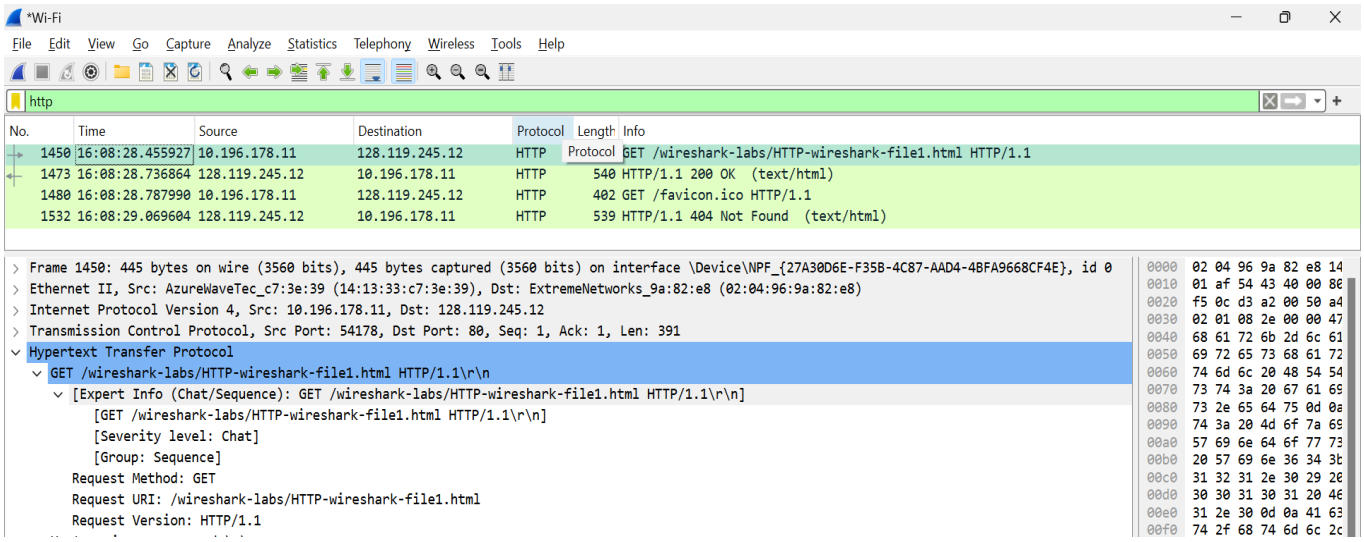
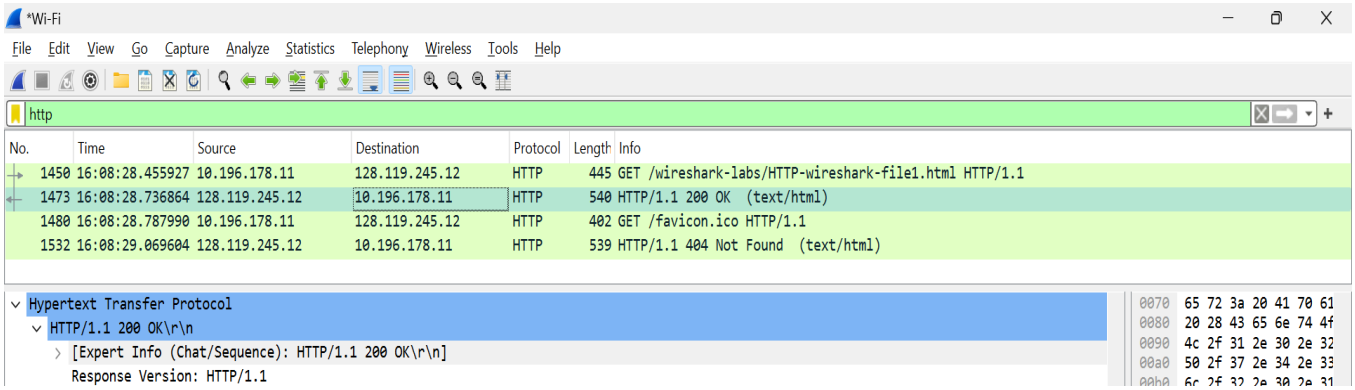
Assignment 3

Part-1

1. The browser is running HTTP version 1.1(Request Version: HTTP/1.1)

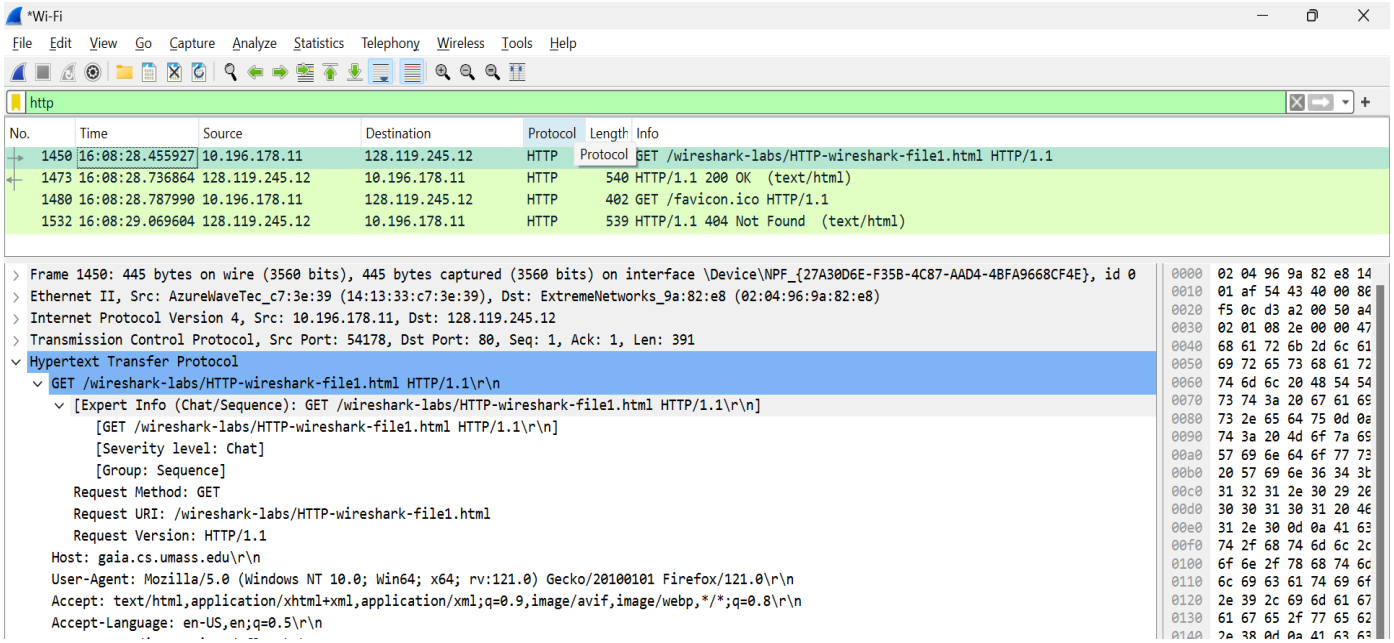


The server is running HTTP version 1.1(Response Version: HTTP/1.1)

