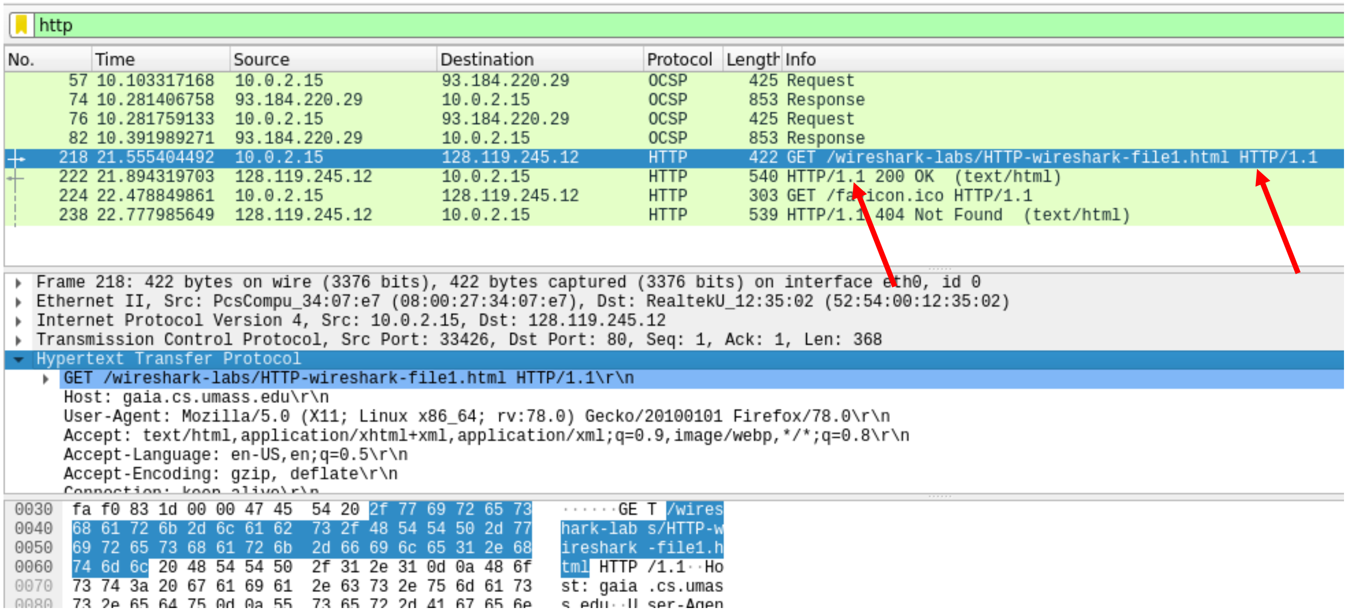
Rosemary Agbozo – Cyber Security

PRACTICAL ACTIVITY WEEK 6-WIRESHARK

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

   Both are running HTTP 1.1 version as seen in the screenshot below.



```
http
```

```
No.    Time         Source          Destination     Protocol Length Info
    57 10.103317168 10.0.2.15       93.184.220.29   OCSP       425 Request
    74 10.281406758 93.184.220.29   10.0.2.15       OCSP       853 Response
    76 10.281759133 10.0.2.15       93.184.220.29   OCSP       425 Request
    82 10.391989271 93.184.220.29   10.0.2.15       OCSP       853 Response
   218 21.555404492 10.0.2.15       128.119.245.12  HTTP       422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   222 21.894319703 128.119.245.12  10.0.2.15       HTTP       540 HTTP/1.1 200 OK  (text/html)
   224 22.478849861 10.0.2.15       128.119.245.12  HTTP       303 GET /favicon.ico HTTP/1.1
   238 22.777985649 128.119.245.12  10.0.2.15       HTTP       539 HTTP/1.1 404 Not Found  (text/html)
```

