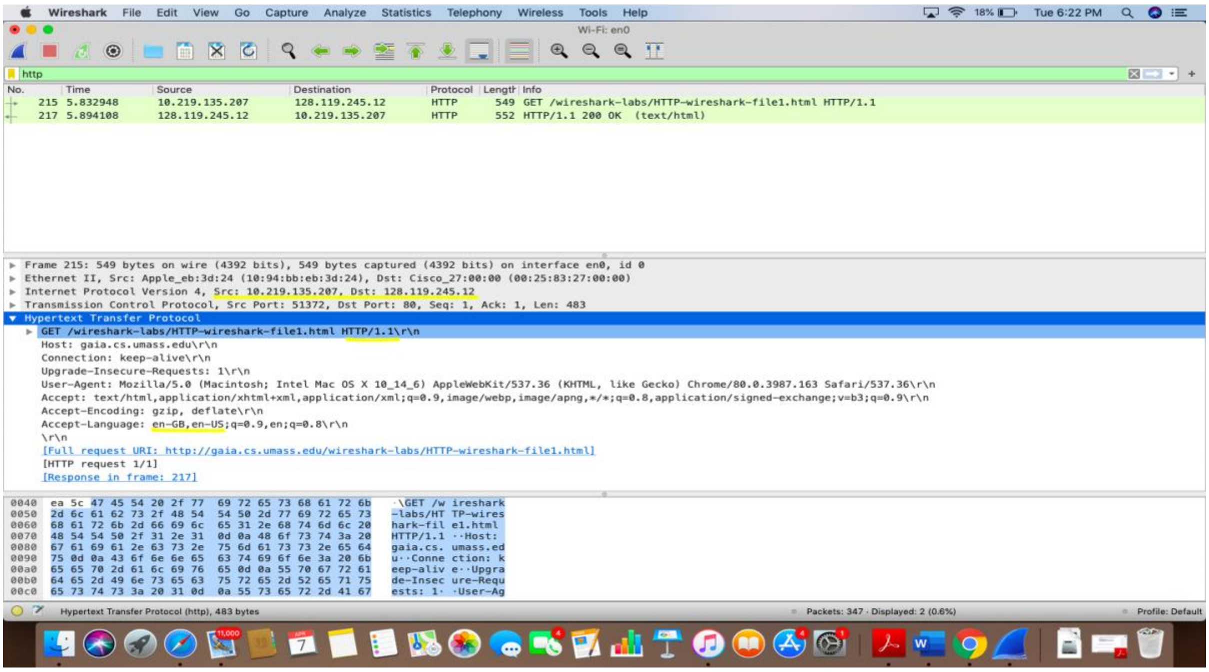
NAME: SHITIZ KUMAR AGGARWAL **UTA ID:** 1001669578

ASSIGNMENT NO.2



http

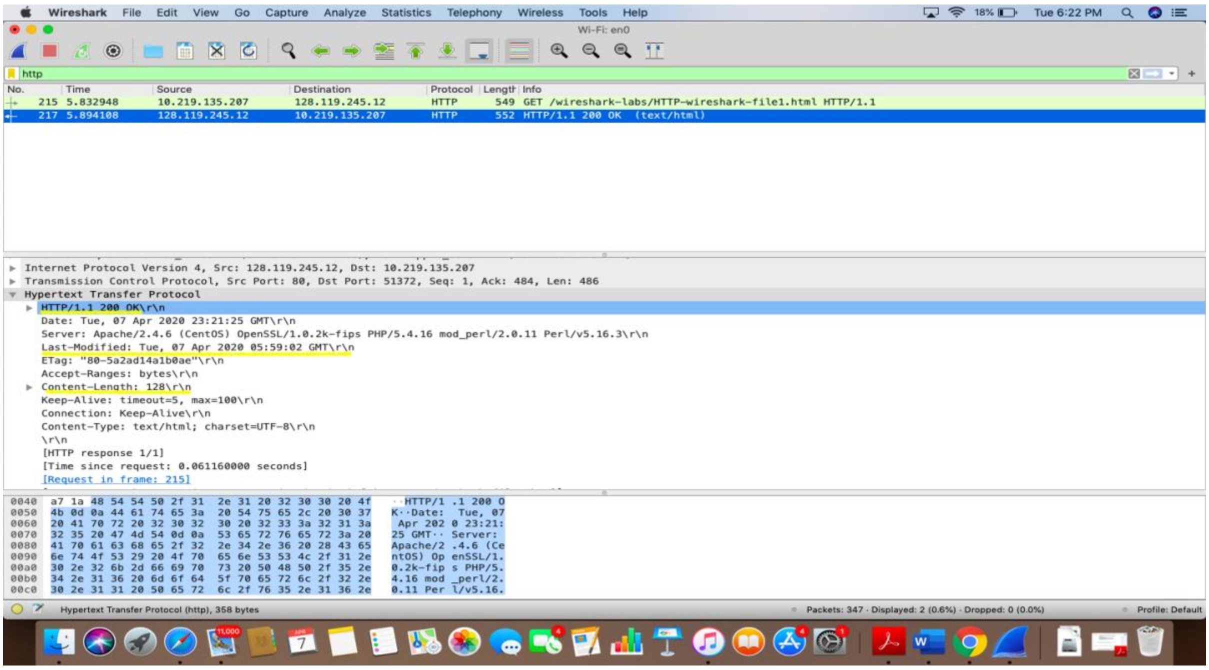
```
No.   Time      Source           Destination      Protocol Length Info
  215 5.832948  10.219.135.207   128.119.245.12   HTTP      549  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  217 5.894108  128.119.245.12   10.219.135.207   HTTP      552  HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 215: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface en0, id 0
▸ Ethernet II, Src: Apple_eb:3d:24 (10:94:bb:eb:3d:24), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
▸ Internet Protocol Version 4, Src: 10.219.135.207, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 51372, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
▾ 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 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 217]
```

```
0040  ea 5c 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 31 2e 68 74 6d 6c 20   hark-fil e1.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
```

Hypertext Transfer Protocol (http), 483 bytes · Packets: 347 · Displayed: 2 (0.6%) · Profile: Default

(Screenshot-1)



http

```
No.   Time      Source           Destination      Protocol Length Info
  215 5.832948  10.219.135.207   128.119.245.12   HTTP      549  GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
  217 5.894108  128.119.245.12   10.219.135.207   HTTP      552  HTTP/1.1 200 OK  (text/html)
```

```
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.135.207
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 51372, Seq: 1, Ack: 484, Len: 486