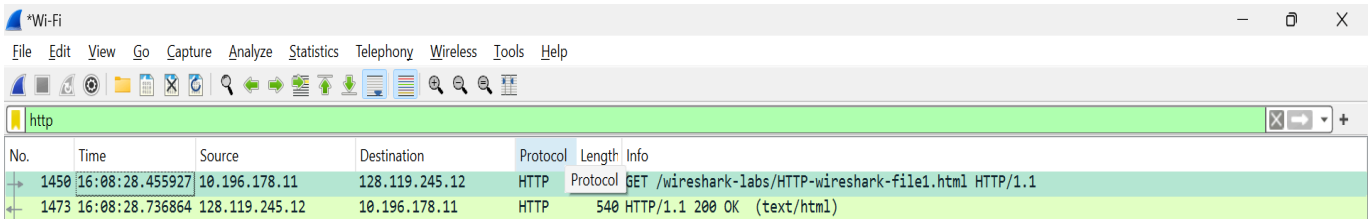


2. Accept-language: en-US,en with q(relative-factor)=0.5

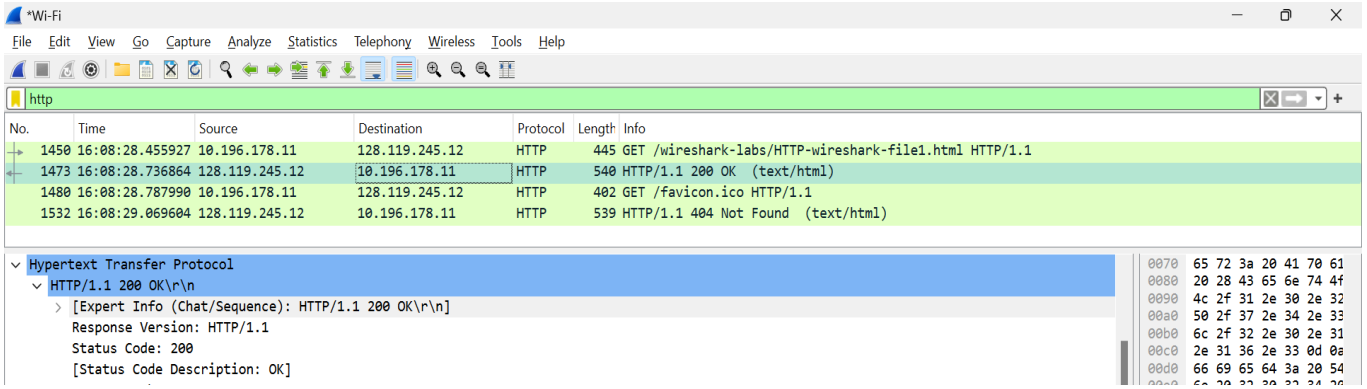
The browser indicates that it can accept US English and other types of english to the server.



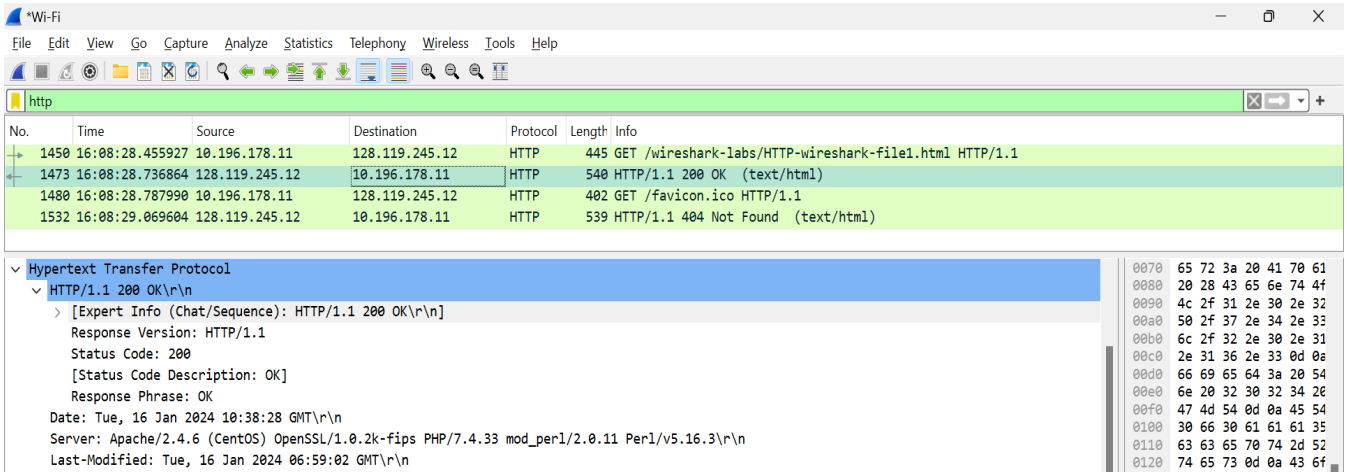
3. IP address of my computer is 10.196.178.11
IP address of the gaia.cs.umass.edu server is 128.119.245.12



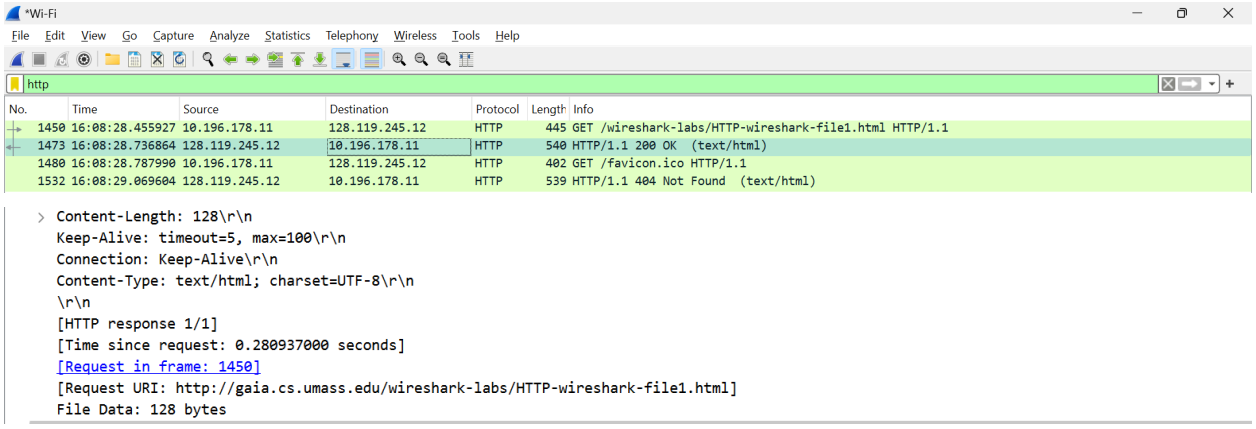
4. The status code returned from the server to my browser is 200(Status Code Description: OK)



