786

Name: Muhammad Sherjeel Akhtar

Roll No: 20p-0101

Subject: Computer Network Lab

Task No: 8

Submitted **T**o **R**espect Ma'am: **Miss Hurmat Hidayat**

Section: B

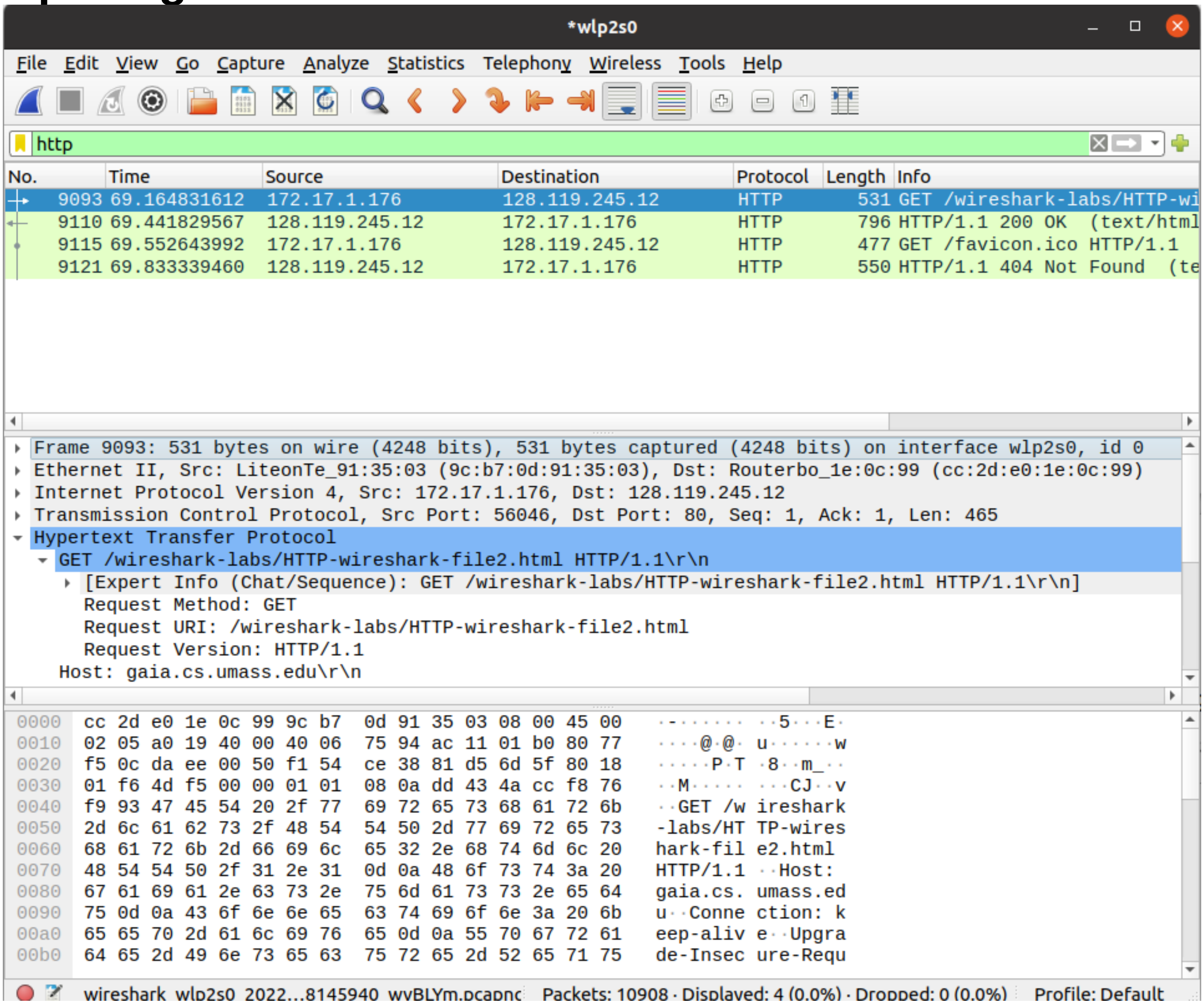
Question 1:

Answer:

Wireshark:

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.

Opening the Wireshark:



http

```
No.    Time              Source          Destination      Protocol  Length  Info
9093   69.164831612      172.17.1.176    128.119.245.12   HTTP      531     GET /wireshark-labs/HTTP-wi
9110   69.441829567      128.119.245.12  172.17.1.176     HTTP      796     HTTP/1.1 200 OK  (text/html
9115   69.552643992      172.17.1.176    128.119.245.12   HTTP      477     GET /favicon.ico HTTP/1.1
9121   69.833339460      128.119.245.12  172.17.1.176     HTTP      550     HTTP/1.1 404 Not Found  (te
```

```
▸ Frame 9093: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: LiteonTe_91:35:03 (9c:b7:0d:91:35:03), Dst: Routerbo_1e:0c:99 (cc:2d:e0:1e:0c:99)
▸ Internet Protocol Version 4, Src: 172.17.1.176, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 56046, Dst Port: 80, Seq: 1, Ack: 1, Len: 465
▾ Hypertext Transfer Protocol
  ▾ GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    ▸ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file2.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
```

```
0000  cc 2d e0 1e 0c 99 9c b7  0d 91 35 03 08 00 45 00   ·-······ ··5···E·
0010  02 05 a0 19 40 00 40 06  75 94 ac 11 01 b0 80 77   ····@·@· u······w
0020  f5 0c da ee 00 50 f1 54  ce 38 81 d5 6d 5f 80 18   ·····P·T ·8··m_··
0030  01 f6 4d f5 00 00 01 01  08 0a dd 43 4a cc f8 76   ··M····· ···CJ··v
0040  f9 93 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 32 2e 68 74 6d 6c 20   hark-fil e2.html 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
00b0  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
```

wireshark_wlp2s0_2022...8145940_wvBLYm.pcapng   Packets: 10908 · Displayed: 4 (0.0%) · Dropped: 0 (0.0%)   Profile: Default

.

First of all open the wireshark.

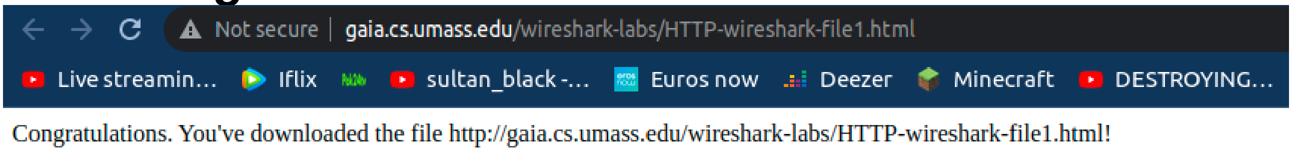
Opening The Link:

.

This is the link given in the manual, click on it and a web page will open in front of you.

