP        452 GET /favicon.ico
 142 22:34:39.504217 128.119.245.12  192.168.1.72    HTTP        538 HTTP/1.1 404 Not
 212 22:34:55.093795 77.234.44.84    192.168.1.72    HTTP        234 HTTP/1.1 200 OK
 213 22:34:55.096949 192.168.1.72    77.234.44.84    HTTP        356 GET /R/A3gKIGJ1ZG
```

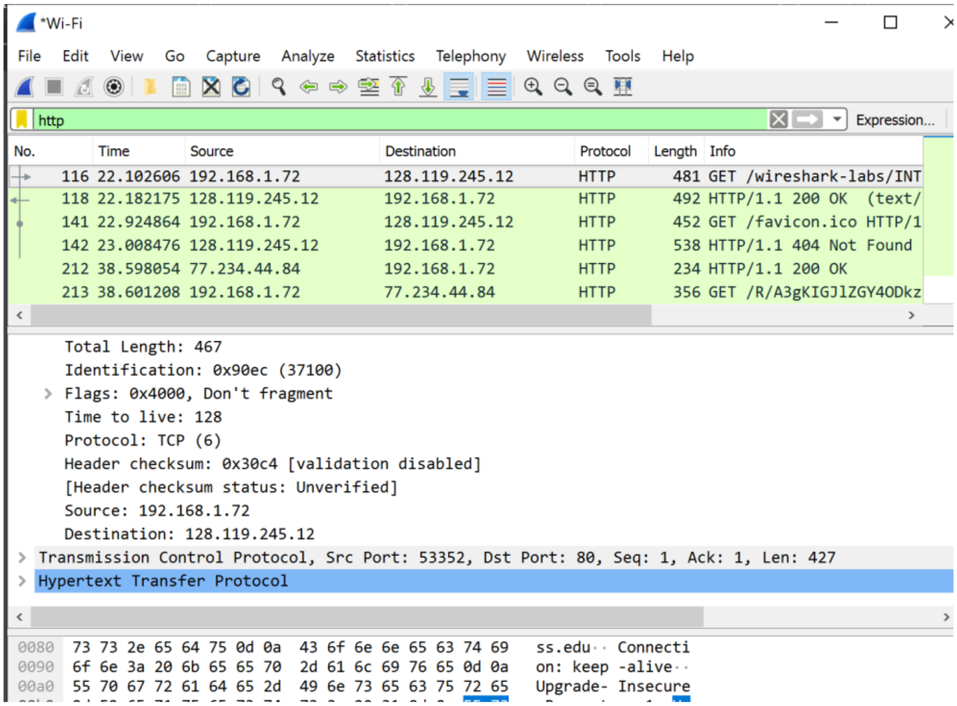
```
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 118]
    [Next request in frame: 141]
```

```
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
00b0  2d 52 65 71 75 65 73 74  73 3a 20 31 0d 0a 55 73   -Request s: 1··Us
```

```
HTTP Connection (http.connection), 24 bytes || Packets: 790 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%) || Profile: Defaul
```

38.677916 – 38.598347 = **0.079569 seconds**

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