5. The HTML file that I am retrieving was last modified at the server at Tuesday, 16th Jan 2024 06:59:02 AM.

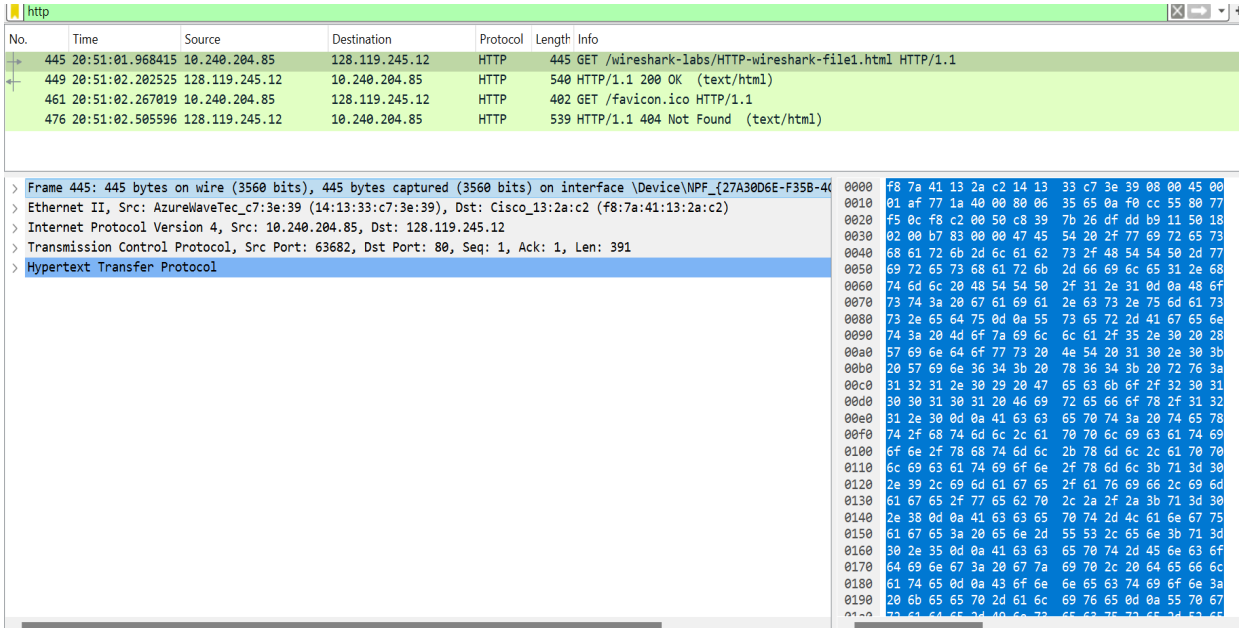


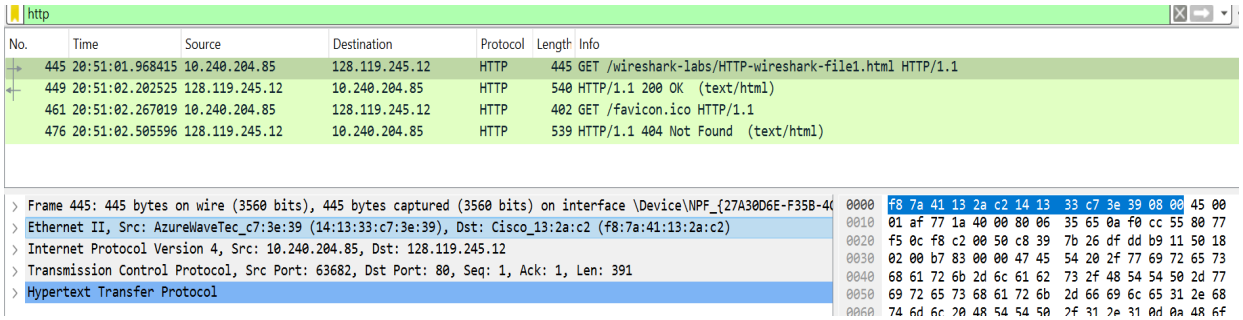
6. 128 bytes of content are being returned to your browser(Content-Length: 128).

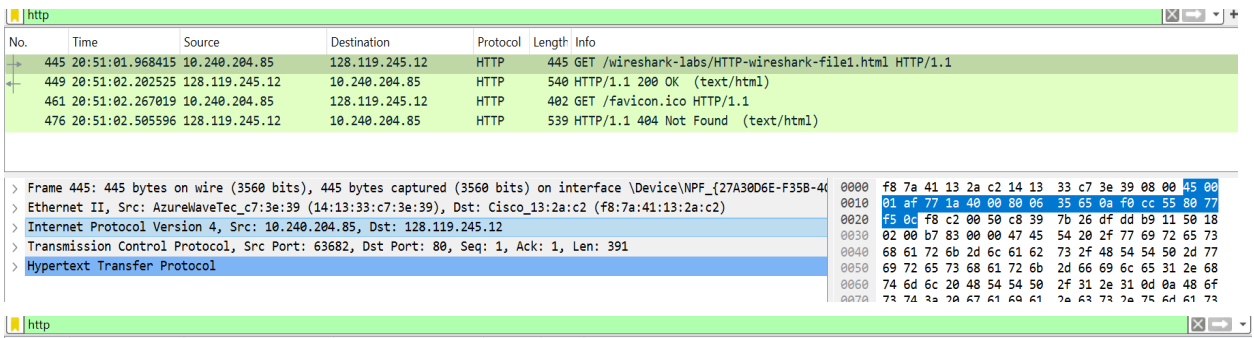


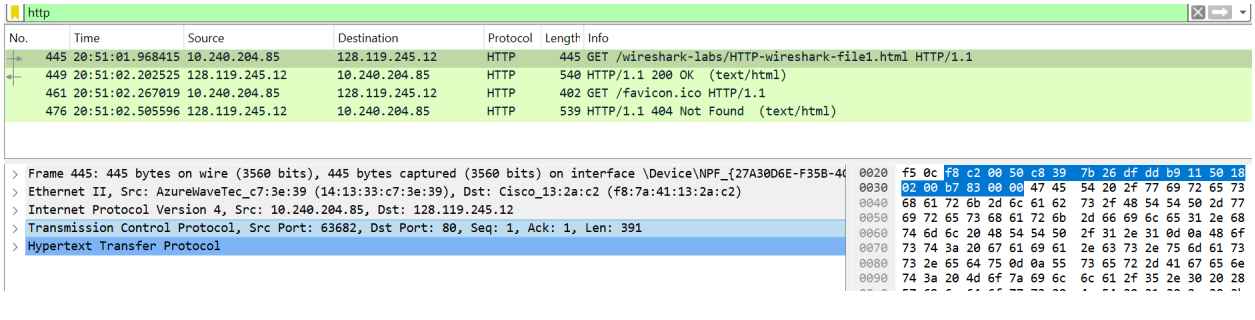
7. No, I don't see any headers within the data that are not displayed in the packet-listing window.