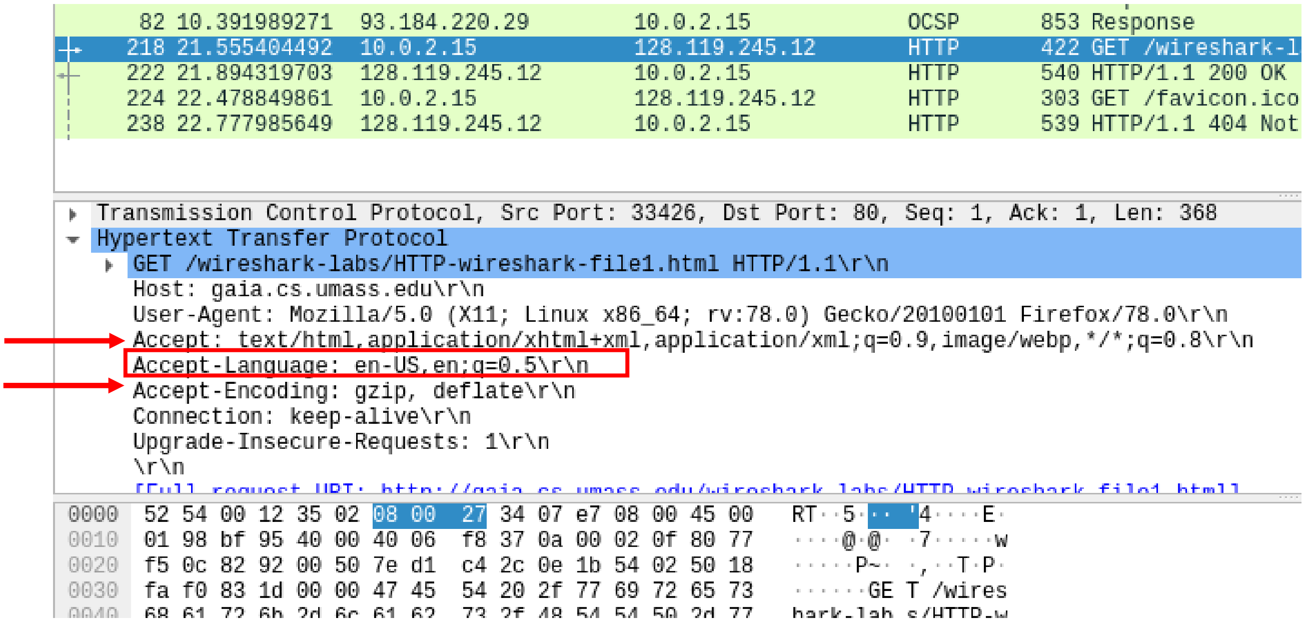
```
▸ Frame 218: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_34:07:e7 (08:00:27:34:07:e7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 33426, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
```

```
0030  fa f0 83 1d 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 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
```

2. What languages (if any) does your browser indicate that it can accept to the server? In the captured session, what other information (if any) does the browser provide the server with regarding the user/browser?

   The language is en-US (US English) and can be seen at the Accept-language part, under the dropdown of the ‘Hypertext Transfer protocol’ in the GET request.

   Other information the browser provides is the Accept (showing what it accepts) and the accept-encoding -gzip, deflate- (showing what encoding scheme it accepts).



```
 82 10.391989271   93.184.220.29     10.0.2.15         OCSP     853 Response
218 21.555404492   10.0.2.15         128.119.245.12    HTTP     422 GET /wireshark-l
222 21.894319703   128.119.245.12    10.0.2.15         HTTP     540 HTTP/1.1 200 OK
224 22.478849861   10.0.2.15         128.119.245.12    HTTP     303 GET /favicon.ico
238 22.777985649   128.119.245.12    10.0.2.15         HTTP     539 HTTP/1.1 404 Not
```

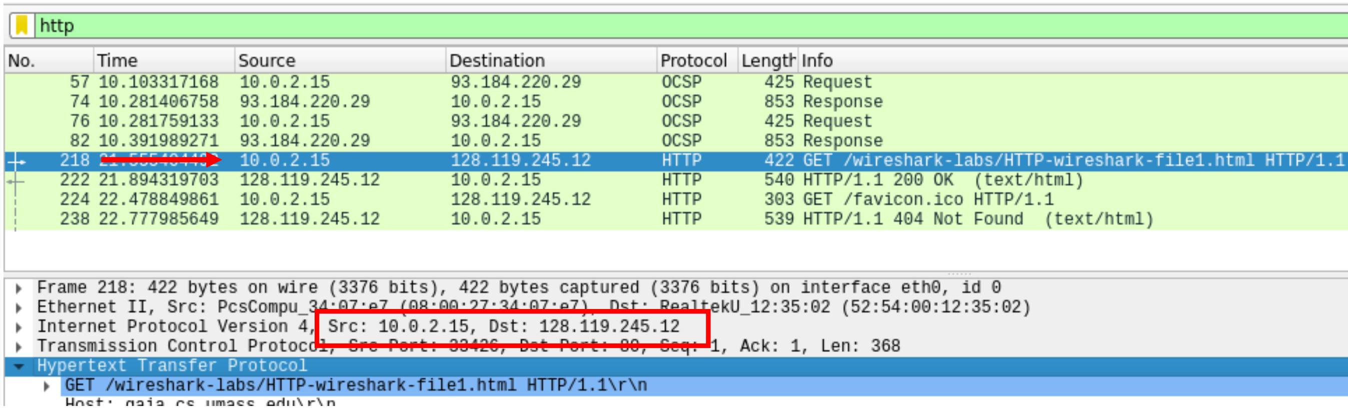
```
▸ Transmission Control Protocol, Src Port: 33426, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

```
0000  52 54 00 12 35 02 08 00  27 34 07 e7 08 00 45 00   RT··5···'4····E·
0010  01 98 bf 95 40 00 40 06  f8 37 0a 00 02 0f 80 77   ····@·@··7·····w
0020  f5 0c 82 92 00 50 7e d1  c4 2c 0e 1b 54 02 50 18   ·····P~··,··T·P·
0030  fa f0 83 1d 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
```

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

   IP of computer: **10.0.2.15** is source address of the GET request.

   IP of gaia.cs.umass.edu server: **128.119.245.12** is the destination address of the GET request.

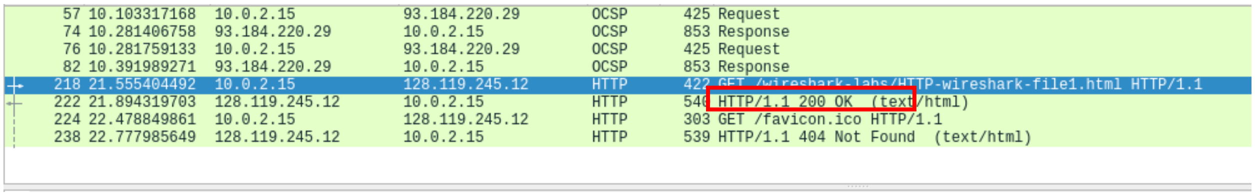


```
No.   Time           Source           Destination      Protocol Length Info
   57 10.103317168   10.0.2.15        93.184.220.29    OCSP     425 Request
   74 10.281406758   93.184.220.29    10.0.2.15        OCSP     853 Response
   76 10.281759133   10.0.2.15        93.184.220.29    OCSP     425 Request
   82 10.391989271   93.184.220.29    10.0.2.15        OCSP     853 Response
  218 21.555404492   10.0.2.15        128.119.245.12   HTTP     422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  222 21.894319703   128.119.245.12   10.0.2.15        HTTP     540 HTTP/1.1 200 OK  (text/html)
  224 22.478849861   10.0.2.15        128.119.245.12   HTTP     303 GET /favicon.ico HTTP/1.1
  238 22.777985649   128.119.245.12   10.0.2.15        HTTP     539 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Frame 218: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_34:07:e7 (08:00:27:34:07:e7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 33426, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
▾ Hypertext Transfer Protocol
  ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
```

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

   Information from the server is recorded in the response message. The status code is **200 OK** – which means request was successful.

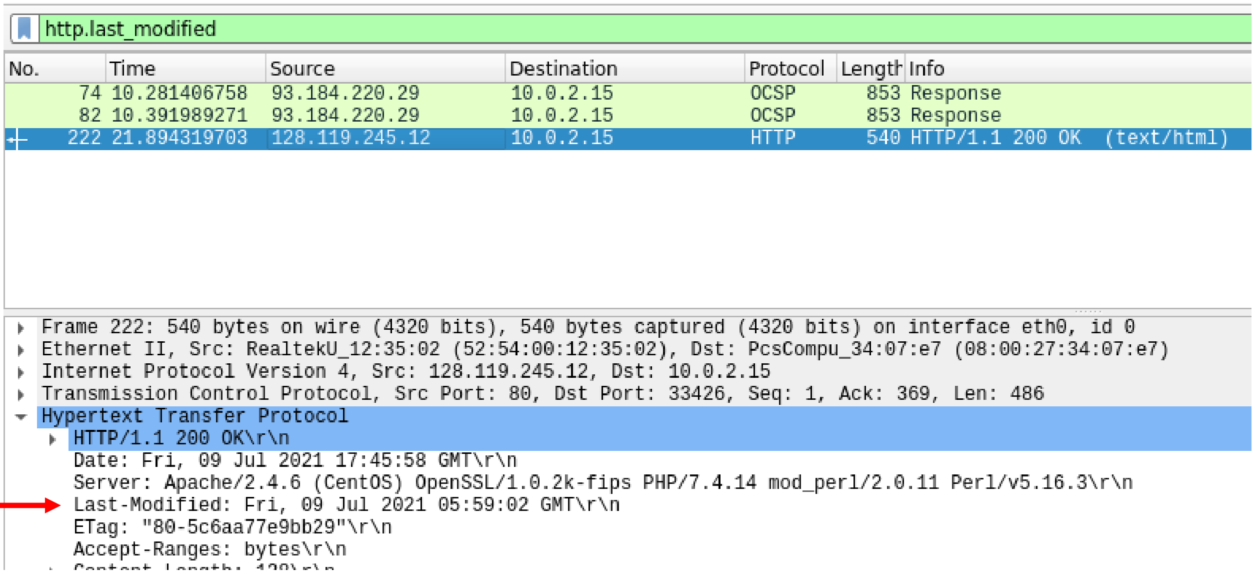


```
     57 10.103317168  10.0.2.15        93.184.220.29    OCSP     425 Request
     74 10.281406758  93.184.220.29    10.0.2.15        OCSP     853 Response
     76 10.281759133  10.0.2.15        93.184.220.29    OCSP     425 Request
     82 10.391989271  93.184.220.29    10.0.2.15        OCSP     853 Response
    218 21.555404492  10.0.2.15        128.119.245.12   HTTP     422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
    222 21.894319703  128.119.245.12   10.0.2.15        HTTP     540 HTTP/1.1 200 OK  (text/html)
    224 22.478849861  10.0.2.15        128.119.245.12   HTTP     303 GET /favicon.ico HTTP/1.1
    238 22.777985649  128.119.245.12   10.0.2.15        HTTP     539 HTTP/1.1 404 Not Found  (text/html)
```

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

   To get the last modified, I filtered the messages by **http.last_modified** and got the last modified date in the HTTP response field.

   The date was **Fri, 09 Jul 2021 at 05:59:02 GMT.**



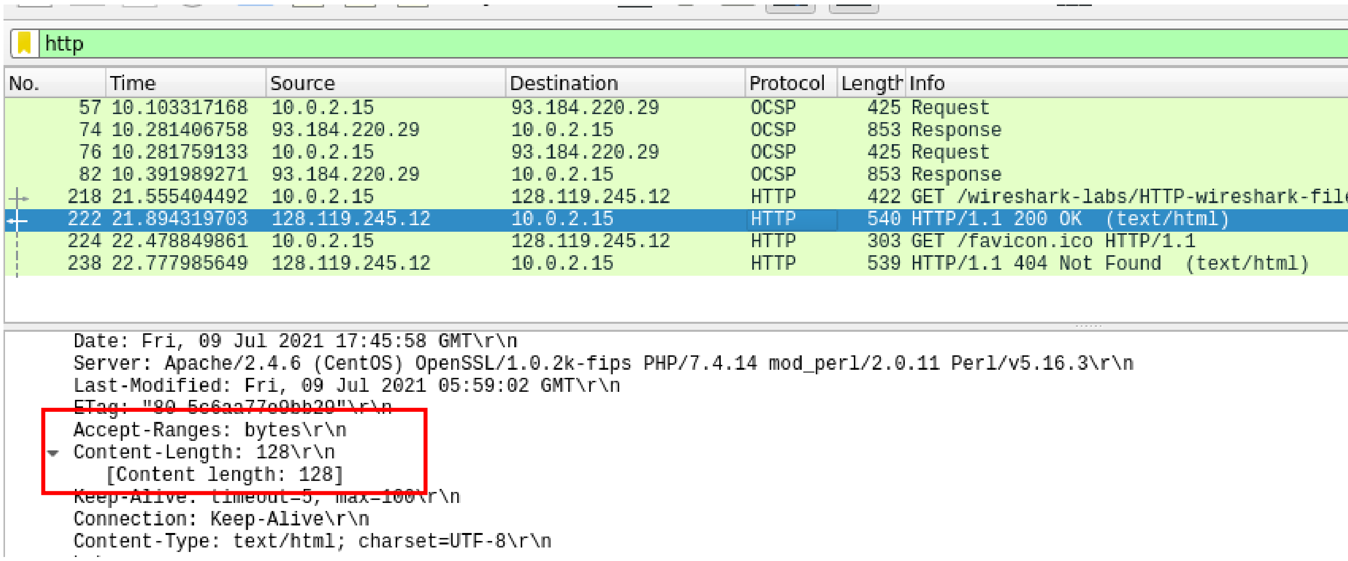
```
http.last_modified

No.    Time          Source           Destination   Protocol  Length Info
    74 10.281406758  93.184.220.29    10.0.2.15     OCSP         853 Response
    82 10.391989271  93.184.220.29    10.0.2.15     OCSP         853 Response
   222 21.894319703  128.119.245.12   10.0.2.15     HTTP         540 HTTP/1.1 200 OK  (text/html)

Frame 222: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface eth0, id 0
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_34:07:e7 (08:00:27:34:07:e7)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 80, Dst Port: 33426, Seq: 1, Ack: 369, Len: 486
Hypertext Transfer Protocol
   HTTP/1.1 200 OK\r\n
   Date: Fri, 09 Jul 2021 17:45:58 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
   Last-Modified: Fri, 09 Jul 2021 05:59:02 GMT\r\n
   ETag: "80-5c6aa77e9bb29"\r\n
   Accept-Ranges: bytes\r\n
```

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

   This is also known from the http response. Content length in bytes are **128 bytes**



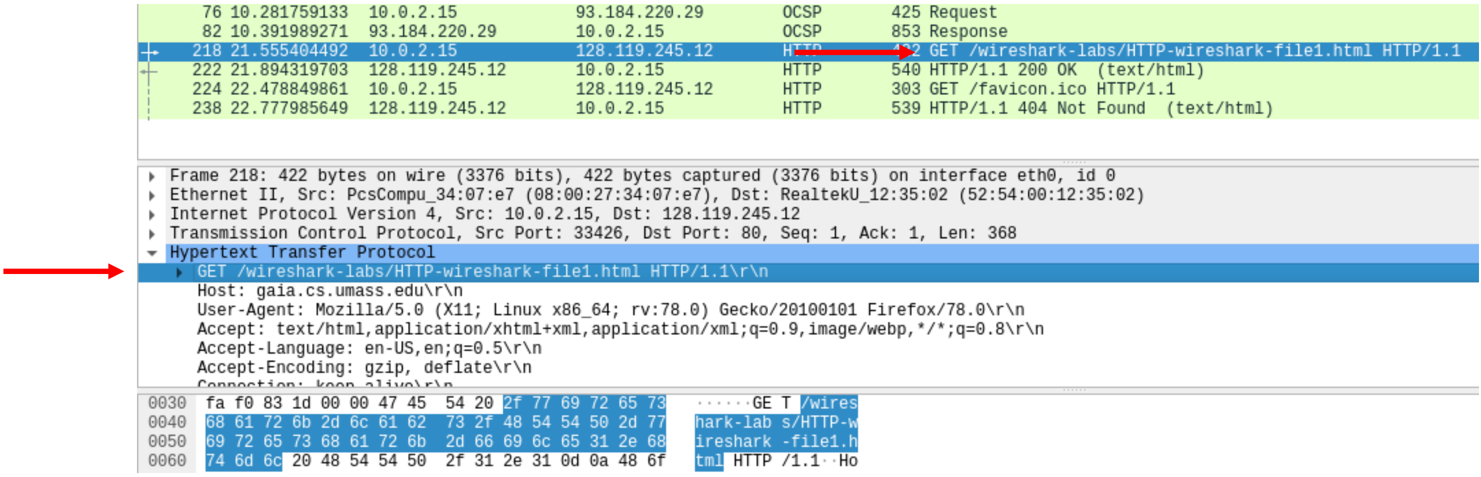
```
http
```

```
No.    Time          Source           Destination      Protocol  Length Info
    57 10.103317168  10.0.2.15        93.184.220.29    OCSP      425 Request
    74 10.281406758  93.184.220.29    10.0.2.15        OCSP      853 Response
    76 10.281759133  10.0.2.15        93.184.220.29    OCSP      425 Request
    82 10.391989271  93.184.220.29    10.0.2.15        OCSP      853 Response
   218 21.555404492  10.0.2.15        128.119.245.12   HTTP      422 GET /wireshark-labs/HTTP-wireshark-fil
   222 21.894319703  128.119.245.12   10.0.2.15        HTTP      540 HTTP/1.1 200 OK  (text/html)
   224 22.478849861  10.0.2.15        128.119.245.12   HTTP      303 GET /favicon.ico HTTP/1.1
   238 22.777985649  128.119.245.12   10.0.2.15        HTTP      539 HTTP/1.1 404 Not Found  (text/html)
```

```
      Date: Fri, 09 Jul 2021 17:45:58 GMT\r\n
      Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Fri, 09 Jul 2021 05:59:02 GMT\r\n
      ETag: "80-5c6aa77e9bb29"\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
```

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

   The http headers in the raw data match with what is displayed in the packet-listing window.



```
    76 10.281759133  10.0.2.15        93.184.220.29    OCSP      425 Request
    82 10.391989271  93.184.220.29    10.0.2.15        OCSP      853 Response
   218 21.555404492  10.0.2.15        128.119.245.12   HTTP      422 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
   222 21.894319703  128.119.245.12   10.0.2.15        HTTP      540 HTTP/1.1 200 OK  (text/html)
   224 22.478849861  10.0.2.15        128.119.245.12   HTTP      303 GET /favicon.ico HTTP/1.1
   238 22.777985649  128.119.245.12   10.0.2.15        HTTP      539 HTTP/1.1 404 Not Found  (text/html)
```

```
▸ Frame 218: 422 bytes on wire (3376 bits), 422 bytes captured (3376 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_34:07:e7 (08:00:27:34:07:e7), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 33426, Dst Port: 80, Seq: 1, Ack: 1, Len: 368
▾ Hypertext Transfer Protocol
   ▸ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
     Host: gaia.cs.umass.edu\r\n
     User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
     Accept-Language: en-US,en;q=0.5\r\n
     Accept-Encoding: gzip, deflate\r\n
     Connection: keep-alive\r\n
```

```
0030  fa f0 83 1d 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
```

SUMMARY

All the information in the packet-listing window is present in the packet-content window. The packet-content window contains even more details.

In the HTTP GET request, the browser gives its specifications to the server, so the server knows exactly what to return. Like the language (english) to respond in, the encoding it accepts, and many others as seen in question 2.

Another observation I made was that, in the GET request packet-content window, the frame containing the response was stated. Also, in the response, the frame number of the GET request was stated, this makes navigation easier.

Using filters like in question 5 makes sampling easier. When you filter messages, you easily located exactly what you need. One can filter http/https, http.last_modified, and many others.

IP address details can be obtained from the IP version 4 part in the packet-content panel, or even directly from the packet-listing widow. One can get the source IP and destination IP easily.