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 07 Apr 2020 23:21:25 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 07 Apr 2020 05:59:02 GMT\r\n
    ETag: "80-5a2ad14a1b0ae"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.061160000 seconds]
    [Request in frame: 215]
```

```
0040  a7 1a 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ··HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 54 75 65 2c 20 30 37   K··Date:  Tue, 07
0060  20 41 70 72 20 32 30 32  30 20 32 33 3a 32 31 3a    Apr 202 0 23:21:
0070  32 35 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   25 GMT·· Server:
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 20 28 43 65   Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-fip s PHP/5.
00b0  34 2e 31 36 20 6d 6f 64  5f 70 65 72 6c 2f 32 2e   4.16 mod _perl/2.
00c0  30 2e 31 31 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.11 Per l/v5.16.
```

Hypertext Transfer Protocol (http), 358 bytes · Packets: 347 · Displayed: 2 (0.6%) · Dropped: 0 (0.0%) · Profile: Default

(Screenshot-2)

ANSWER NO.1

From Screenshot-1 it is clear that both browser and server are running HTTP version 1.1.

ANSWER NO.2

From Screenshot-1 we get to know what languages our browser can accept to the Server:
Accept Language: en-GB, en-US.

ANSWER NO.3

IP address of Computer: 10.219.135.207
IP address of gaia.cs.umass.edu server: 128.119.245.12

ANSWER NO.4

Status code returned from the server to browser is:
HTTP/1.1 200 OK\r\n (From Screenshot-2)

ANSWER NO.5

From the Screenshot-2 we can see when was the file last modified at the server:
Last-Modified: Tue, 07 Apr 2020 05:59:02 GMT.