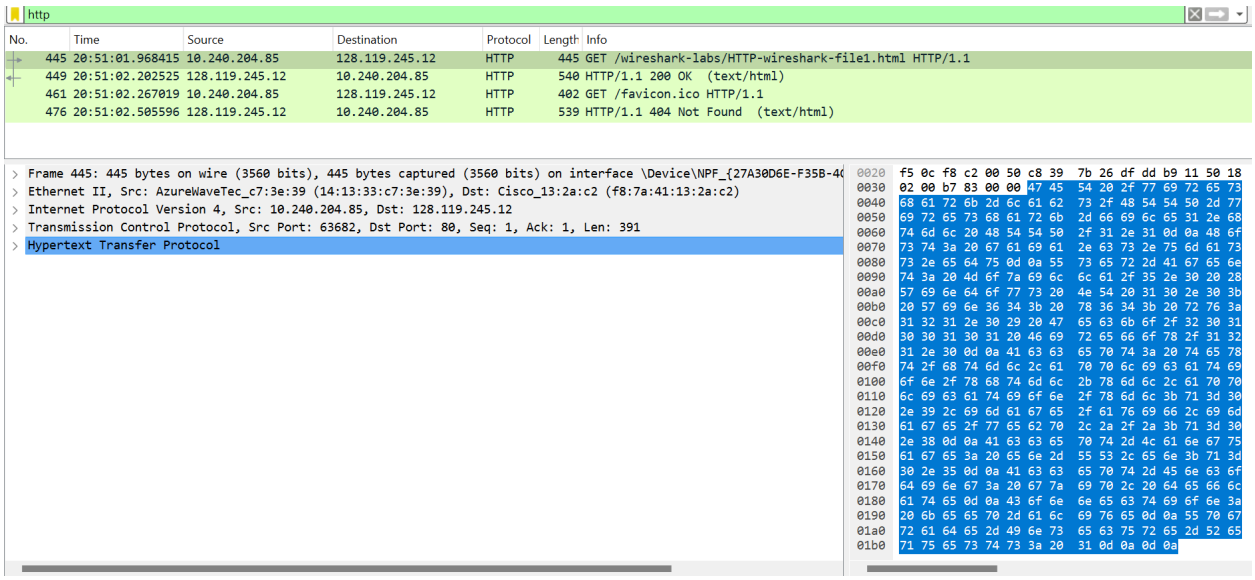
The below is an example checking for a GET message, similarly for all other requests/responses every field is displayed in the packet-listing window.


http
No. Time Source Destination Protocol Length Info
445 20:51:01.968415 10.240.204.85 128.119.245.12 HTTP 445 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449 20:51:02.202525 128.119.245.12 10.240.204.85 HTTP 540 HTTP/1.1 200 OK (text/html)
461 20:51:02.267019 10.240.204.85 128.119.245.12 HTTP 402 GET /favicon.ico HTTP/1.1
476 20:51:02.505596 128.119.245.12 10.240.204.85 HTTP 539 HTTP/1.1 404 Not Found (text/html)
Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-4
Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)
Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
Hypertext Transfer Protocol
0000 f8 7a 41 13 2a c2 14 13 33 c7 3e 39 08 00 45 00
0010 01 af 77 1a 40 00 80 06 35 65 0a f0 cc 55 80 77
0020 f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
0030 02 00 b7 83 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
0080 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e
0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28
0190 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67


http
No. Time Source Destination Protocol Length Info
445 20:51:01.968415 10.240.204.85 128.119.245.12 HTTP 445 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449 20:51:02.202525 128.119.245.12 10.240.204.85 HTTP 540 HTTP/1.1 200 OK (text/html)
461 20:51:02.267019 10.240.204.85 128.119.245.12 HTTP 402 GET /favicon.ico HTTP/1.1
476 20:51:02.505596 128.119.245.12 10.240.204.85 HTTP 539 HTTP/1.1 404 Not Found (text/html)
Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-4
Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)
Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
Hypertext Transfer Protocol
0000 f8 7a 41 13 2a c2 14 13 33 c7 3e 39 08 00 45 00
0010 01 af 77 1a 40 00 80 06 35 65 0a f0 cc 55 80 77
0020 f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
0030 02 00 b7 83 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68