```
http
```

```
No.   Time      Source          Destination     Protocol Length Info
  116 22.102606 192.168.1.72    128.119.245.12  HTTP      481 GET /wireshark-labs/INT
  118 22.182175 128.119.245.12  192.168.1.72    HTTP      492 HTTP/1.1 200 OK  (text/
  141 22.924864 192.168.1.72    128.119.245.12  HTTP      452 GET /favicon.ico HTTP/1
  142 23.008476 128.119.245.12  192.168.1.72    HTTP      538 HTTP/1.1 404 Not Found
  212 38.598054 77.234.44.84    192.168.1.72    HTTP      234 HTTP/1.1 200 OK
  213 38.601208 192.168.1.72    77.234.44.84    HTTP      356 GET /R/A3gKIGJlZGY4ODkz
```

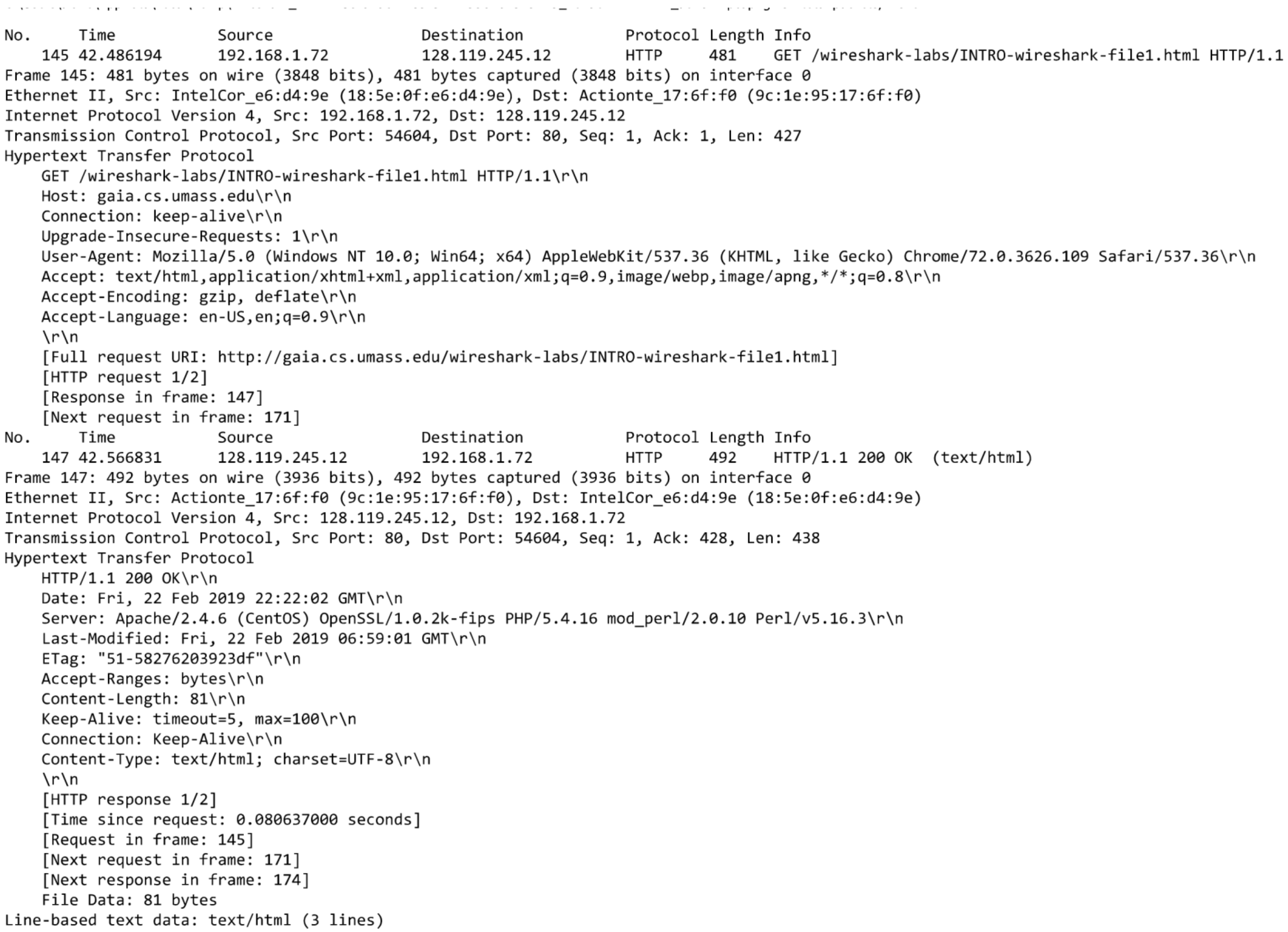
```
    Total Length: 467
    Identification: 0x90ec (37100)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x30c4 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.72
    Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 53352, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
> Hypertext Transfer Protocol
```