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

Observing The Link:



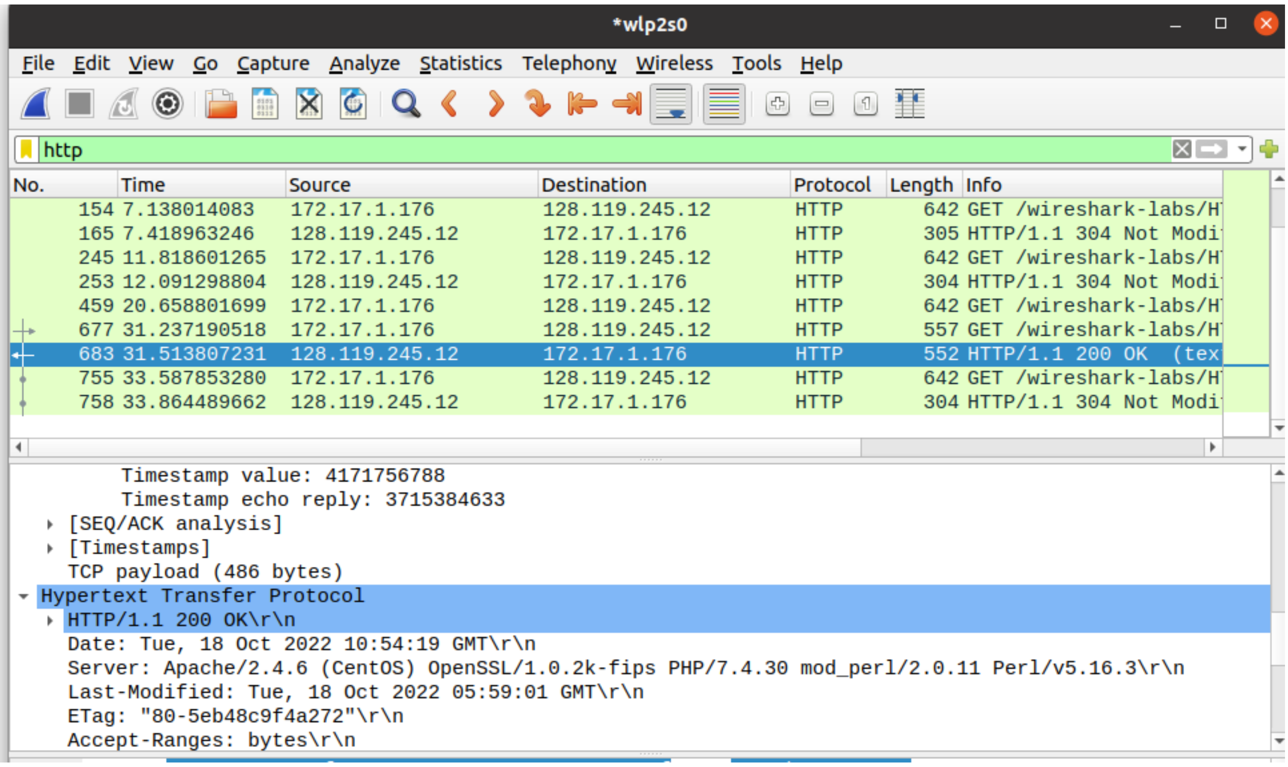
gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

.

Observing The Wireshark:

.



http

```
No.    Time          Source           Destination      Protocol  Length  Info
   154 7.138014083   172.17.1.176     128.119.245.12   HTTP          642 GET /wireshark-labs/H
   165 7.418963246   128.119.245.12   172.17.1.176     HTTP          305 HTTP/1.1 304 Not Modi
   245 11.818601265  172.17.1.176     128.119.245.12   HTTP          642 GET /wireshark-labs/H
   253 12.091298804  128.119.245.12   172.17.1.176     HTTP          304 HTTP/1.1 304 Not Modi
   459 20.658801699  172.17.1.176     128.119.245.12   HTTP          642 GET /wireshark-labs/H
   677 31.237190518  172.17.1.176     128.119.245.12   HTTP          557 GET /wireshark-labs/H
   683 31.513807231  128.119.245.12   172.17.1.176     HTTP          552 HTTP/1.1 200 OK  (tex
   755 33.587853280  172.17.1.176     128.119.245.12   HTTP          642 GET /wireshark-labs/H
   758 33.864489662  128.119.245.12   172.17.1.176     HTTP          304 HTTP/1.1 304 Not Modi
```

```
        Timestamp value: 4171756788
        Timestamp echo reply: 3715384633
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (486 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Tue, 18 Oct 2022 10:54:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 18 Oct 2022 05:59:01 GMT\r\n
    ETag: "80-5eb48c9f4a272"\r\n
    Accept-Ranges: bytes\r\n
```

.

.

.

.

This is the data being observed on the wireshark.
You can see, the the **200 OK** message in the info of the Wireshark. This is being observed after stoping the wireshark from the bottom Top corner.

Question 2:

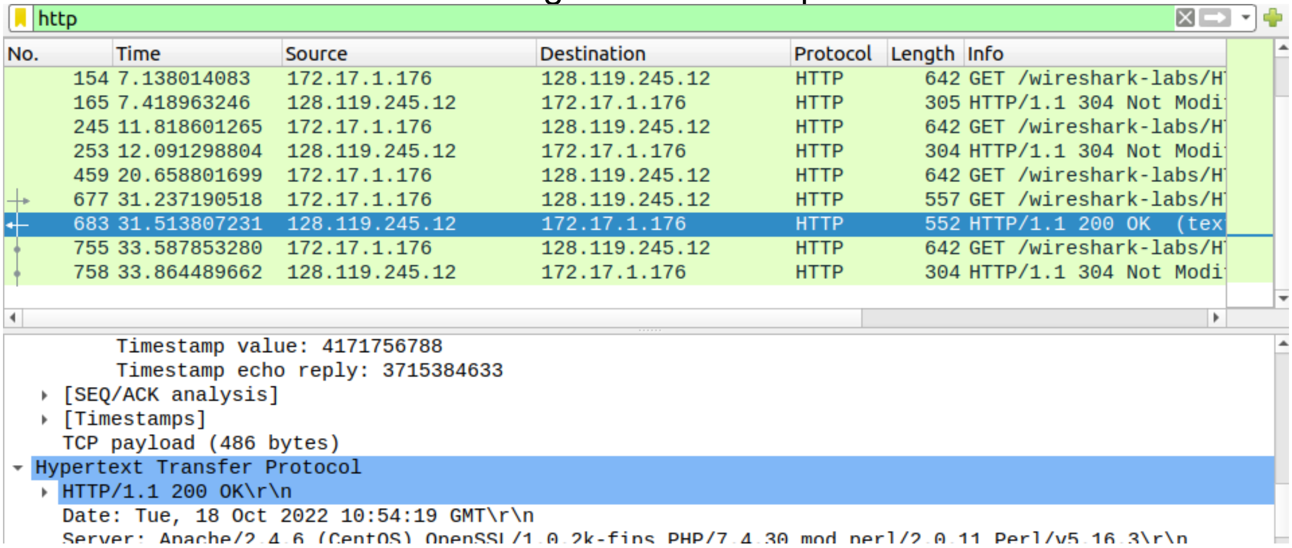
Part 1:

Answer:

Checking The Version Of The Browser Running The HTTP:

.

The version of the browser running the HTTP Request is 1.1



```
No.   Time            Source           Destination      Protocol  Length  Info
  154 7.138014083     172.17.1.176     128.119.245.12   HTTP         642 GET /wireshark-labs/H
  165 7.418963246     128.119.245.12   172.17.1.176     HTTP         305 HTTP/1.1 304 Not Modi
  245 11.818601265    172.17.1.176     128.119.245.12   HTTP         642 GET /wireshark-labs/H
  253 12.091298804    128.119.245.12   172.17.1.176     HTTP         304 HTTP/1.1 304 Not Modi
  459 20.658801699    172.17.1.176     128.119.245.12   HTTP         642 GET /wireshark-labs/H
  677 31.237190518    172.17.1.176     128.119.245.12   HTTP         557 GET /wireshark-labs/H
  683 31.513807231    128.119.245.12   172.17.1.176     HTTP         552 HTTP/1.1 200 OK  (tex
  755 33.587853280    172.17.1.176     128.119.245.12   HTTP         642 GET /wireshark-labs/H
  758 33.864489662    128.119.245.12   172.17.1.176     HTTP         304 HTTP/1.1 304 Not Modi
```

```
        Timestamp value: 4171756788
        Timestamp echo reply: 3715384633
  ▸ [SEQ/ACK analysis]
  ▸ [Timestamps]
    TCP payload (486 bytes)
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 18 Oct 2022 10:54:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
```

(HTTP/1.1).