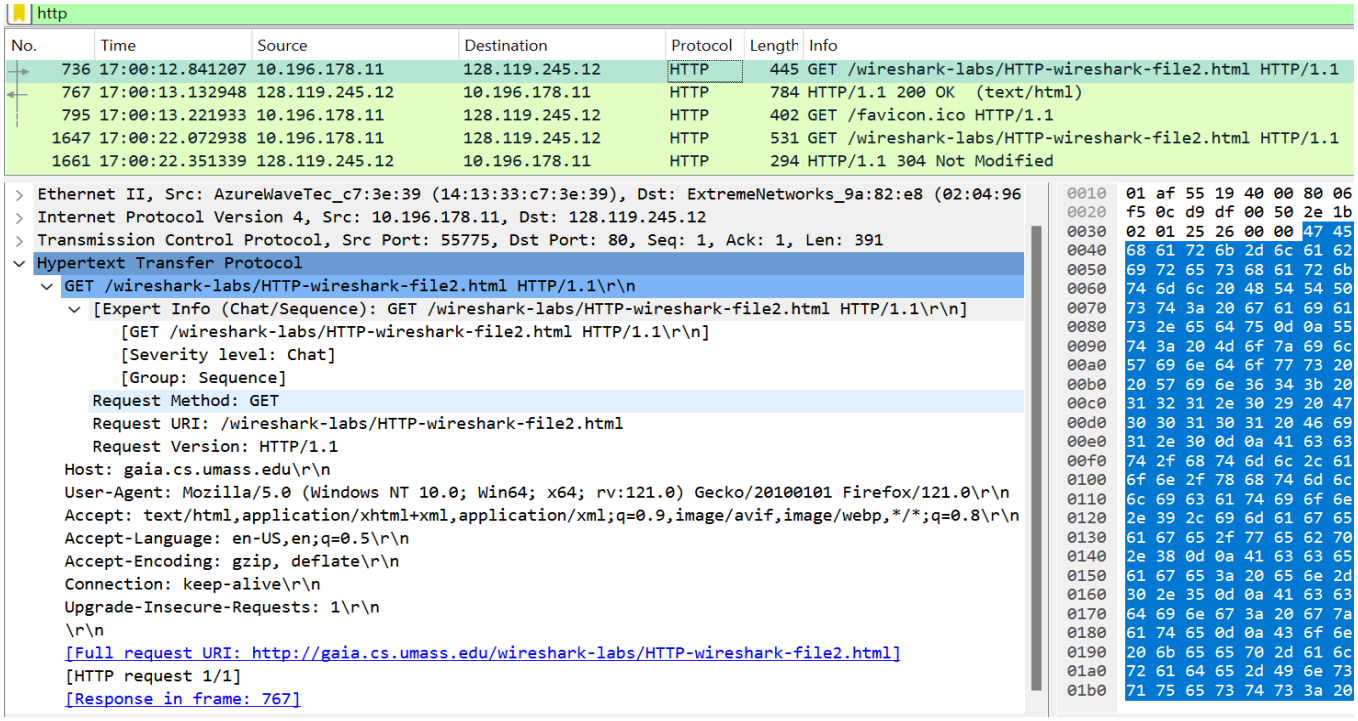

http
No. Time Source Destination Protocol Length Info
445 20:51:01.968415 10.240.204.85 128.119.245.12 HTTP 445 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449 20:51:02.202525 128.119.245.12 10.240.204.85 HTTP 540 HTTP/1.1 200 OK (text/html)
461 20:51:02.267019 10.240.204.85 128.119.245.12 HTTP 402 GET /favicon.ico HTTP/1.1
476 20:51:02.505596 128.119.245.12 10.240.204.85 HTTP 539 HTTP/1.1 404 Not Found (text/html)
Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-4
Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)
Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
Hypertext Transfer Protocol
0000 f8 7a 41 13 2a c2 14 13 33 c7 3e 39 08 00 45 00
0010 01 af 77 1a 40 00 80 06 35 65 0a f0 cc 55 80 77
0020 f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
0030 02 00 b7 83 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f


http
No. Time Source Destination Protocol Length Info
445 20:51:01.968415 10.240.204.85 128.119.245.12 HTTP 445 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
449 20:51:02.202525 128.119.245.12 10.240.204.85 HTTP 540 HTTP/1.1 200 OK (text/html)
461 20:51:02.267019 10.240.204.85 128.119.245.12 HTTP 402 GET /favicon.ico HTTP/1.1
476 20:51:02.505596 128.119.245.12 10.240.204.85 HTTP 539 HTTP/1.1 404 Not Found (text/html)
Frame 445: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{27A30D6E-F35B-4
Ethernet II, Src: AzureWaveTec_c7:3e:39 (14:13:33:c7:3e:39), Dst: Cisco_13:2a:c2 (f8:7a:41:13:2a:c2)
Internet Protocol Version 4, Src: 10.240.204.85, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63682, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
Hypertext Transfer Protocol
0020 f5 0c f8 c2 00 50 c8 39 7b 26 df dd b9 11 50 18
0030 02 00 b7 83 00 00 47 45 54 20 2f 77 69 72 65 73
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73
0080 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e
0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28