ANSWER NO.6

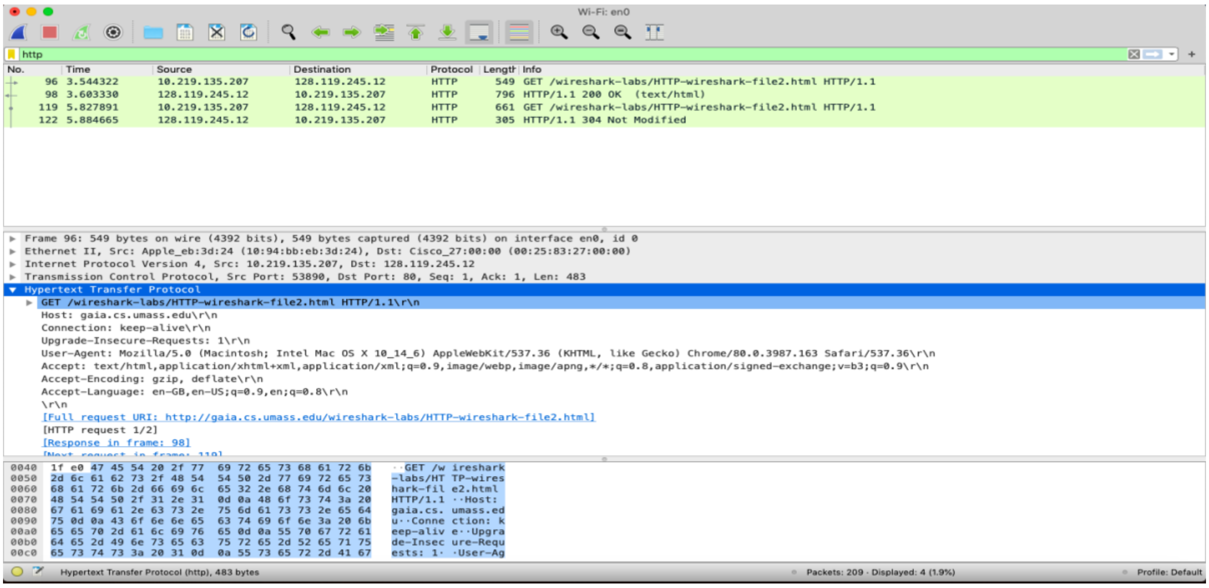
From the Screenshot-2 we can see:
Content-Length : 128

ANSWER NO.7

No, all the headers can be found in the raw data.

ANSWER NO.8

No, not present as it can be observed from the Screenshot-3 below:



```
No.  Time      Source          Destination     Protocol Length Info
  96 3.544322  10.219.135.207  128.119.245.12  HTTP     549 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  98 3.603330  128.119.245.12  10.219.135.207  HTTP     796 HTTP/1.1 200 OK  (text/html)
 119 5.827891  10.219.135.207  128.119.245.12  HTTP     661 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 122 5.884665  128.119.245.12  10.219.135.207  HTTP     305 HTTP/1.1 304 Not Modified
```

```
▶ Frame 96: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_eb:3d:24 (10:94:bb:eb:3d:24), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
▶ Internet Protocol Version 4, Src: 10.219.135.207, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 53890, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
▼ 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/2]
    [Response in frame: 98]
    [Next request in frame: 119]
```

```
0040  1f e0 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
```

Hypertext Transfer Protocol (http), 483 bytes

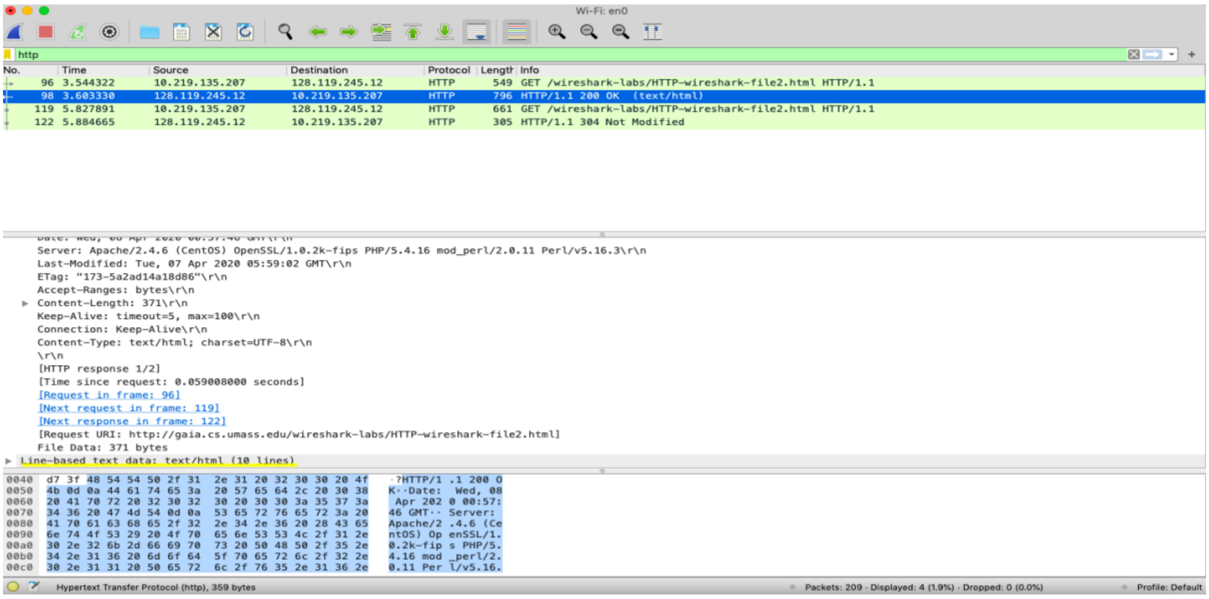
Packets: 209 · Displayed: 4 (1.9%)

Profile: Default

(Screenshot-3)

ANSWER NO.9

Yes, as it can be clearly seen from the Screenshot-4 below that server has returned the contents of the file as it is present in “Line-based text data” field.



```
No.  Time      Source          Destination     Protocol Length Info
  96 3.544322  10.219.135.207  128.119.245.12  HTTP     549 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  98 3.603330  128.119.245.12  10.219.135.207  HTTP     796 HTTP/1.1 200 OK  (text/html)
 119 5.827891  10.219.135.207  128.119.245.12  HTTP     661 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
 122 5.884665  128.119.245.12  10.219.135.207  HTTP     305 HTTP/1.1 304 Not Modified
```

```
    Date: Wed, 08 Apr 2020 00:57:46 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 07 Apr 2020 05:59:02 GMT\r\n
    ETag: "173-5a2ad14a18d86"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 371\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: 0.059008000 seconds]
    [Request in frame: 96]
    [Next request in frame: 119]
    [Next response in frame: 122]
    [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)
```

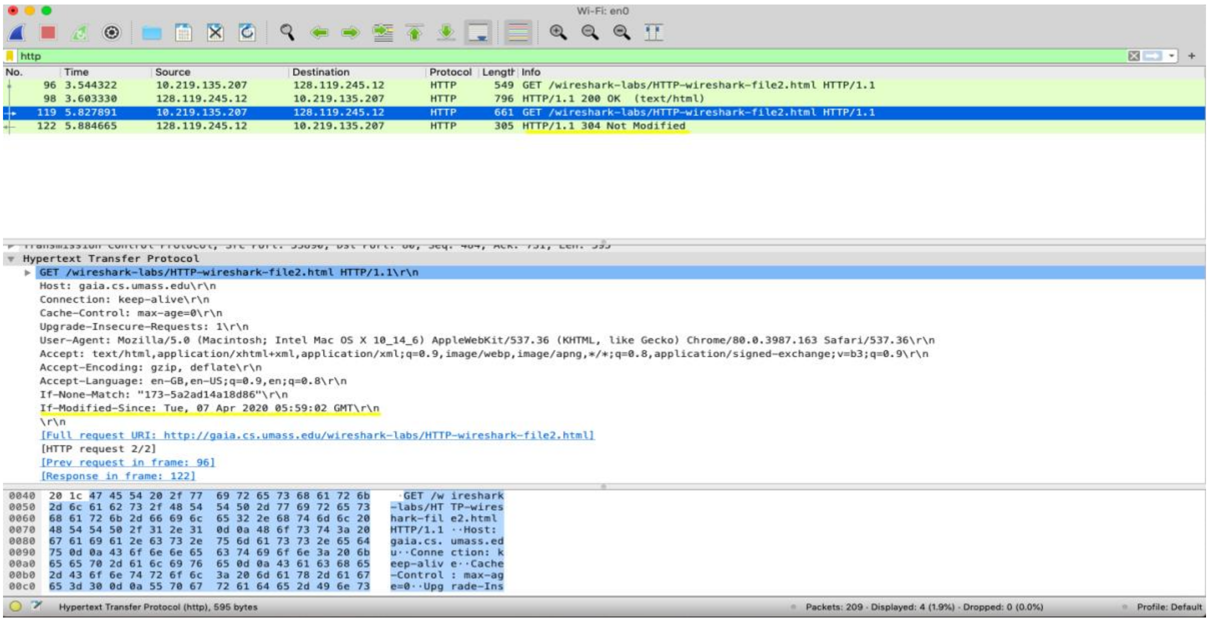
```
0040  d7 3f 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   ·?HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 57 65 64 2c 20 30 38   K··Date:  Wed, 08
0060  20 41 70 72 20 32 30 32  30 20 30 30 3a 35 37 3a    Apr 202 0 00:57:
0070  34 36 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   46 GMT·· Server: 
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 20 28 43 65   Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-fip s PHP/5.
00b0  34 2e 31 36 20 6d 6f 64  5f 70 65 72 6c 2f 32 2e   4.16 mod _perl/2.
00c0  30 2e 31 31 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.11 Per l/v5.16.
```