```
0080  73 73 2e 65 64 75 0d 0a  43 6f 6e 6e 65 63 74 69   ss.edu·· Connecti
0090  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
00a0  55 70 67 72 61 64 65 2d  49 6e 73 65 63 75 72 65   Upgrade- Insecure
```

The internet address of the gaia.cs.umass.edu appears to be 128.119.245.12 and the Internet address of my computer appears to be 192.168.1.72.

4) Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the "Selected Packet Only" and "Print as displayed" radial buttons, and then click OK

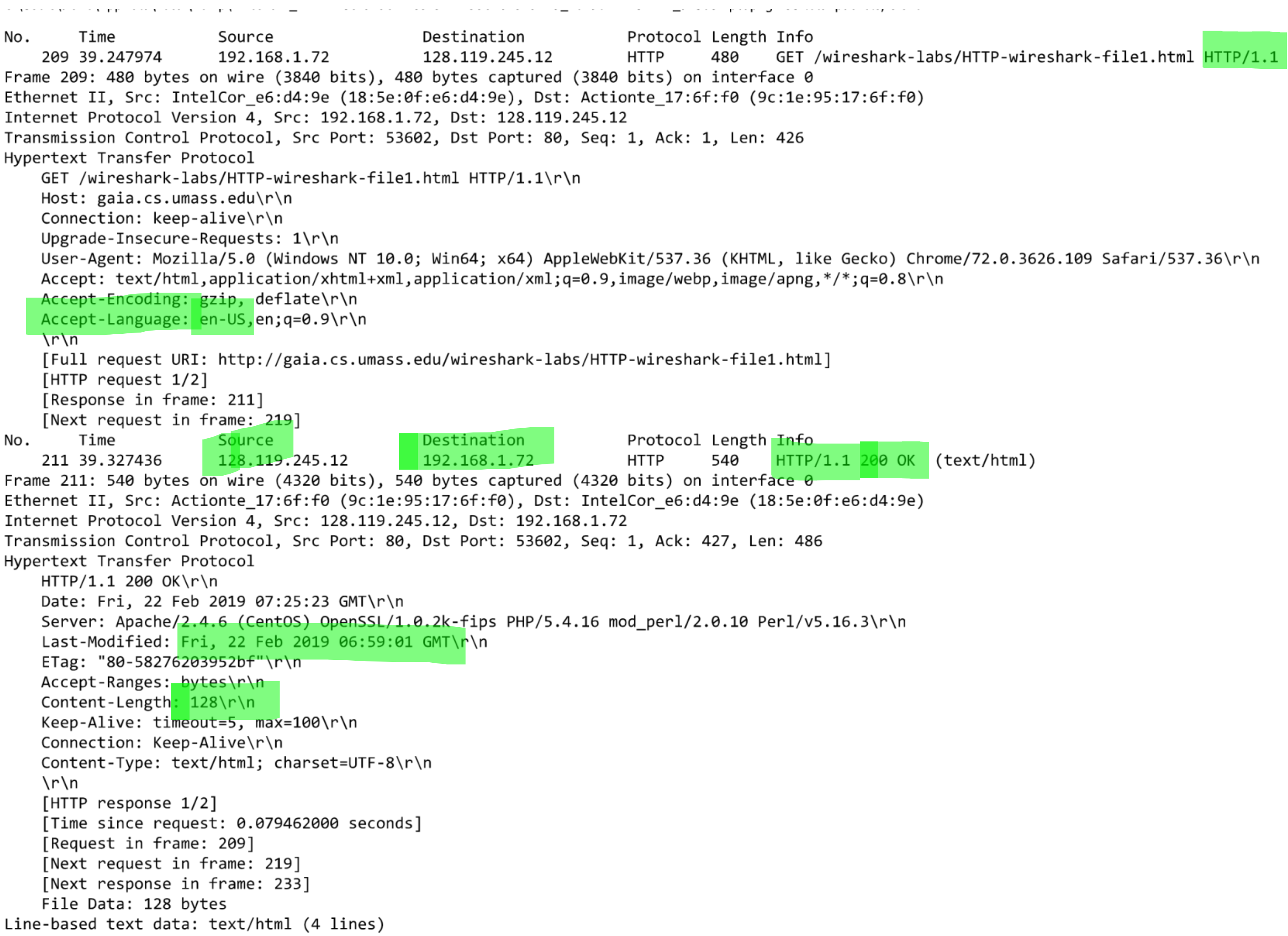
Shown below



```
No.     Time           Source                Destination           Protocol Length Info
    145 42.486194      192.168.1.72          128.119.245.12        HTTP     481    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 145: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface 0
Ethernet II, Src: IntelCor_e6:d4:9e (18:5e:0f:e6:d4:9e), Dst: Actionte_17:6f:f0 (9c:1e:95:17:6f:f0)
Internet Protocol Version 4, Src: 192.168.1.72, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 54604, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36\r\n
    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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 147]
    [Next request in frame: 171]
No.     Time           Source                Destination           Protocol Length Info
    147 42.566831      128.119.245.12        192.168.1.72          HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 147: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface 0
Ethernet II, Src: Actionte_17:6f:f0 (9c:1e:95:17:6f:f0), Dst: IntelCor_e6:d4:9e (18:5e:0f:e6:d4:9e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.72
Transmission Control Protocol, Src Port: 80, Dst Port: 54604, Seq: 1, Ack: 428, Len: 438
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 22 Feb 2019 22:22:02 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: Fri, 22 Feb 2019 06:59:01 GMT\r\n
    ETag: "51-58276203923df"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.080637000 seconds]
    [Request in frame: 145]
    [Next request in frame: 171]
    [Next response in frame: 174]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