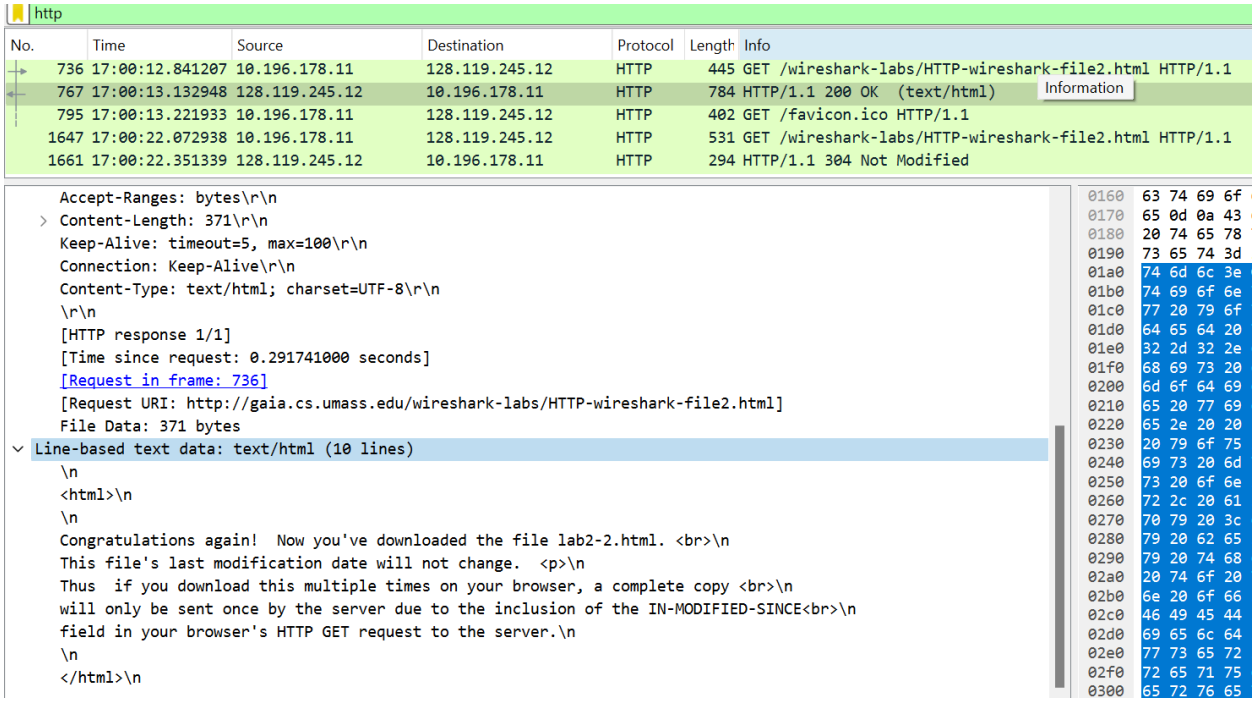


Part-2

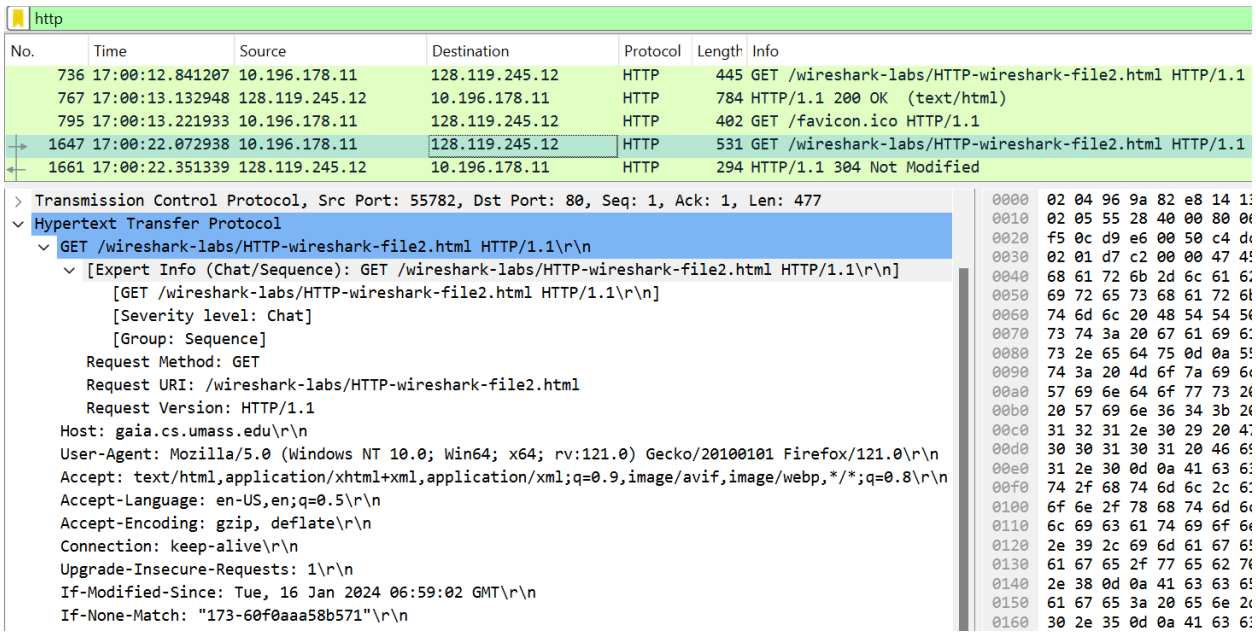
1. No, “IF-MODIFIED-SINCE” line in the first HTTP GET is not present.



2. The server explicitly returned the contents of the file. The “Line-based text data” field in the message represents the file content.



3. Yes, “IF-MODIFIED-SINCE” line in the second HTTP GET is present. The information followed by it is: Tue, 16 Jan 2024 06:59:02 GMT.



The If-Modified-Since HTTP header indicates the time for which a browser first downloaded a resource from the server. When used in combination with the If-None-Match, it is ignored, unless the server does not support If-None-Match.

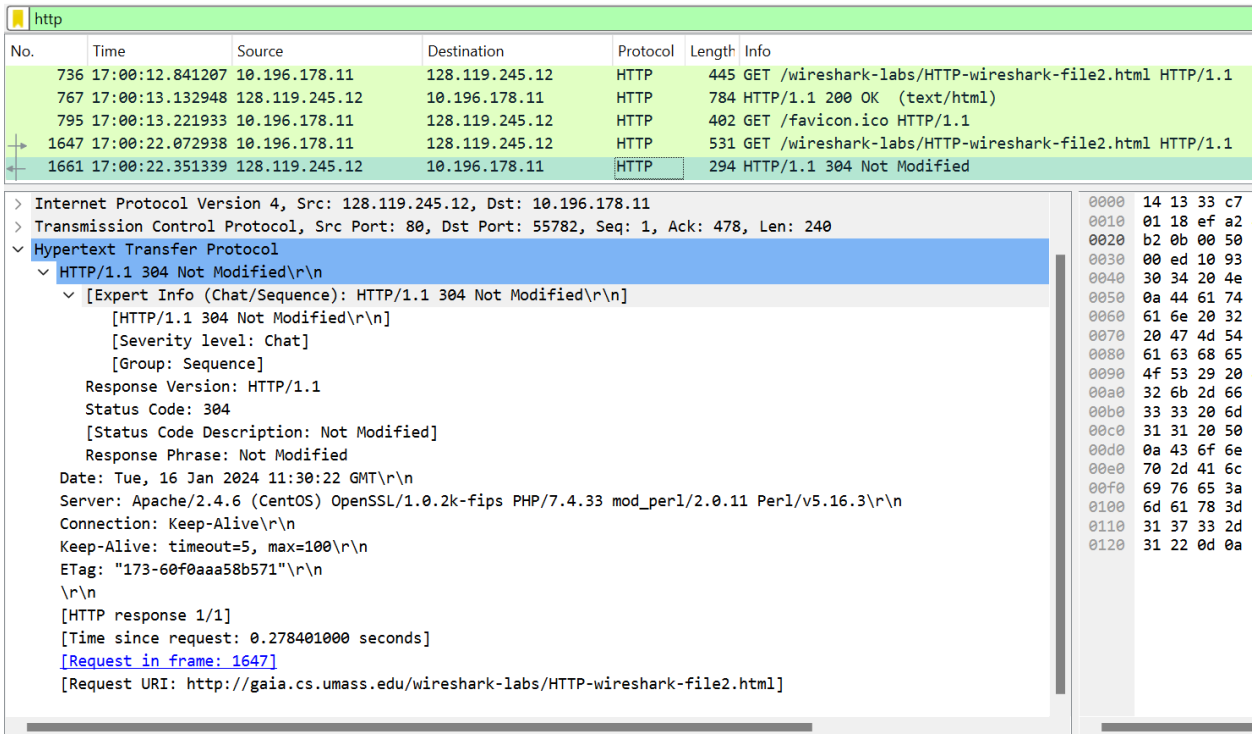
4. For the second HTTP GET,
Status code: 200

Response phrase: OK

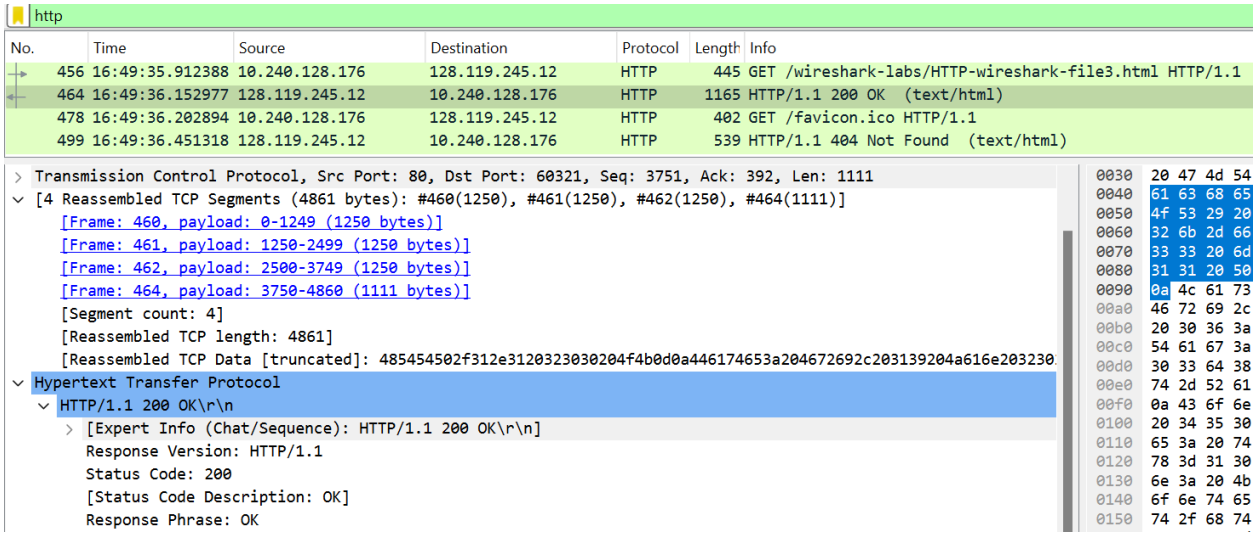
The server didn't explicitly return the contents of the file. As the “Line-based text data” field is not present in the response. This may be due to:

Here the content is already in the browser's cache, the browser issued a conditional GET request, and the server responded with a "304 Not Modified" status instead of sending the full content.

Modern web browsers use HTTP persistent connections to improve performance. This means that a single TCP connection is reused for multiple requests, reducing the overhead of establishing new connections. The HTTP "Keep-Alive" header is used to request that the connection be kept open for additional requests. Here the connection between server and the browser is kept alive throughout, so we can say subsequent requests may be part of the same TCP connection.



Part-3



1. 1 HTTP GET request message was sent by my browser. 456 packet number in the trace contains the GET message for the Bill or Rights.

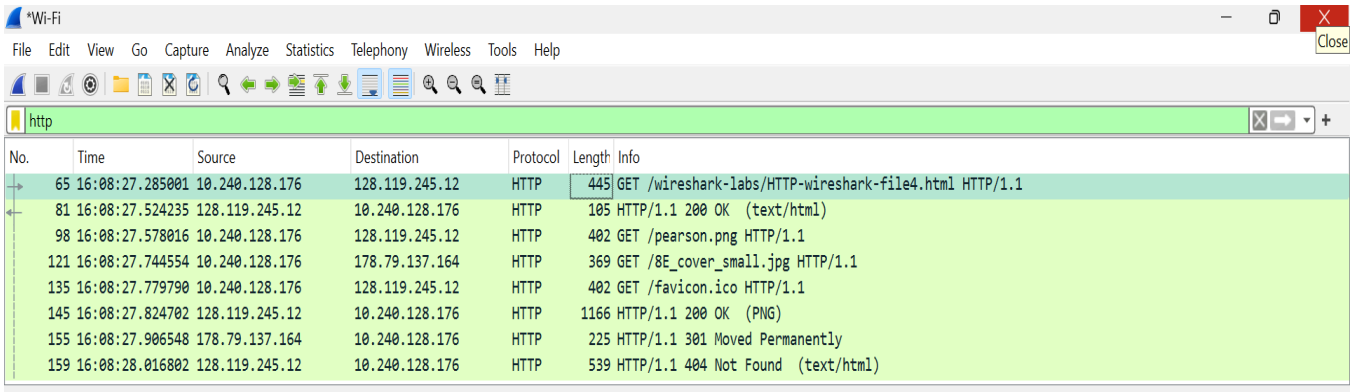
2. The 464 packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request.

3. Status code: 200
Response phrase: OK

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

Part-4

1.



A total of 4(packet no: 65,98,121,135) GET messages(including GET message for favicon icon, else 3 GET messages) are sent from the browser. The requests are sent to the following Internet addresses:

```
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
[HTTP request 1/1]
[Response in frame: 81]
```

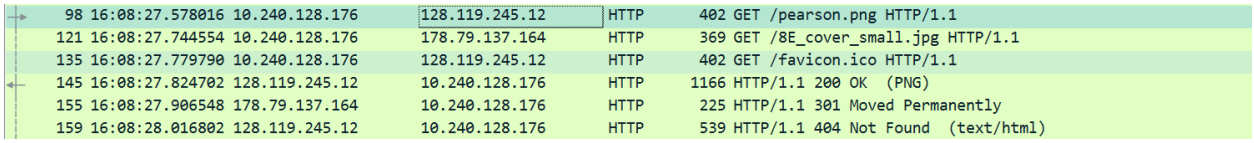
```
[Full request URI: http://gaia.cs.umass.edu/pearson.png]
[HTTP request 1/1]
[Response in frame: 145]
```

```
[Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
[HTTP request 1/1]
[Response in frame: 155]
```

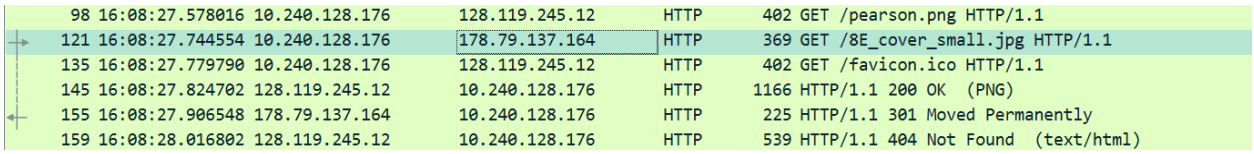
```
[Full request URI: http://gaia.cs.umass.edu/favicon.ico]
[HTTP request 1/1]
[Response in frame: 159]
```

1st GET request sent to “http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html”
2nd GET request sent to “http://gaia.cs.umass.edu/pearson.png”
3rd GET request sent to “http://kurose.cslash.net/8E_cover_small.jpg”
4th GET request sent to “http://gaia.cs.umass.edu/favicon.ico”

2. The two images were downloaded from the two websites in parallel.



```
  98 16:08:27.578016 10.240.128.176 128.119.245.12    HTTP  402 GET /pearson.png HTTP/1.1
 121 16:08:27.744554 10.240.128.176 178.79.137.164    HTTP  369 GET /8E_cover_small.jpg HTTP/1.1
 135 16:08:27.779790 10.240.128.176 128.119.245.12    HTTP  402 GET /favicon.ico HTTP/1.1
 145 16:08:27.824702 128.119.245.12 10.240.128.176    HTTP 1166 HTTP/1.1 200 OK  (PNG)
 155 16:08:27.906548 178.79.137.164 10.240.128.176    HTTP  225 HTTP/1.1 301 Moved Permanently
 159 16:08:28.016802 128.119.245.12 10.240.128.176    HTTP  539 HTTP/1.1 404 Not Found  (text/html)
```