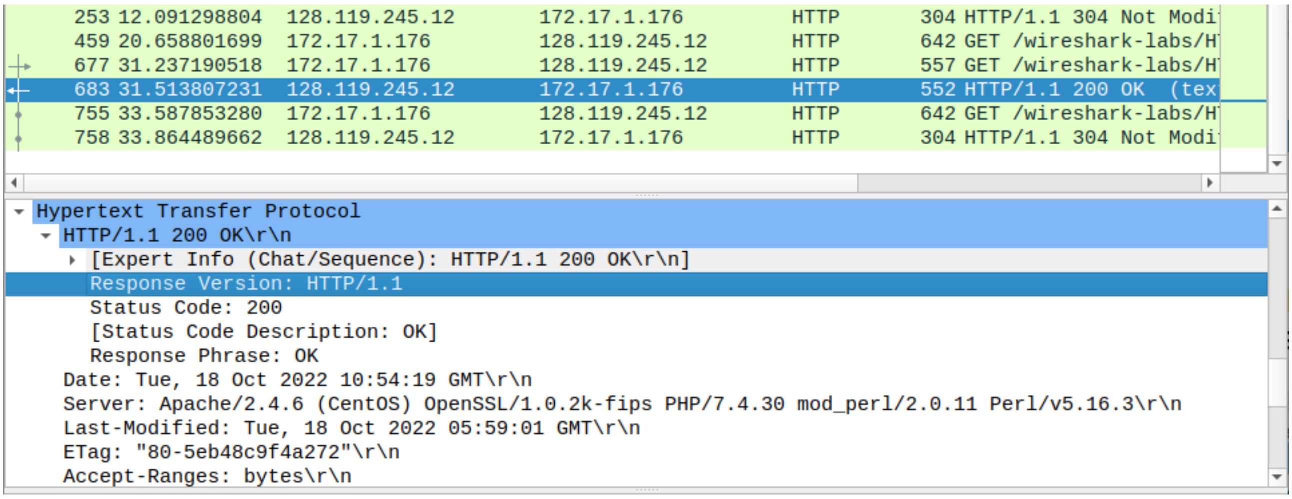
Part 2:

Answer:

Version Of The HTTP On Which Server Is Running:

The version of the HTTP on which the server is running is also HTTP/1.1 which is shown below.

.



```
  253 12.091298804    128.119.245.12   172.17.1.176     HTTP         304 HTTP/1.1 304 Not Modi
  459 20.658801699    172.17.1.176     128.119.245.12   HTTP         642 GET /wireshark-labs/H
  677 31.237190518    172.17.1.176     128.119.245.12   HTTP         557 GET /wireshark-labs/H
  683 31.513807231    128.119.245.12   172.17.1.176     HTTP         552 HTTP/1.1 200 OK  (tex
  755 33.587853280    172.17.1.176     128.119.245.12   HTTP         642 GET /wireshark-labs/H
  758 33.864489662    128.119.245.12   172.17.1.176     HTTP         304 HTTP/1.1 304 Not Modi
```

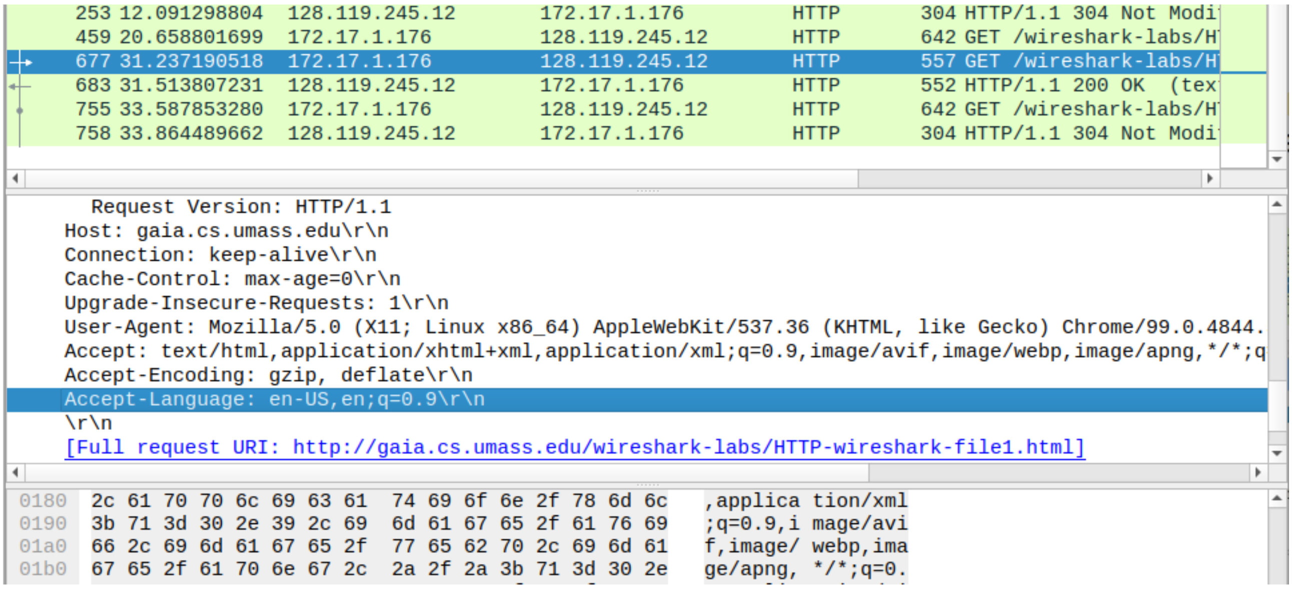
```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 18 Oct 2022 10:54:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 18 Oct 2022 05:59:01 GMT\r\n
    ETag: "80-5eb48c9f4a272"\r\n
    Accept-Ranges: bytes\r\n
```

.

Part 3:

Answer:

Language Indicated By The Browser:



```
253 12.091298804  128.119.245.12    172.17.1.176      HTTP      304 HTTP/1.1 304 Not Modi
459 20.658801699  172.17.1.176      128.119.245.12    HTTP      642 GET /wireshark-labs/H
677 31.237190518  172.17.1.176      128.119.245.12    HTTP      557 GET /wireshark-labs/H
683 31.513807231  128.119.245.12    172.17.1.176      HTTP      552 HTTP/1.1 200 OK  (tex
755 33.587853280  172.17.1.176      128.119.245.12    HTTP      642 GET /wireshark-labs/H
758 33.864489662  128.119.245.12    172.17.1.176      HTTP      304 HTTP/1.1 304 Not Modi
```

```
   Request Version: HTTP/1.1
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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
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]
```

```
0180  2c 61 70 70 6c 69 63 61  74 69 6f 6e 2f 78 6d 6c   ,applica tion/xml
0190  3b 71 3d 30 2e 39 2c 69  6d 61 67 65 2f 61 76 69   ;q=0.9,i mage/avi
01a0  66 2c 69 6d 61 67 65 2f  77 65 62 70 2c 69 6d 61   f,image/ webp,ima
01b0  67 65 2f 61 70 6e 67 2c  2a 2f 2a 3b 71 3d 30 2e   ge/apng, */*;q=0.
```

.