Project 1: CMPT 371 **Alan Ou**
301320642

P183: HTTP



```
No.     Time           Source                Destination           Protocol Length Info
    209 39.247974      192.168.1.72          128.119.245.12        HTTP     480    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
Frame 209: 480 bytes on wire (3840 bits), 480 bytes captured (3840 bits) on interface 0
Ethernet II, Src: IntelCor_e6:d4:9e (18:5e:0f:e6:d4:9e), Dst: Actionte_17:6f:f0 (9c:1e:95:17:6f:f0)
Internet Protocol Version 4, Src: 192.168.1.72, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53602, Dst Port: 80, Seq: 1, Ack: 1, Len: 426
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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.109 Safari/537.36\r\n
    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: en-US,en;q=0.9\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 211]
    [Next request in frame: 219]
No.     Time           Source                Destination           Protocol Length Info
    211 39.327436      128.119.245.12        192.168.1.72          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 211: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
Ethernet II, Src: Actionte_17:6f:f0 (9c:1e:95:17:6f:f0), Dst: IntelCor_e6:d4:9e (18:5e:0f:e6:d4:9e)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.72
Transmission Control Protocol, Src Port: 80, Dst Port: 53602, Seq: 1, Ack: 427, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Fri, 22 Feb 2019 07:25:23 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: Fri, 22 Feb 2019 06:59:01 GMT\r\n
    ETag: "80-58276203952bf"\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]
    [Time since request: 0.079462000 seconds]
    [Request in frame: 209]
    [Next request in frame: 219]
    [Next response in frame: 233]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

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. The server is running HTTP version 1.1 as well.

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

   My browser indicates on the line Accept-Language: en-US that it can accept en-US (English US).

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

   The IP address of my computer is 192.168.1.72. The IP address of the gaia.cs.umass.edu server is 128.119.245.12. These are specified by the source and destination IPs.

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

   The status code returned from the server to my browser is 200 OK. This is found in the info section of the OK message.

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

   The HTML file was last modified Friday, February 22, 2019 06:59:01 GMT. This is found by the "Last-Modified" line in the OK message.

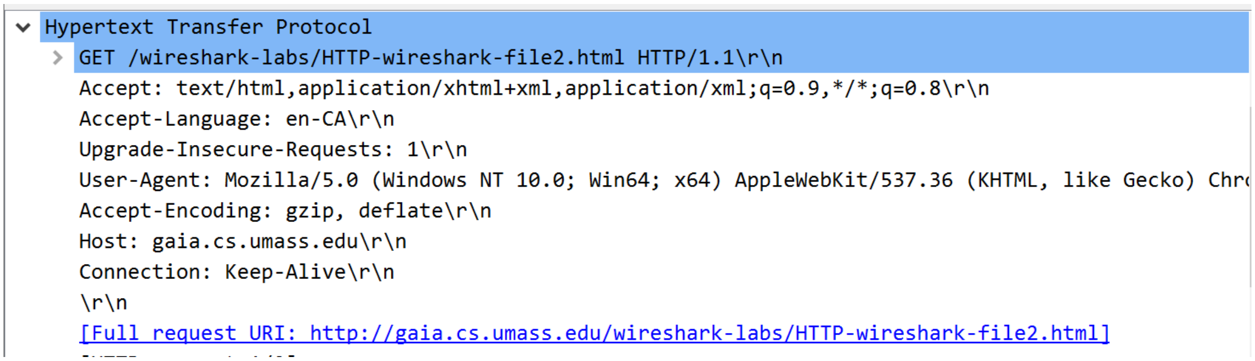
6) How many bytes of content are being returned to your browser?

   128 bytes are being returned. This is found by the "Content-Length" line in the OK message.

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

   No, all headers are displayed in the packet-listing window.

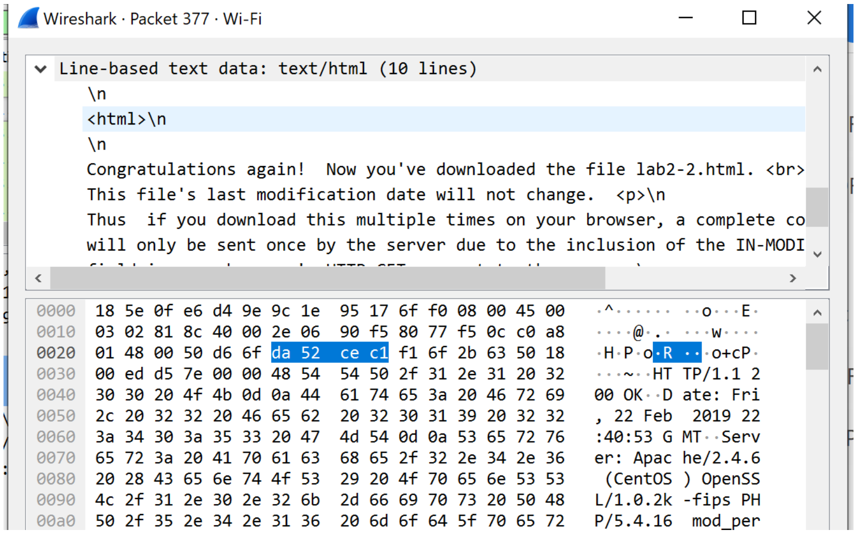
8) Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?



```
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-CA\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) Chr
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

No, there is no "IF-MODIFIED-SINCE" line in the HTTP GET.

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

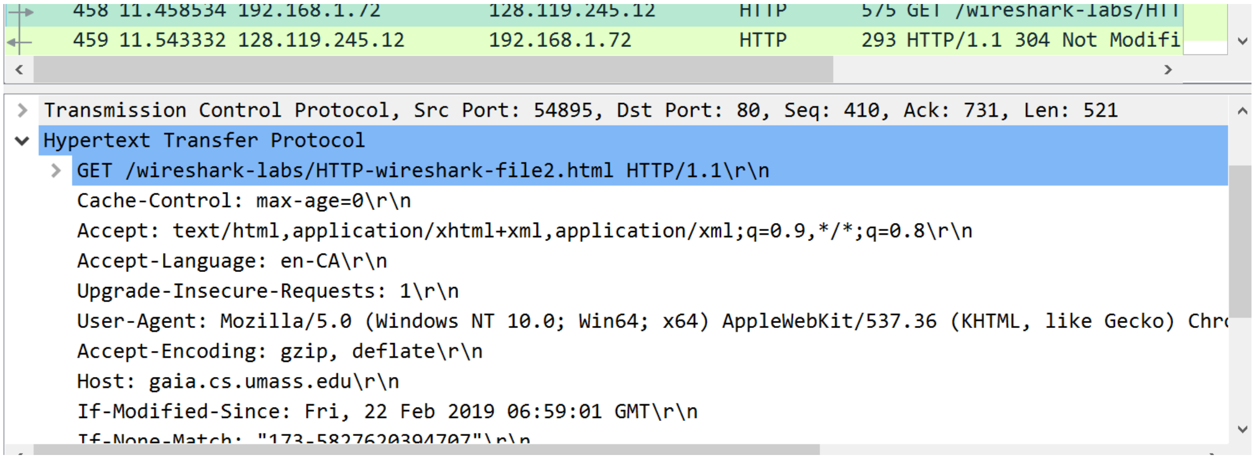


```
Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete co
    will only be sent once by the server due to the inclusion of the IN-MODI
```

```
0000  18 5e 0f e6 d4 9e 9c 1e  95 17 6f f0 08 00 45 00   ·^······ ··o···E·
0010  03 02 81 8c 40 00 2e 06  90 f5 80 77 f5 0c c0 a8   ····@·.· ···w····
0020  01 48 00 50 d6 6f da 52  ce c1 f1 6f 2b 63 50 18   ·H·P·o·R ···o+cP·
0030  00 ed d5 7e 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 46 72 69   00 OK··D ate: Fri
0050  2c 20 32 32 20 46 65 62  20 32 30 31 39 20 32 32   , 22 Feb  2019 22
0060  3a 34 30 3a 35 33 20 47  4d 54 0d 0a 53 65 72 76   :40:53 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
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
```

Yes, the server explicitly returned the contents of the file. This can be seen by looking at the "Line-based text data", which contains the content of the page content.

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?