Hypertext Transfer Protocol (http), 359 bytes

Packets: 209 · Displayed: 4 (1.9%) · Dropped: 0 (0.0%)

Profile: Default

(Screenshot-4)



```
http
```

```
No.     Time        Source            Destination       Protocol  Length  Info
   96   3.544322    10.219.135.207    128.119.245.12    HTTP      549     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
   98   3.603330    128.119.245.12    10.219.135.207    HTTP      796     HTTP/1.1 200 OK  (text/html)
  119   5.827891    10.219.135.207    128.119.245.12    HTTP      661     GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  122   5.884665    128.119.245.12    10.219.135.207    HTTP      305     HTTP/1.1 304 Not Modified
```

```
▸ Transmission Control Protocol, Src Port: 55890, Dst Port: 80, Seq: 484, Ack: 731, Len: 595
▾ 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 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    If-None-Match: "173-5a2ad14a18d86"\r\n
    If-Modified-Since: Tue, 07 Apr 2020 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 2/2]
    [Prev request in frame: 96]
    [Response in frame: 122]
```

```
0040  20 1c 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 43 61 63 68 65   eep-aliv e··Cache
00b0  2d 43 6f 6e 74 72 6f 6c  3a 20 6d 61 78 2d 61 67   -Control : max-ag
00c0  65 3d 30 0d 0a 55 70 67  72 61 64 65 2d 49 6e 73   e=0··Upg rade-Ins
```

```
Hypertext Transfer Protocol (http), 595 bytes    Packets: 209 · Displayed: 4 (1.9%) · Dropped: 0 (0.0%)    Profile: Default
```

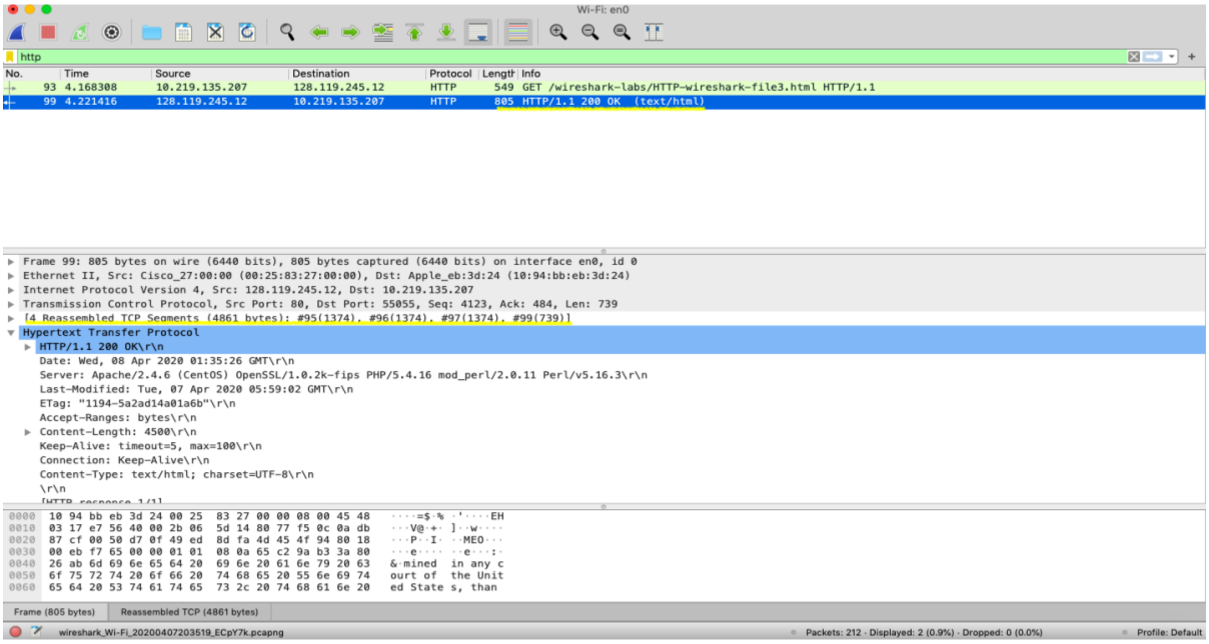
(Screenshot-5)

ANSWER NO.10

Yes, as it can be seen from Screenshot-5 above:
If-Modified-Since: Tue, 07 Apr 2020 05:59:02 GMT.