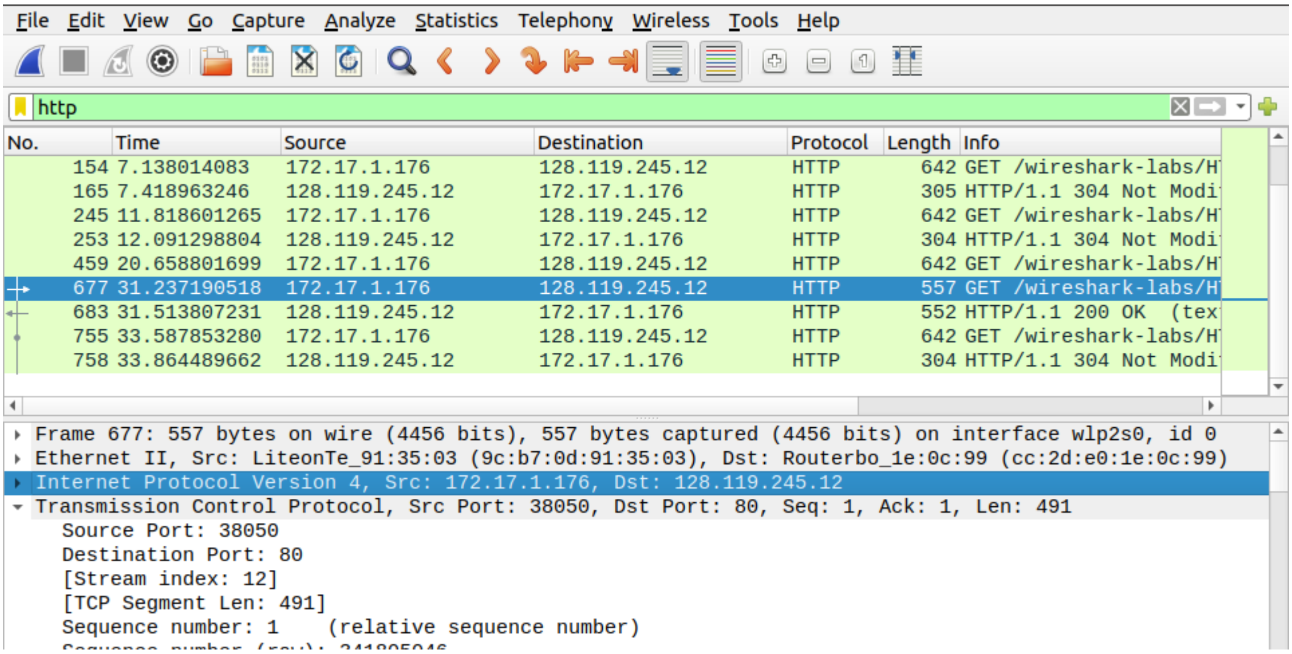
You can see the language indicated in the Accept Language.

Part 4:

Answer:

The IP Address of the server and IP Address of the computer are attached in the picture below.

They are represented as source and destination IP’s.


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

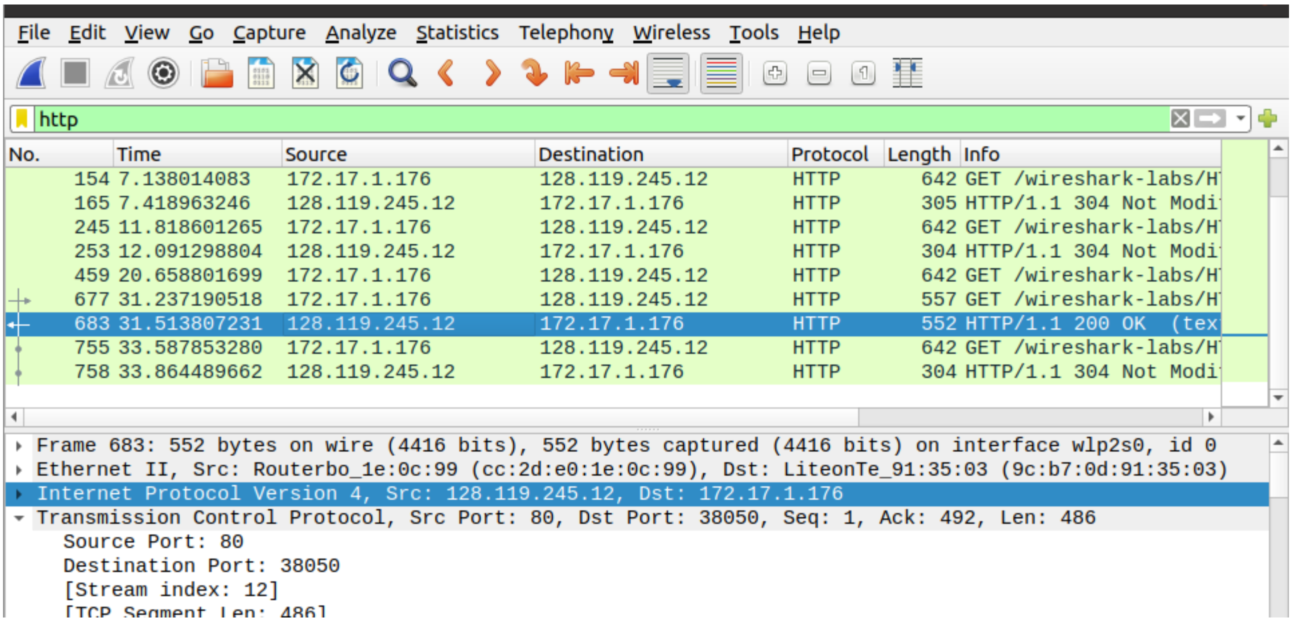
```
No.   Time          Source          Destination     Protocol Length Info
  154 7.138014083   172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  165 7.418963246   128.119.245.12  172.17.1.176    HTTP     305 HTTP/1.1 304 Not Modi
  245 11.818601265  172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  253 12.091298804  128.119.245.12  172.17.1.176    HTTP     304 HTTP/1.1 304 Not Modi
  459 20.658801699  172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  677 31.237190518  172.17.1.176    128.119.245.12  HTTP     557 GET /wireshark-labs/H
  683 31.513807231  128.119.245.12  172.17.1.176    HTTP     552 HTTP/1.1 200 OK  (tex
  755 33.587853280  172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  758 33.864489662  128.119.245.12  172.17.1.176    HTTP     304 HTTP/1.1 304 Not Modi
```

```
▸ Frame 677: 557 bytes on wire (4456 bits), 557 bytes captured (4456 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: LiteonTe_91:35:03 (9c:b7:0d:91:35:03), Dst: Routerbo_1e:0c:99 (cc:2d:e0:1e:0c:99)
▸ Internet Protocol Version 4, Src: 172.17.1.176, Dst: 128.119.245.12
▾ Transmission Control Protocol, Src Port: 38050, Dst Port: 80, Seq: 1, Ack: 1, Len: 491
    Source Port: 38050
    Destination Port: 80
    [Stream index: 12]
    [TCP Segment Len: 491]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 341805046
```

.

Part 5:
Answer:
Status Code Returned:

The browser will return a status code of “**200 OK**”.


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

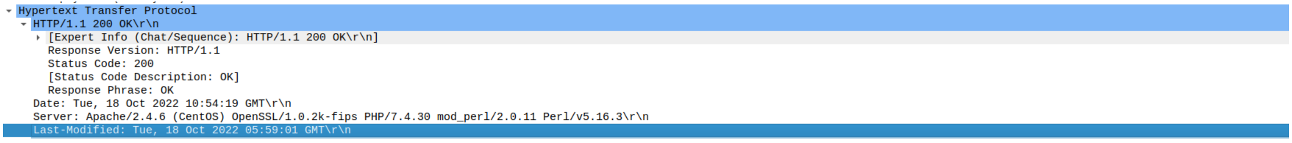
```
No.   Time          Source          Destination     Protocol Length Info
  154 7.138014083   172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  165 7.418963246   128.119.245.12  172.17.1.176    HTTP     305 HTTP/1.1 304 Not Modi
  245 11.818601265  172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  253 12.091298804  128.119.245.12  172.17.1.176    HTTP     304 HTTP/1.1 304 Not Modi
  459 20.658801699  172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  677 31.237190518  172.17.1.176    128.119.245.12  HTTP     557 GET /wireshark-labs/H
  683 31.513807231  128.119.245.12  172.17.1.176    HTTP     552 HTTP/1.1 200 OK  (tex
  755 33.587853280  172.17.1.176    128.119.245.12  HTTP     642 GET /wireshark-labs/H
  758 33.864489662  128.119.245.12  172.17.1.176    HTTP     304 HTTP/1.1 304 Not Modi
```

```
▸ Frame 683: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: Routerbo_1e:0c:99 (cc:2d:e0:1e:0c:99), Dst: LiteonTe_91:35:03 (9c:b7:0d:91:35:03)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.17.1.176
▾ Transmission Control Protocol, Src Port: 80, Dst Port: 38050, Seq: 1, Ack: 492, Len: 486
    Source Port: 80
    Destination Port: 38050
    [Stream index: 12]
    [TCP Segment Len: 486]
```

.

Part 6:
Answer:

The “**Last-Modified**” for the HTML file for the server is displayed in the picture below:



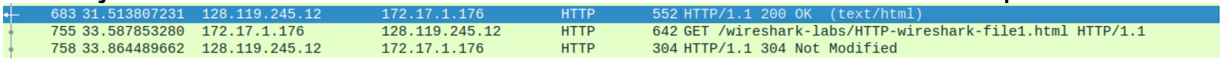
```
▾ Hypertext Transfer Protocol
  ▾ HTTP/1.1 200 OK\r\n
    ▸ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
      Response Version: HTTP/1.1
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
    Date: Tue, 18 Oct 2022 10:54:19 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 18 Oct 2022 05:59:01 GMT\r\n
```

.

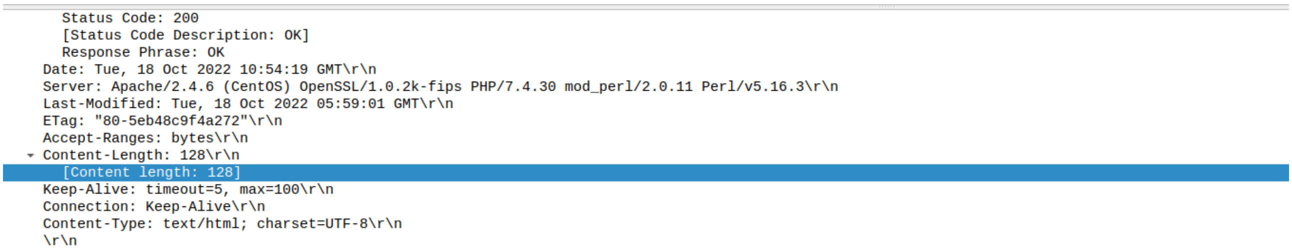
Part 7:

Answer:

The bytes of content returned to our browser are shown in the picture below.



```
683 31.513807231  128.119.245.12   172.17.1.176     HTTP    552 HTTP/1.1 200 OK  (text/html)
755 33.587853280  172.17.1.176     128.119.245.12   HTTP    642 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
758 33.864489662  128.119.245.12   172.17.1.176     HTTP    304 HTTP/1.1 304 Not Modified
```



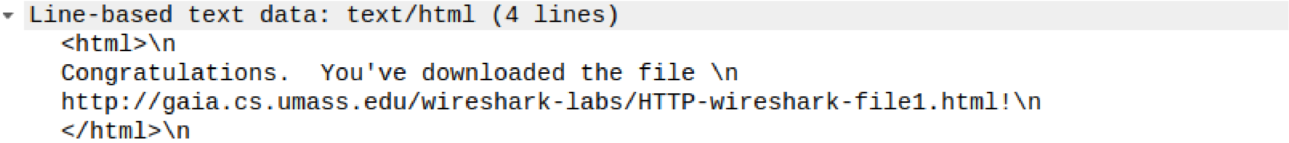
```
      Status Code: 200
      [Status Code Description: OK]
      Response Phrase: OK
   Date: Tue, 18 Oct 2022 10:54:19 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
   Last-Modified: Tue, 18 Oct 2022 05:59:01 GMT\r\n
   ETag: "80-5eb48c9f4a272"\r\n
   Accept-Ranges: bytes\r\n
 ▾ Content-Length: 128\r\n
      [Content length: 128]
   Keep-Alive: timeout=5, max=100\r\n
   Connection: Keep-Alive\r\n
   Content-Type: text/html; charset=UTF-8\r\n
   \r\n
```

.

Part 8:

Answer:

By inspecting the raw data in the packet content window, it is being observed that no all of the headers can be found in the raw data.



```
▾ Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

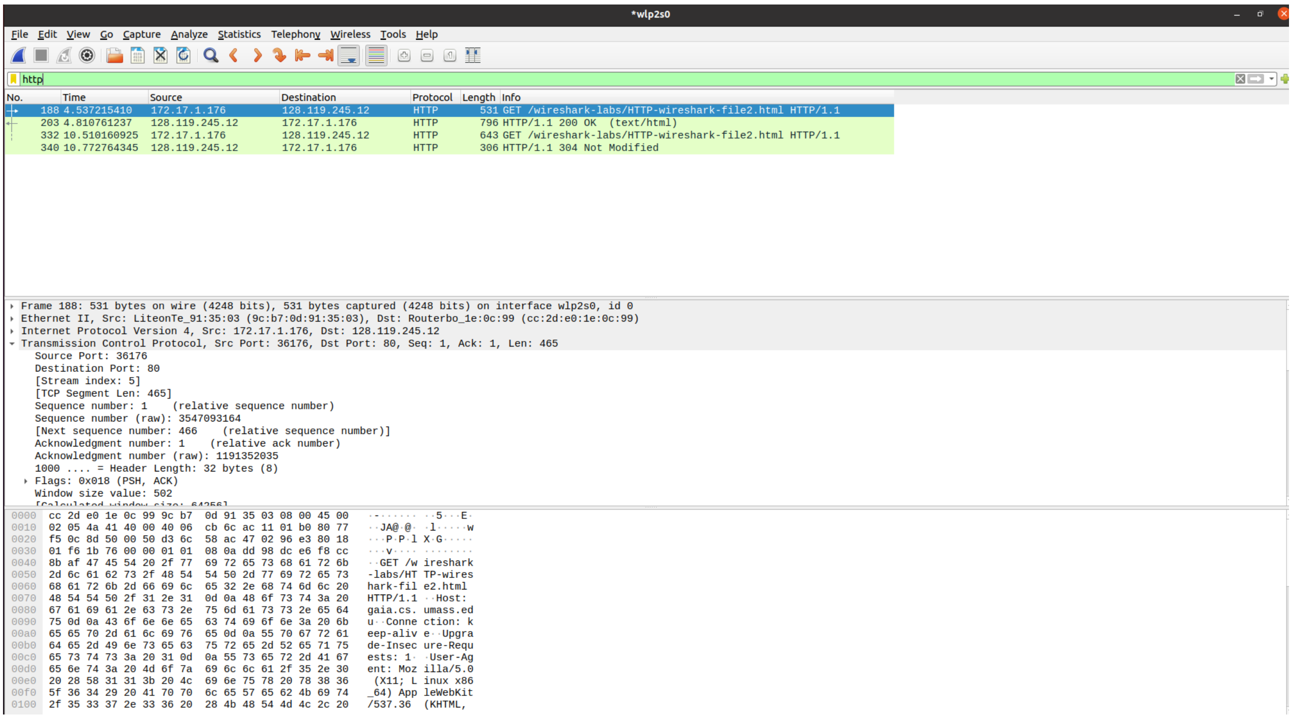
Question 3:

Part 1:

Answer:

We’ve inspected the contents of the first HTTP Get Request from our browser to the server. We’ve not seen any “**IF-Modified**” since we’ve observed the first line in the **HTTP Get.**

Demonstration From The Screenshot:



*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

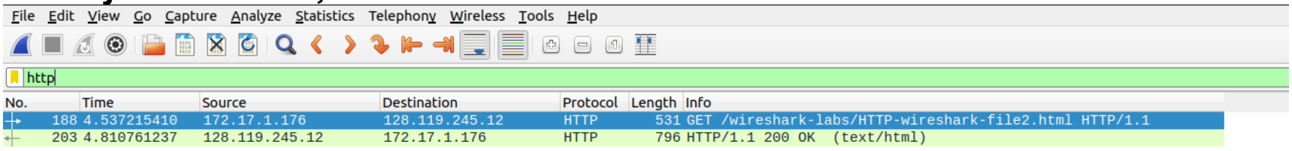
```
No.   Time         Source          Destination     Protocol  Length  Info
188   4.537215410  172.17.1.176    128.119.245.12  HTTP      531     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
203   4.810761237  128.119.245.12  172.17.1.176    HTTP      796     HTTP/1.1 200 OK  (text/html)
332   10.510160925 172.17.1.176    128.119.245.12  HTTP      643     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
340   10.772764345 128.119.245.12  172.17.1.176    HTTP      306     HTTP/1.1 304 Not Modified
```

```
▸ Frame 188: 531 bytes on wire (4248 bits), 531 bytes captured (4248 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: LiteonTe_91:35:03 (9c:b7:0d:91:35:03), Dst: Routerbo_1e:0c:99 (cc:2d:e0:1e:0c:99)
▸ Internet Protocol Version 4, Src: 172.17.1.176, Dst: 128.119.245.12
▾ Transmission Control Protocol, Src Port: 36176, Dst Port: 80, Seq: 1, Ack: 1, Len: 465
    Source Port: 36176
    Destination Port: 80
    [Stream index: 5]
    [TCP Segment Len: 465]
    Sequence number: 1    (relative sequence number)
    Sequence number (raw): 3547093164
    [Next sequence number: 466    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    Acknowledgment number (raw): 1191352035
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x018 (PSH, ACK)
    Window size value: 502
    [Calculated window size: 64256]
```

```
0000  cc 2d e0 1e 0c 99 9c b7  0d 91 35 03 08 00 45 00   ·-······ ··5···E·
0010  02 05 4a 41 40 00 40 06  cb 6c ac 11 01 b0 80 77   ··JA@·@· ·l·····w
0020  f5 0c 8d 50 00 50 d3 6c  58 ac 47 02 96 e3 80 18   ···P·P·l X·G·····
0030  01 f6 1b 76 00 00 01 01  08 0a dd 98 dc e6 f8 cc   ···v···· ········
0040  8b af 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ··GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 77 69 72 65 73   -labs/HT TP-wires
0060  68 61 72 6b 2d 66 69 6c  65 32 2e 68 74 6d 6c 20   hark-fil e2.html 
0070  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1 ··Host: 
0080  67 61 69 61 2e 63 73 2e  75 6d 61 73 73 2e 65 64   gaia.cs. umass.ed
0090  75 0d 0a 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   u··Conne ction: k
00a0  65 65 70 2d 61 6c 69 76  65 0d 0a 55 70 67 72 61   eep-aliv e··Upgra
00b0  64 65 2d 49 6e 73 65 63  75 72 65 2d 52 65 71 75   de-Insec ure-Requ
00c0  65 73 74 73 3a 20 31 0d  0a 55 73 65 72 2d 41 67   ests: 1· ·User-Ag
00d0  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00e0  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 78 38 36    (X11; L inux x86
00f0  5f 36 34 29 20 41 70 70  6c 65 57 65 62 4b 69 74   _64) App leWebKit
0100  2f 35 33 37 2e 33 36 20  28 4b 48 54 4d 4c 2c 20   /537.36  (KHTML, 
```

▪

Here you can see, no if-modified in the first line.



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

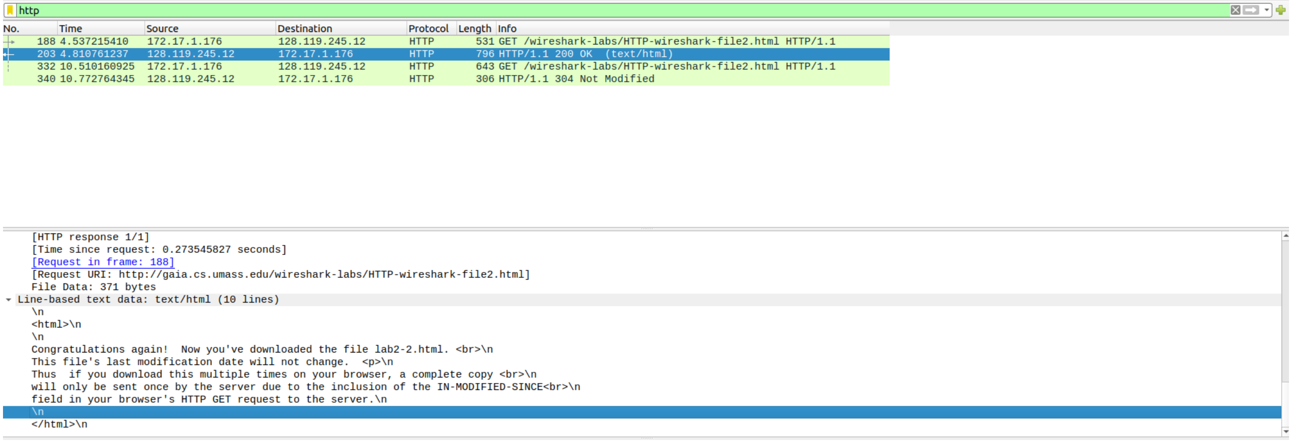
```
No.   Time         Source          Destination     Protocol  Length  Info
188   4.537215410  172.17.1.176    128.119.245.12  HTTP      531     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
203   4.810761237  128.119.245.12  172.17.1.176    HTTP      796     HTTP/1.1 200 OK  (text/html)
```

.

Part 2:

Answer:

Yes the server explicitly return the contents of the file. Here is the visual demonstration of the response in the picture below.



```
No.   Time         Source          Destination     Protocol  Length  Info
188   4.537215410  172.17.1.176    128.119.245.12  HTTP      531     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
203   4.810761237  128.119.245.12  172.17.1.176    HTTP      796     HTTP/1.1 200 OK  (text/html)
332   10.510160925 172.17.1.176    128.119.245.12  HTTP      643     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
340   10.772764345 128.119.245.12  172.17.1.176    HTTP      306     HTTP/1.1 304 Not Modified
```

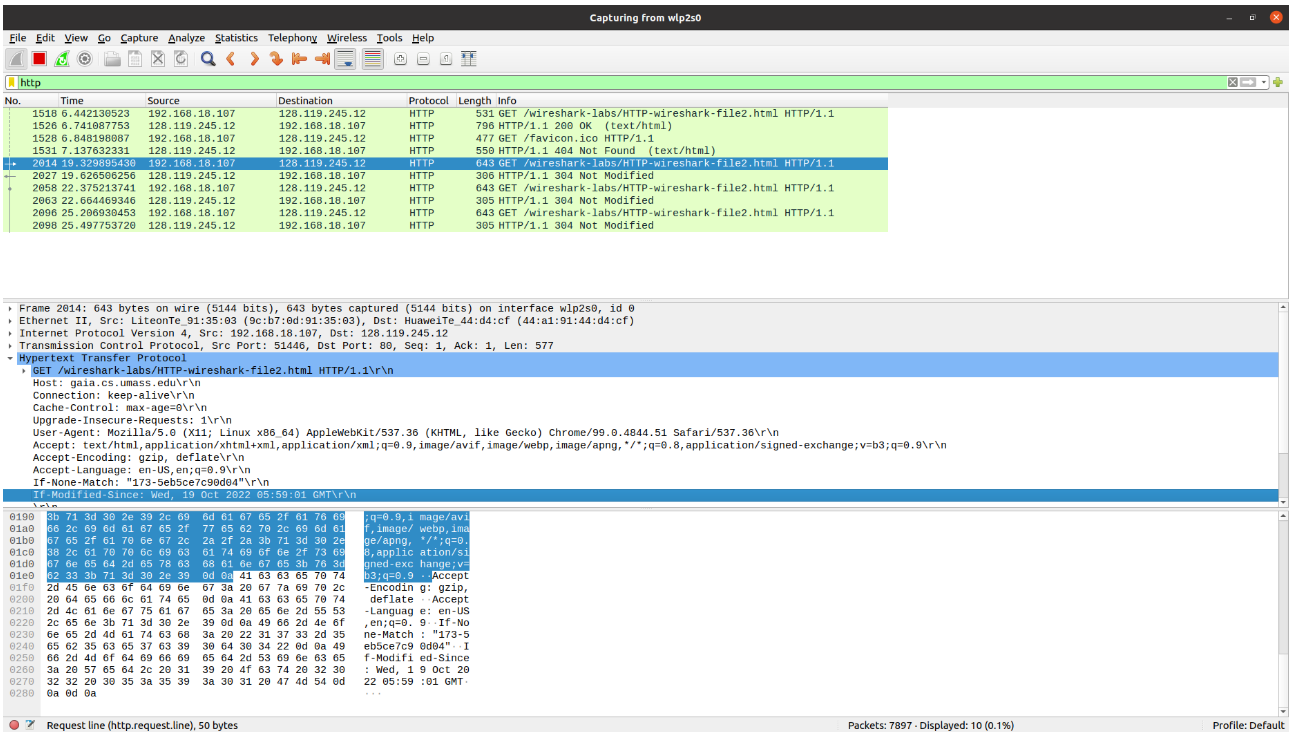
```
    [HTTP response 1/1]
    [Time since request: 0.273545827 seconds]
    [Request in frame: 188]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    File Data: 371 bytes
▾ Line-based text data: text/html (10 lines)
    \n
    <html>\n
    \n
    Congratulations again!  Now you've downloaded the file lab2-2.html. <br>\n
    This file's last modification date will not change.  <p>\n
    Thus  if you download this multiple times on your browser, a complete copy <br>\n
    will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
    field in your browser's HTTP GET request to the server.\n
    \n
    </html>\n
```

.

Part 3:

Answer:

Yes, we've observed the "IF-Modified-Since" in the HTTP GET6 as mentioned in the picture below.


Capturing from wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http
No.      Time          Source           Destination      Protocol  Length Info
    1518 6.442130523   192.168.18.107   128.119.245.12   HTTP       531 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    1526 6.741087753   128.119.245.12   192.168.18.107   HTTP       796 HTTP/1.1 200 OK  (text/html)
    1528 6.848198087   192.168.18.107   128.119.245.12   HTTP       477 GET /favicon.ico HTTP/1.1
    1531 7.137632331   128.119.245.12   192.168.18.107   HTTP       550 HTTP/1.1 404 Not Found  (text/html)
    2014 19.329895430  192.168.18.107   128.119.245.12   HTTP       643 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    2027 19.626506256  128.119.245.12   192.168.18.107   HTTP       306 HTTP/1.1 304 Not Modified
    2058 22.375213741  192.168.18.107   128.119.245.12   HTTP       643 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    2063 22.664469346  128.119.245.12   192.168.18.107   HTTP       305 HTTP/1.1 304 Not Modified
    2096 25.206930453  192.168.18.107   128.119.245.12   HTTP       643 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
    2098 25.497753720  128.119.245.12   192.168.18.107   HTTP       305 HTTP/1.1 304 Not Modified
```

```
› Frame 2014: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface wlp2s0, id 0
› Ethernet II, Src: LiteonTe_91:35:03 (9c:b7:0d:91:35:03), Dst: HuaweiTe_44:d4:cf (44:a1:91:44:d4:cf)
› Internet Protocol Version 4, Src: 192.168.18.107, Dst: 128.119.245.12
› Transmission Control Protocol, Src Port: 51446, Dst Port: 80, Seq: 1, Ack: 1, Len: 577
⌄ 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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-5eb5ce7c90d04"\r\n
    If-Modified-Since: Wed, 19 Oct 2022 05:59:01 GMT\r\n
```

```
0190  3b 71 3d 30 2e 39 2c 69  6d 61 67 65 2f 61 76 69   ;q=0.9,i mage/avi
01a0  66 2c 69 6d 61 67 65 2f  77 65 62 70 2c 69 6d 61   f,image/ webp,ima
01b0  67 65 2f 61 70 6e 67 2c  2a 2f 2a 3b 71 3d 30 2e   ge/apng, */*;q=0.
01c0  38 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f 73 69   8,applic ation/si
01d0  67 6e 65 64 2d 65 78 63  68 61 6e 67 65 3b 76 3d   gned-exc hange;v=
01e0  62 33 3b 71 3d 30 2e 39  0d 0a 41 63 63 65 70 74   b3;q=0.9 ··Accept
01f0  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0200  20 64 65 66 6c 61 74 65  0d 0a 41 63 63 65 70 74    deflate ··Accept
0210  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
0220  2c 65 6e 3b 71 3d 30 2e  39 0d 0a 49 66 2d 4e 6f   ,en;q=0. 9··If-No
0230  6e 65 2d 4d 61 74 63 68  3a 20 22 31 37 33 2d 35   ne-Match : "173-5
0240  65 62 35 63 65 37 63 39  30 64 30 34 22 0d 0a 49   eb5ce7c9 0d04"··I
0250  66 2d 4d 6f 64 69 66 69  65 64 2d 53 69 6e 63 65   f-Modifi ed-Since
0260  3a 20 57 65 64 2c 20 31  39 20 4f 63 74 20 32 30   : Wed, 1 9 Oct 20
0270  32 32 20 30 35 3a 35 39  3a 30 31 20 47 4d 54 0d   22 05:59 :01 GMT·
0280  0a 0d 0a                                           ···
```

Request line (http.request.line), 50 bytes · Packets: 7897 · Displayed: 10 (0.1%) · Profile: Default