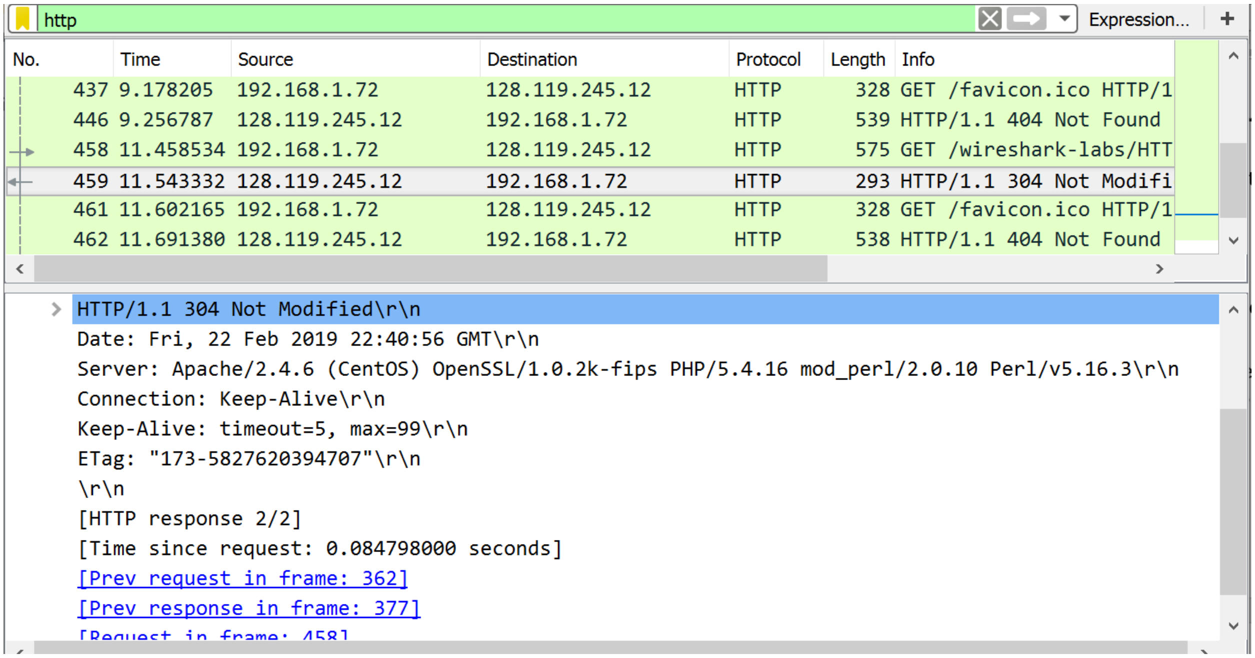


```
458 11.458534 192.168.1.72       128.119.245.12      HTTP     575 GET /wireshark-labs/HTT
459 11.543332 128.119.245.12     192.168.1.72        HTTP     293 HTTP/1.1 304 Not Modifi
```

```
> Transmission Control Protocol, Src Port: 54895, Dst Port: 80, Seq: 410, Ack: 731, Len: 521
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Cache-Control: max-age=0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-CA\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) Chr
    Accept-Encoding: gzip, deflate\r\n
    Host: gaia.cs.umass.edu\r\n
    If-Modified-Since: Fri, 22 Feb 2019 06:59:01 GMT\r\n
    If-None-Match: "173-5827620394707"\r\n
```

Yes, there is an "IF-MODIFIED-SINCE" line in the second HTTP GET request. The information the follows is Fri, 22 Feb 2019 06:59:01 GMT, which is the "Last-Modified" date and time of the first HTTP GET request.

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?

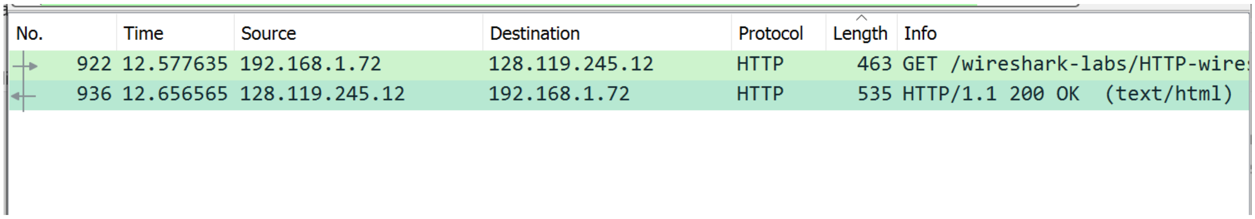


No.	Time	Source	Destination	Protocol	Length	Info
437	9.178205	192.168.1.72	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1
446	9.256787	128.119.245.12	192.168.1.72	HTTP	539	HTTP/1.1 404 Not Found
458	11.458534	192.168.1.72	128.119.245.12	HTTP	575	GET /wireshark-labs/HTT
459	11.543332	128.119.245.12	192.168.1.72	HTTP	293	HTTP/1.1 304 Not Modifi
461	11.602165	192.168.1.72	128.119.245.12	HTTP	328	GET /favicon.ico HTTP/1
462	11.691380	128.119.245.12	192.168.1.72	HTTP	538	HTTP/1.1 404 Not Found

```
> HTTP/1.1 304 Not Modified\r\n
  Date: Fri, 22 Feb 2019 22:40:56 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: "173-5827620394707"\r\n
  \r\n
  [HTTP response 2/2]
  [Time since request: 0.084798000 seconds]
  [Prev request in frame: 362]
  [Prev response in frame: 377]
  [Request in frame: 458]
```

The HTTP status code and phrase returned from the server in response to this second HTTP GET is “304 Not Modified”. The server did not explicitly return the contents of the file in this request because there were no modifications since the last time I downloaded the contents from the server, as a result, it simply reloaded the data from browser cache.

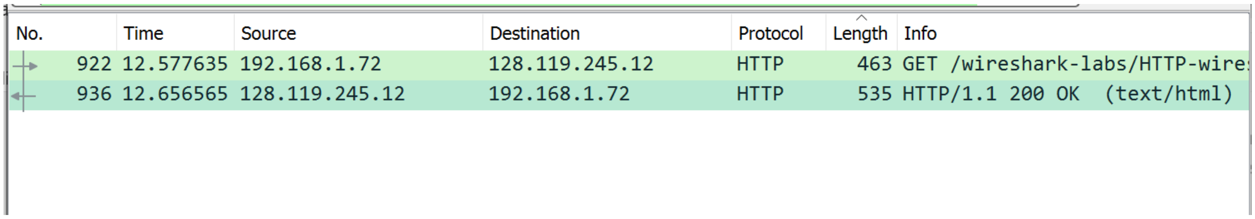
12) How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?



No.	Time	Source	Destination	Protocol	Length	Info
922	12.577635	192.168.1.72	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wire
936	12.656565	128.119.245.12	192.168.1.72	HTTP	535	HTTP/1.1 200 OK (text/html)

My browser only sent one HTTP GET request. The packet number was 922.

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



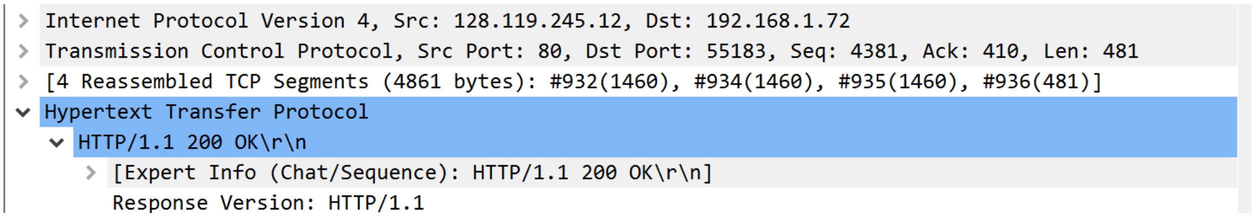
No.	Time	Source	Destination	Protocol	Length	Info
922	12.577635	192.168.1.72	128.119.245.12	HTTP	463	GET /wireshark-labs/HTTP-wire
936	12.656565	128.119.245.12	192.168.1.72	HTTP	535	HTTP/1.1 200 OK (text/html)

The packet number in the trace which contains the status code and phrase associated with the response to the HTTP GET request is 936.

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

The status code and phrase in the response is 200 OK.

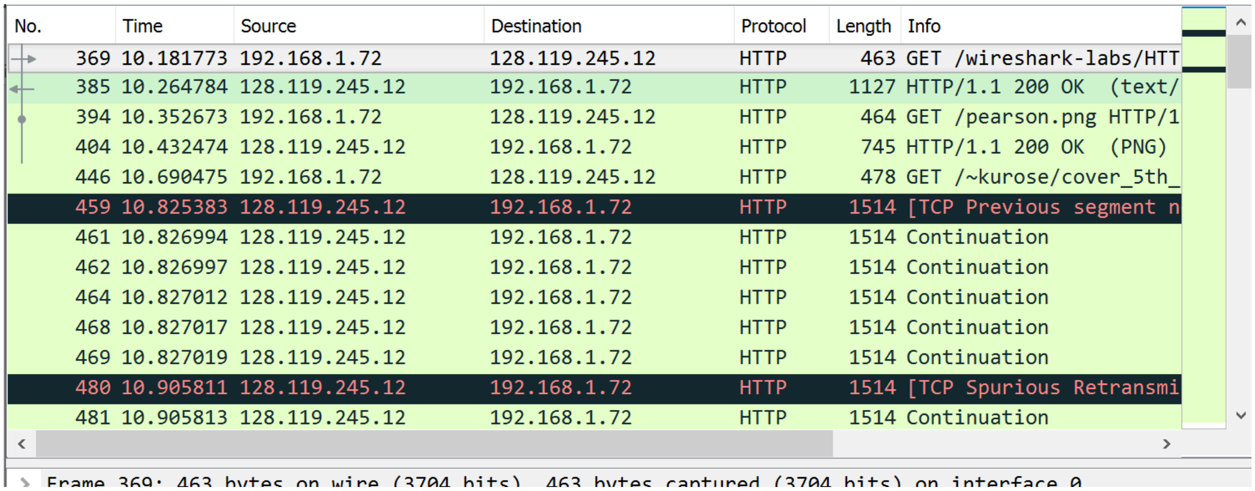
15) How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?



```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.72
> Transmission Control Protocol, Src Port: 80, Dst Port: 55183, Seq: 4381, Ack: 410, Len: 481
> [4 Reassembled TCP Segments (4861 bytes): #932(1460), #934(1460), #935(1460), #936(481)]
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
```

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

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



No.	Time	Source	Destination	Protocol	Length	Info
369	10.181773	192.168.1.72	128.119.245.12	HTTP	463	GET /wireshark-labs/HTT
385	10.264784	128.119.245.12	192.168.1.72	HTTP	1127	HTTP/1.1 200 OK (text/
394	10.352673	192.168.1.72	128.119.245.12	HTTP	464	GET /pearson.png HTTP/1
404	10.432474	128.119.245.12	192.168.1.72	HTTP	745	HTTP/1.1 200 OK (PNG)
446	10.690475	192.168.1.72	128.119.245.12	HTTP	478	GET /~kurose/cover_5th_
459	10.825383	128.119.245.12	192.168.1.72	HTTP	1514	[TCP Previous segment n
461	10.826994	128.119.245.12	192.168.1.72	HTTP	1514	Continuation
462	10.826997	128.119.245.12	192.168.1.72	HTTP	1514	Continuation
464	10.827012	128.119.245.12	192.168.1.72	HTTP	1514	Continuation
468	10.827017	128.119.245.12	192.168.1.72	HTTP	1514	Continuation
469	10.827019	128.119.245.12	192.168.1.72	HTTP	1514	Continuation
480	10.905811	128.119.245.12	192.168.1.72	HTTP	1514	[TCP Spurious Retransmi
481	10.905813	128.119.245.12	192.168.1.72	HTTP	1514	Continuation

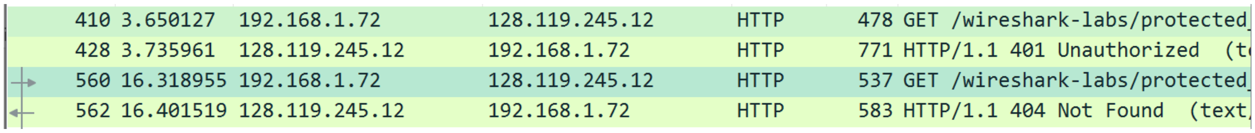
> Frame 369: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interface 0

There were three HTTP GET requests sent. These GET requests were all sent to 128.119.245.12.

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.

I believe the two images were downloaded serially because one, the times of the GET requests were quite a bit apart, and two, the GET request for the second image request was sent after the OK of the first GET request was returned.

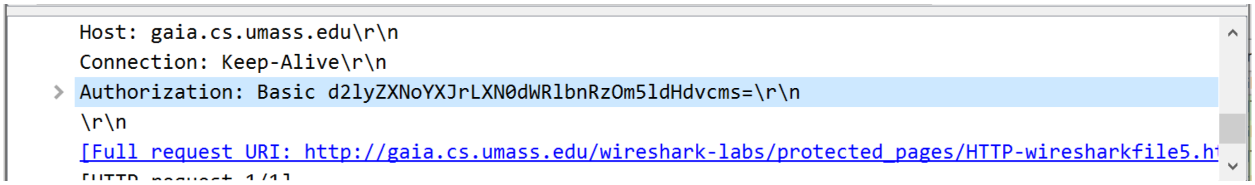
18) What is the server’s response (status code and phrase) in response to the initial HTTP GET message from your browser?



```
410 3.650127  192.168.1.72     128.119.245.12    HTTP    478 GET /wireshark-labs/protected_
428 3.735961  128.119.245.12   192.168.1.72      HTTP    771 HTTP/1.1 401 Unauthorized  (t
560 16.318955 192.168.1.72     128.119.245.12    HTTP    537 GET /wireshark-labs/protected_
562 16.401519 128.119.245.12   192.168.1.72      HTTP    583 HTTP/1.1 404 Not Found  (text
```

The server’s response was 401 Unauthorized

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



```
    Host: gaia.cs.umass.edu\r\n
    Connection: Keep-Alive\r\n
  > Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.ht
    [HTTP request 1/1]
```

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n