ANSWER NO.11

The HTTP status code and phrase returned from the server in response to this second HTTP Get is: 304 Not Modified. (as can be seen from Screenshot-5)
The server does not explicitly return the contents of the file as it is already stored in cache.



```
No.    Time        Source           Destination      Protocol Length Info
   93  4.168308    10.219.135.207   128.119.245.12   HTTP      549  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
   99  4.221416    128.119.245.12   10.219.135.207   HTTP      805  HTTP/1.1 200 OK  (text/html)
```

```
▶ Frame 99: 805 bytes on wire (6440 bits), 805 bytes captured (6440 bits) on interface en0, id 0
▶ Ethernet II, Src: Cisco_27:00:00 (00:25:83:27:00:00), Dst: Apple_eb:3d:24 (10:94:bb:eb:3d:24)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.135.207
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 55055, Seq: 4123, Ack: 484, Len: 739
▶ [4 Reassembled TCP Segments (4861 bytes): #95(1374), #96(1374), #97(1374), #99(739)]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Wed, 08 Apr 2020 01:35:26 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Tue, 07 Apr 2020 05:59:02 GMT\r\n
    ETag: "1194-5a2ad14a01a6b"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 4500\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
```

```
0000  10 94 bb eb 3d 24 00 25  83 27 00 00 08 00 45 48   ····=$·% ·'····EH
0010  03 17 e7 56 40 00 2b 06  5d 14 80 77 f5 0c 0a db   ···V@·+· ]··w····
0020  87 cf 00 50 d7 0f 49 ed  8d fa 4d 45 4f 94 80 18   ···P··I· ··MEO···
0030  00 eb f7 65 00 00 01 01  08 0a 65 c2 9a b3 3a 80   ···e···· ··e···:·
0040  26 ab 6d 69 6e 65 64 20  69 6e 20 61 6e 79 20 63   &·mined  in any c
0050  6f 75 72 74 20 6f 66 20  74 68 65 20 55 6e 69 74   ourt of  the Unit
0060  65 64 20 53 74 61 74 65  73 2c 20 74 68 61 6e 20   ed State s, than
```

Frame (805 bytes)   Reassembled TCP (4861 bytes)

wireshark_Wi-Fi_20200407203519_ECpY7k.pcapng   Packets: 212 · Displayed: 2 (0.9%) · Dropped: 0 (0.0%)   Profile: Default

(Screenshot-6)

ANSWER NO.12

My browser send one HTTP GET request message. Packet number 93 in the trace contains the GET message as it can be seen from the Screenshot-6.

ANSWER NO.13

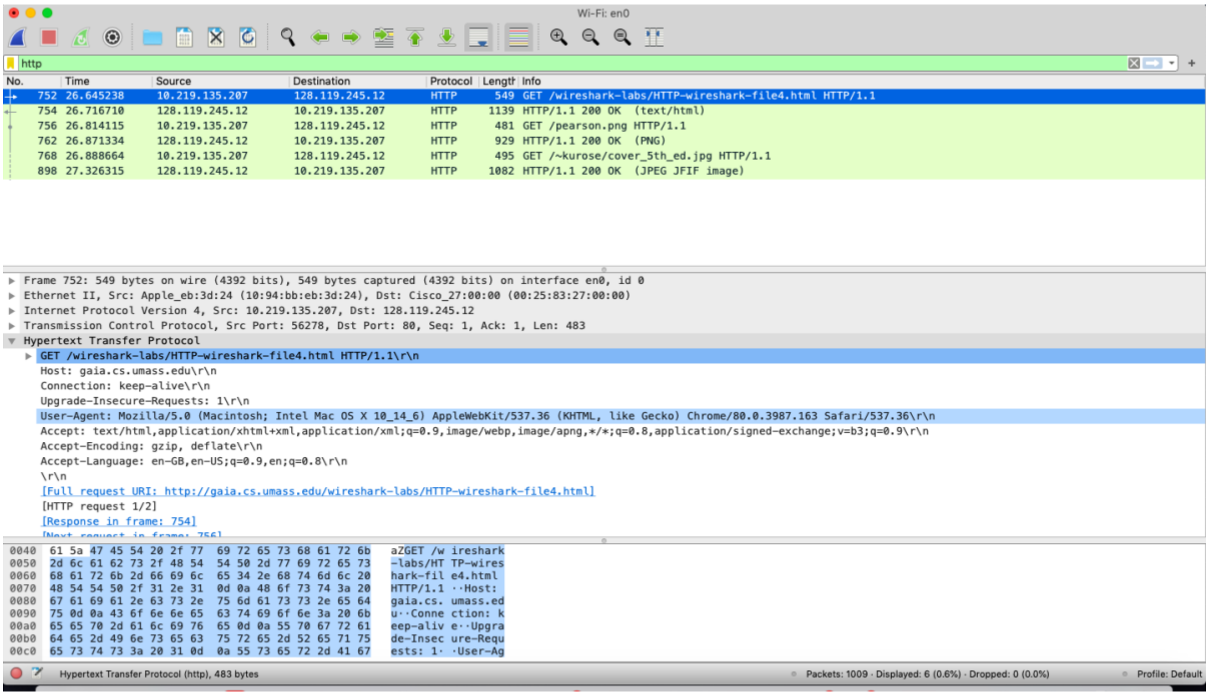
Packet Number 99 in the trace contains the status code and phrase associated with the response as it can be seen from Screenshot-6 above.

ANSWER NO.14

As it can be seen from the Screenshot-6 above the status code and phrase in the response is: 200 OK.

ANSWER NO.15

As it can be seen from the Screenshot-6 above that 4 Reassembled TCP Segments (4861 bytes): #95(1374), #96(1374), #97(1374), #99(739) were needed to carry the single HTTP response and the text of the Bill of Rights.



```
http
```

No.	Time	Source	Destination	Protocol	Length	Info
752	26.645238	10.219.135.207	128.119.245.12	HTTP	549	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
754	26.716710	128.119.245.12	10.219.135.207	HTTP	1139	HTTP/1.1 200 OK (text/html)
756	26.814115	10.219.135.207	128.119.245.12	HTTP	481	GET /pearson.png HTTP/1.1
762	26.871334	128.119.245.12	10.219.135.207	HTTP	929	HTTP/1.1 200 OK (PNG)
768	26.888664	10.219.135.207	128.119.245.12	HTTP	495	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
898	27.326315	128.119.245.12	10.219.135.207	HTTP	1082	HTTP/1.1 200 OK (JPEG JFIF image)

```
▶ Frame 752: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface en0, id 0
▶ Ethernet II, Src: Apple_eb:3d:24 (10:94:bb:eb:3d:24), Dst: Cisco_27:00:00 (00:25:83:27:00:00)
▶ Internet Protocol Version 4, Src: 10.219.135.207, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 56278, Dst Port: 80, Seq: 1, Ack: 1, Len: 483
▼ Hypertext Transfer Protocol
  ▶ GET /wireshark-labs/HTTP-wireshark-file4.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 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
    [HTTP request 1/2]
    [Response in frame: 754]
    [Next request in frame: 756]
```

```
0040  61 5a 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   aZGET /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 34 2e 68 74 6d 6c 20   hark-fil e4.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
```

```
Hypertext Transfer Protocol (http), 483 bytes    Packets: 1009 · Displayed: 6 (0.6%) · Dropped: 0 (0.0%)    Profile: Default
```

(Screenshot-7)

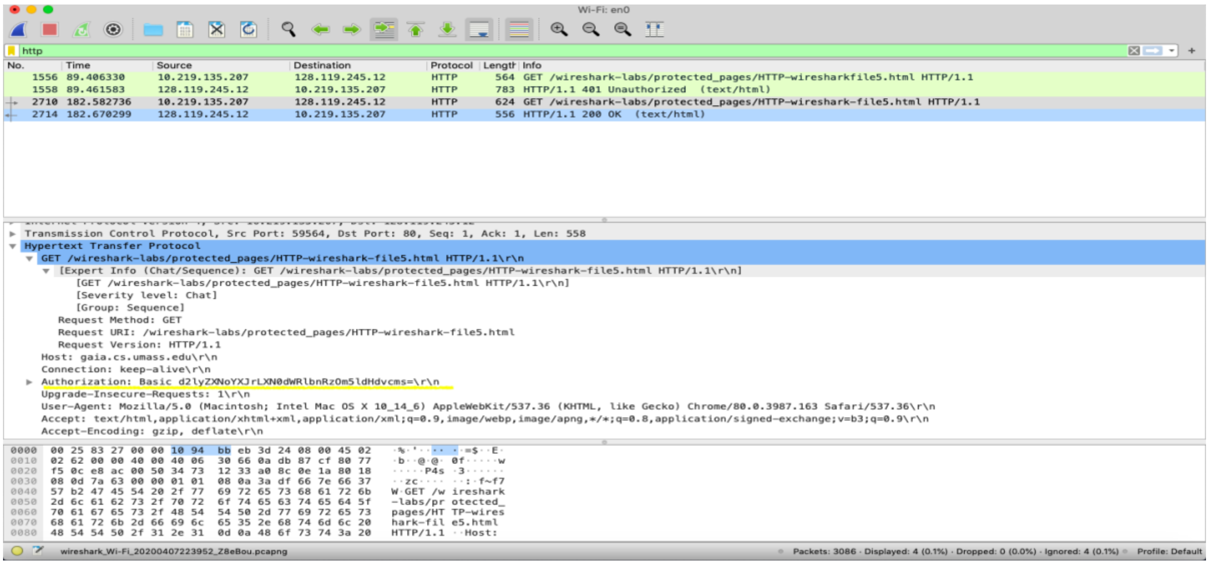
ANSWER NO.16

3 HTTP GET request messages were sent by my browser and they were sent to the following address: 128.119.245.12 (as can be seen from Screenshot-7).

ANSWER NO.17

The browser downloaded the two images serially as first image was requested and then the next image was requested. If they were downloaded in parallel then they would be returned in the same time period but here the second image was requested after the first image was received.

ANSWER NO.18



```
No.   Time        Source           Destination      Protocol Length Info
 1556 89.406330   10.219.135.207   128.119.245.12   HTTP      564 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
 1558 89.461583   128.119.245.12   10.219.135.207   HTTP      783 HTTP/1.1 401 Unauthorized  (text/html)
 2710 182.582736  10.219.135.207   128.119.245.12   HTTP      624 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
 2714 182.670299  128.119.245.12   10.219.135.207   HTTP      556 HTTP/1.1 200 OK  (text/html)
```

```
▶ Transmission Control Protocol, Src Port: 59564, Dst Port: 80, Seq: 1, Ack: 1, Len: 558
▼ Hypertext Transfer Protocol
  ▼ GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
  ▶ Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
```

```
0000  00 25 83 27 00 00 10 94  bb eb 3d 24 08 00 45 02   ·%·'····  ··=$··E·
0010  02 62 00 00 40 00 40 06  30 66 0a db 87 cf 80 77   ·b··@·@·  0f·····w
0020  f5 0c e8 ac 00 50 34 73  12 33 a0 8c 0e 1a 80 18   ·····P4s  ·3······
0030  08 0d 7a 63 00 00 01 01  08 0a 3a df 66 7e 66 37   ··zc····  ··:·f~f7
0040  57 b2 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   W·GET /w  ireshark
0050  2d 6c 61 62 73 2f 70 72  6f 74 65 63 74 65 64 5f   -labs/pr  otected_
0060  70 61 67 65 73 2f 48 54  54 50 2d 77 69 72 65 73   pages/HT  TP-wires
0070  68 61 72 6b 2d 66 69 6c  65 35 2e 68 74 6d 6c 20   hark-fil  e5.html 
0080  48 54 54 50 2f 31 2e 31  0d 0a 48 6f 73 74 3a 20   HTTP/1.1  ··Host: 
```

```
wireshark_Wi-Fi_20200407223952_Z8eBou.pcapng      Packets: 3086 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%) · Ignored: 4 (0.1%)   Profile: Default
```

(Screenshot-8)

From Screenshot-8 it can be observed that the Server’s response was 401 Unauthorized (text/html) where 401 is Status Code and phrase is Unauthorized (text/html).

ANSWER NO.19

From the Screenshot-8 we can see the new field included in the HTTP GET Message:
Authorization: Basic d2lyZXNoYXJrLxn0dWRlbnRzOm5ldHdvcms=\r\n

REFRENCES

- https://www.youtube.com/watch?v=fjalFI11xtE&t=83s