▪

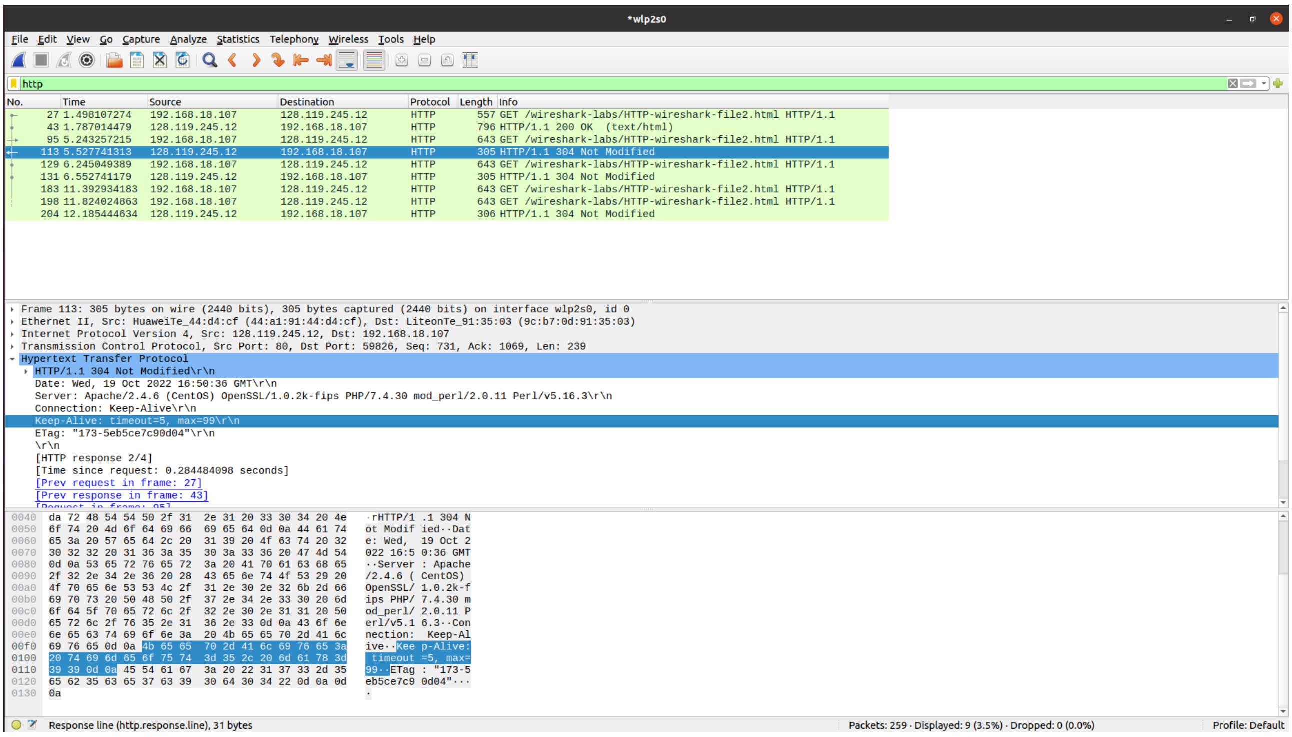
Part 4:

Answer:

Reasoning:

The browser did not return the contents of the file explicitly. This is because the browser is retrieving its contents from its cache. The file has been modified since it was last accessed, therefore it is simply showing to retrieve the old file from the cache memory.

Visual Demonstration:


*wlp2s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http

No.   Time          Source           Destination      Protocol Length Info
   27 1.498107274   192.168.18.107   128.119.245.12   HTTP     557 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   43 1.787014479   128.119.245.12   192.168.18.107   HTTP     796 HTTP/1.1 200 OK  (text/html)
   95 5.243257215   192.168.18.107   128.119.245.12   HTTP     643 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  113 5.527741313   128.119.245.12   192.168.18.107   HTTP     305 HTTP/1.1 304 Not Modified
  129 6.245049389   192.168.18.107   128.119.245.12   HTTP     643 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  131 6.552741179   128.119.245.12   192.168.18.107   HTTP     305 HTTP/1.1 304 Not Modified
  183 11.392934183  192.168.18.107   128.119.245.12   HTTP     643 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  198 11.824024863  192.168.18.107   128.119.245.12   HTTP     643 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  204 12.185444634  128.119.245.12   192.168.18.107   HTTP     306 HTTP/1.1 304 Not Modified
```

```
› Frame 113: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface wlp2s0, id 0
› Ethernet II, Src: HuaweiTe_44:d4:cf (44:a1:91:44:d4:cf), Dst: LiteonTe_91:35:03 (9c:b7:0d:91:35:03)
› Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.18.107
› Transmission Control Protocol, Src Port: 80, Dst Port: 59826, Seq: 731, Ack: 1069, Len: 239
⌄ Hypertext Transfer Protocol
  › HTTP/1.1 304 Not Modified\r\n
    Date: Wed, 19 Oct 2022 16:50:36 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=99\r\n
    ETag: "173-5eb5ce7c90d04"\r\n
    \r\n
    [HTTP response 2/4]
    [Time since request: 0.284484098 seconds]
    [Prev request in frame: 27]
    [Prev response in frame: 43]
    [Request in frame: 95]
```

```
0040  da 72 48 54 54 50 2f 31  2e 31 20 33 30 34 20 4e   ·rHTTP/1 .1 304 N
0050  6f 74 20 4d 6f 64 69 66  69 65 64 0d 0a 44 61 74   ot Modif ied··Dat
0060  65 3a 20 57 65 64 2c 20  31 39 20 4f 63 74 20 32   e: Wed,  19 Oct 2
0070  30 32 32 20 31 36 3a 35  30 3a 33 36 20 47 4d 54   022 16:5 0:36 GMT
0080  0d 0a 53 65 72 76 65 72  3a 20 41 70 61 63 68 65   ··Server : Apache
0090  2f 32 2e 34 2e 36 20 28  43 65 6e 74 4f 53 29 20   /2.4.6 ( CentOS)
00a0  4f 70 65 6e 53 53 4c 2f  31 2e 30 2e 32 6b 2d 66   OpenSSL/ 1.0.2k-f
00b0  69 70 73 20 50 48 50 2f  37 2e 34 2e 33 30 20 6d   ips PHP/ 7.4.30 m
00c0  6f 64 5f 70 65 72 6c 2f  32 2e 30 2e 31 31 20 50   od_perl/ 2.0.11 P
00d0  65 72 6c 2f 76 35 2e 31  36 2e 33 0d 0a 43 6f 6e   erl/v5.1 6.3··Con
00e0  6e 65 63 74 69 6f 6e 3a  20 4b 65 65 70 2d 41 6c   nection:  Keep-Al
00f0  69 76 65 0d 0a 4b 65 65  70 2d 41 6c 69 76 65 3a   ive··Kee p-Alive:
0100  20 74 69 6d 65 6f 75 74  3d 35 2c 20 6d 61 78 3d    timeout =5, max=
0110  39 39 0d 0a 45 54 61 67  3a 20 22 31 37 33 2d 35   99··ETag : "173-5
0120  65 62 35 63 65 37 63 39  30 64 30 34 22 0d 0a 0d   eb5ce7c9 0d04"···
0130  0a                                                 ·
```

```
Response line (http.response.line), 31 bytes      Packets: 259 · Displayed: 9 (3.5%) · Dropped: 0 (0.0%)      Profile: Default
```

.

This can be observed by having a look at the, **“ETag:” and “Keep-Alive”** Data.