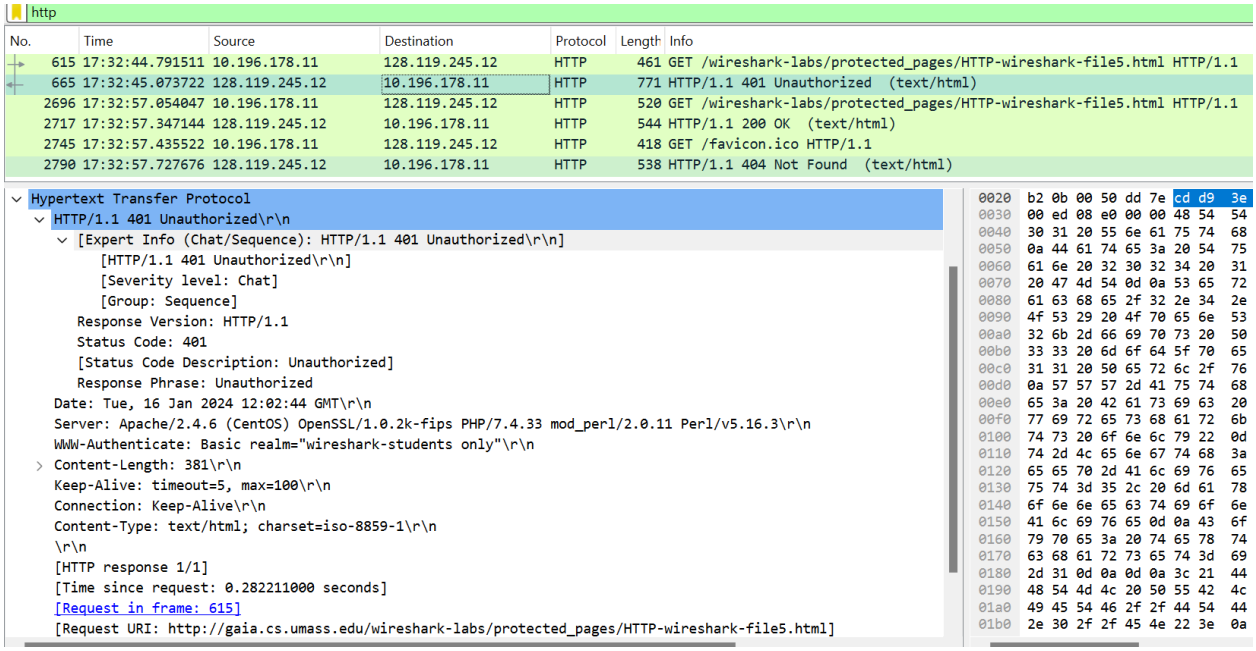
```
  98 16:08:27.578016 10.240.128.176 128.119.245.12    HTTP  402 GET /pearson.png HTTP/1.1
 121 16:08:27.744554 10.240.128.176 178.79.137.164    HTTP  369 GET /8E_cover_small.jpg HTTP/1.1
 135 16:08:27.779790 10.240.128.176 128.119.245.12    HTTP  402 GET /favicon.ico HTTP/1.1
 145 16:08:27.824702 128.119.245.12 10.240.128.176    HTTP 1166 HTTP/1.1 200 OK  (PNG)
 155 16:08:27.906548 178.79.137.164 10.240.128.176    HTTP  225 HTTP/1.1 301 Moved Permanently
 159 16:08:28.016802 128.119.245.12 10.240.128.176    HTTP  539 HTTP/1.1 404 Not Found  (text/html)
```

The GET requests for the two images having packet numbers 98 and 121 respectively are sent simultaneously before either of their responses(i.e. packet no: 145 and 155) are received. Therefore, we can say the images are fetched simultaneously.

Part-5

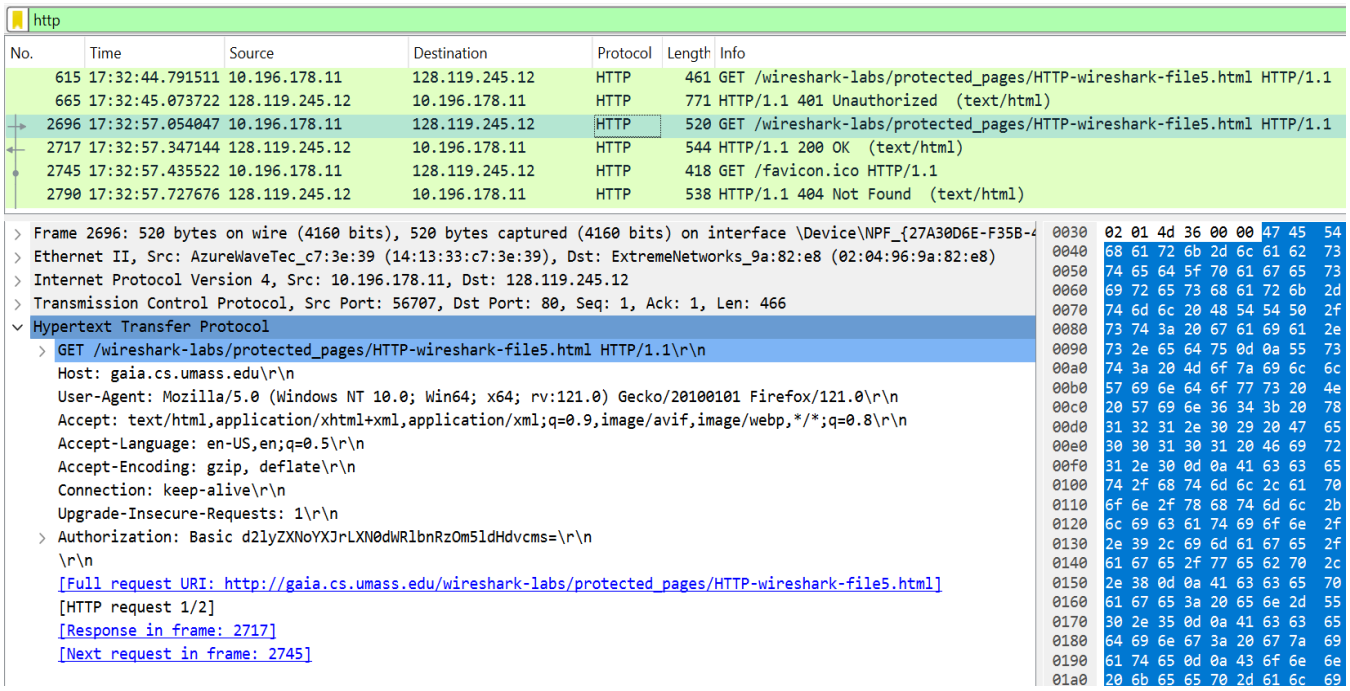
1. The server’s response to the initial HTTP GET message from my browser is
Status Code: 401

Response phrase: Unauthorized



2. The new field which is included in the 2nd HTTP GET message is “Authorization: Basic”

2nd GET message:



1st GET message: