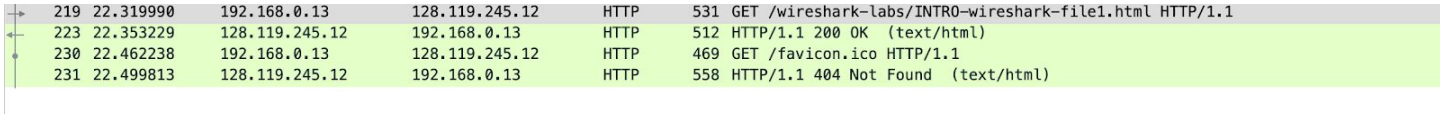
1.

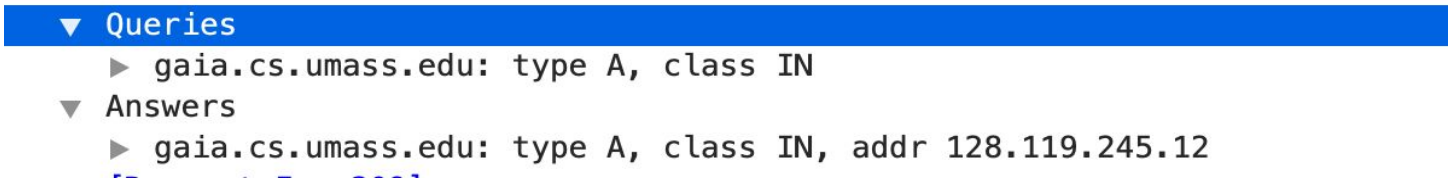
3 different protocols that appear in the protocol column in the unfiltered packet-listing window in the step 7 are:
HTTP, TCP, UDP, DNS

2.



The HTTP request was sent at 22.319990 second by IP 192.168.0.13 to IP 128.119.245.12
The HTTP response was sent by IP 128.119.245.12 to IP 192.168.0.13 at 22.353229 seconds
Hence, the time taken is 22.353229 - 22.319990 = 0.033239 Seconds

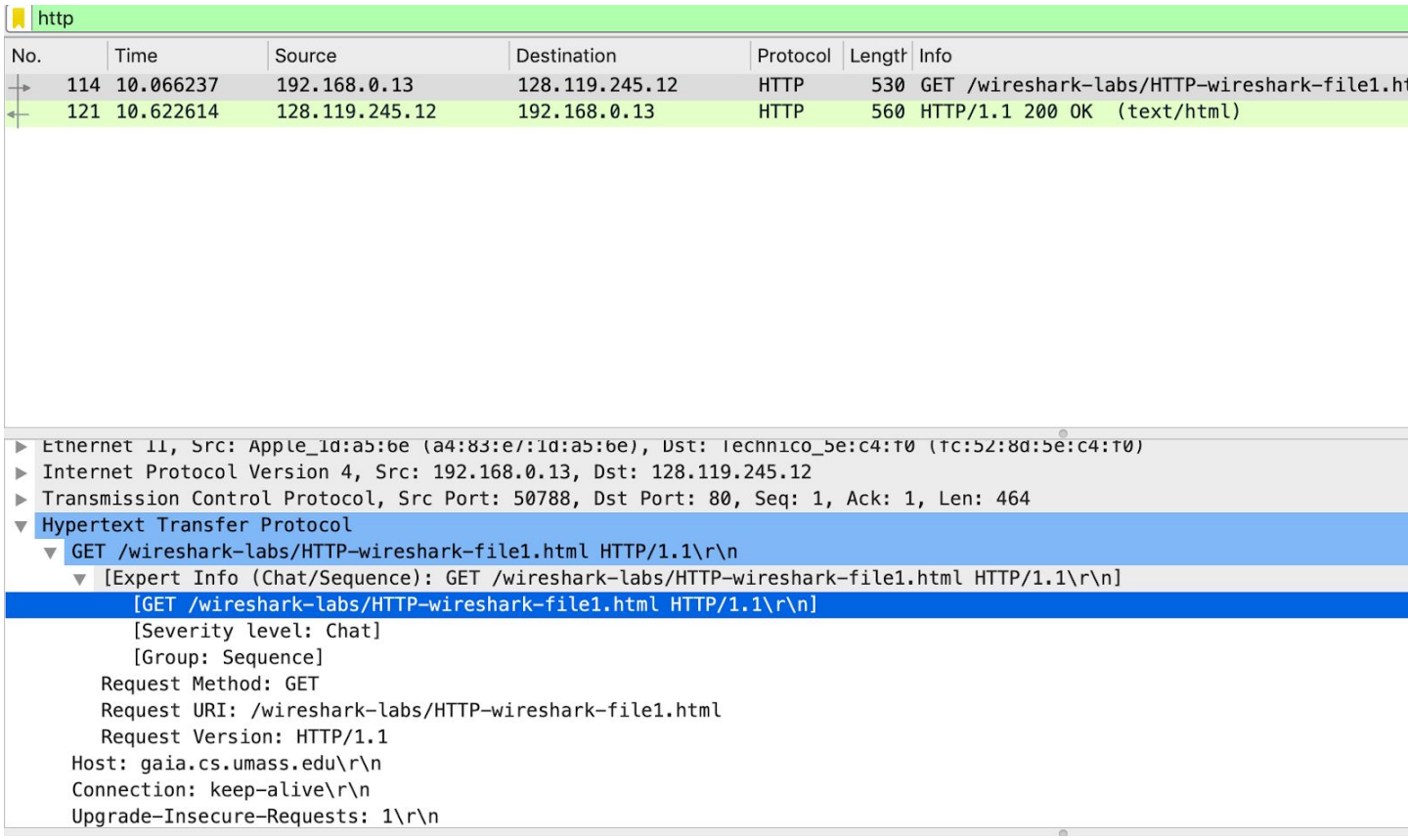
3.
The IP address of wwwnet.cs.umass.edu is
Destination: 128.119.245.12
The same can be observed in the DNS query:



The IP address of my computer is : 192.168.0.13

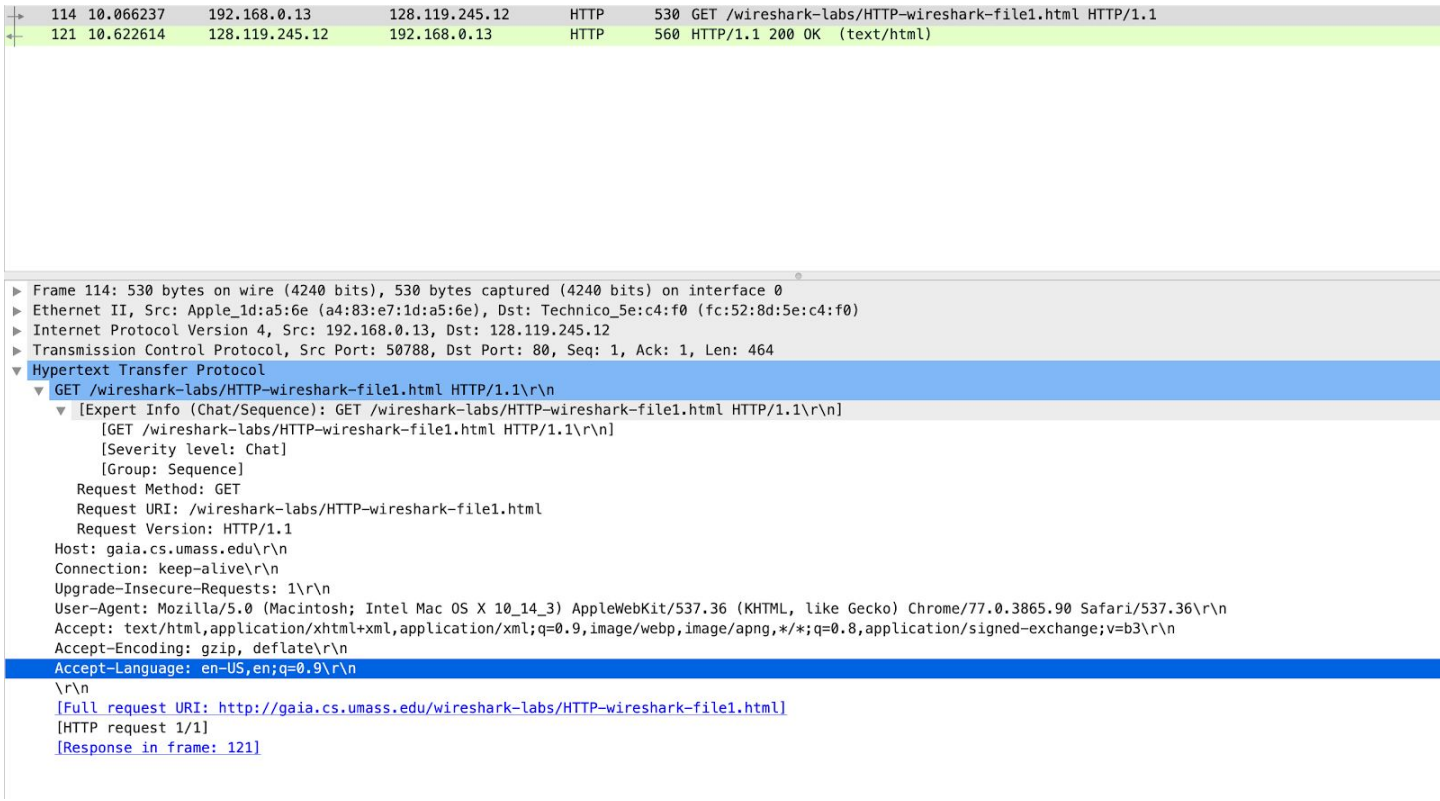
Actual questions to be done

1.
Both my browser and the server to which the request goes are running HTTP version 1.1.
Please see in the attached screenshots:



2.

The languages accepted by the Browser will be : en-US, en

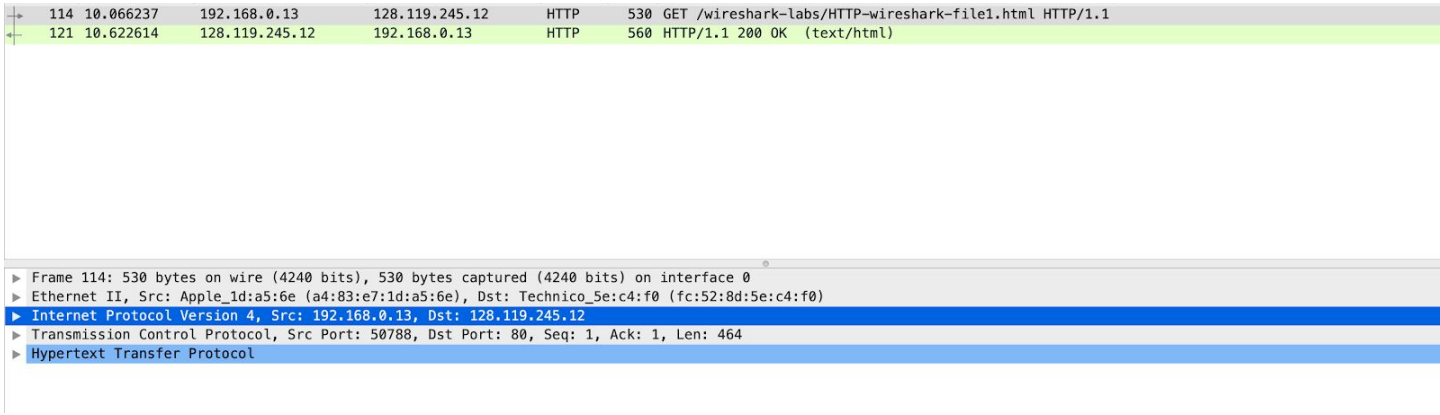


3.

The IP address of My computer and gaia.cs.umass.edu server are :

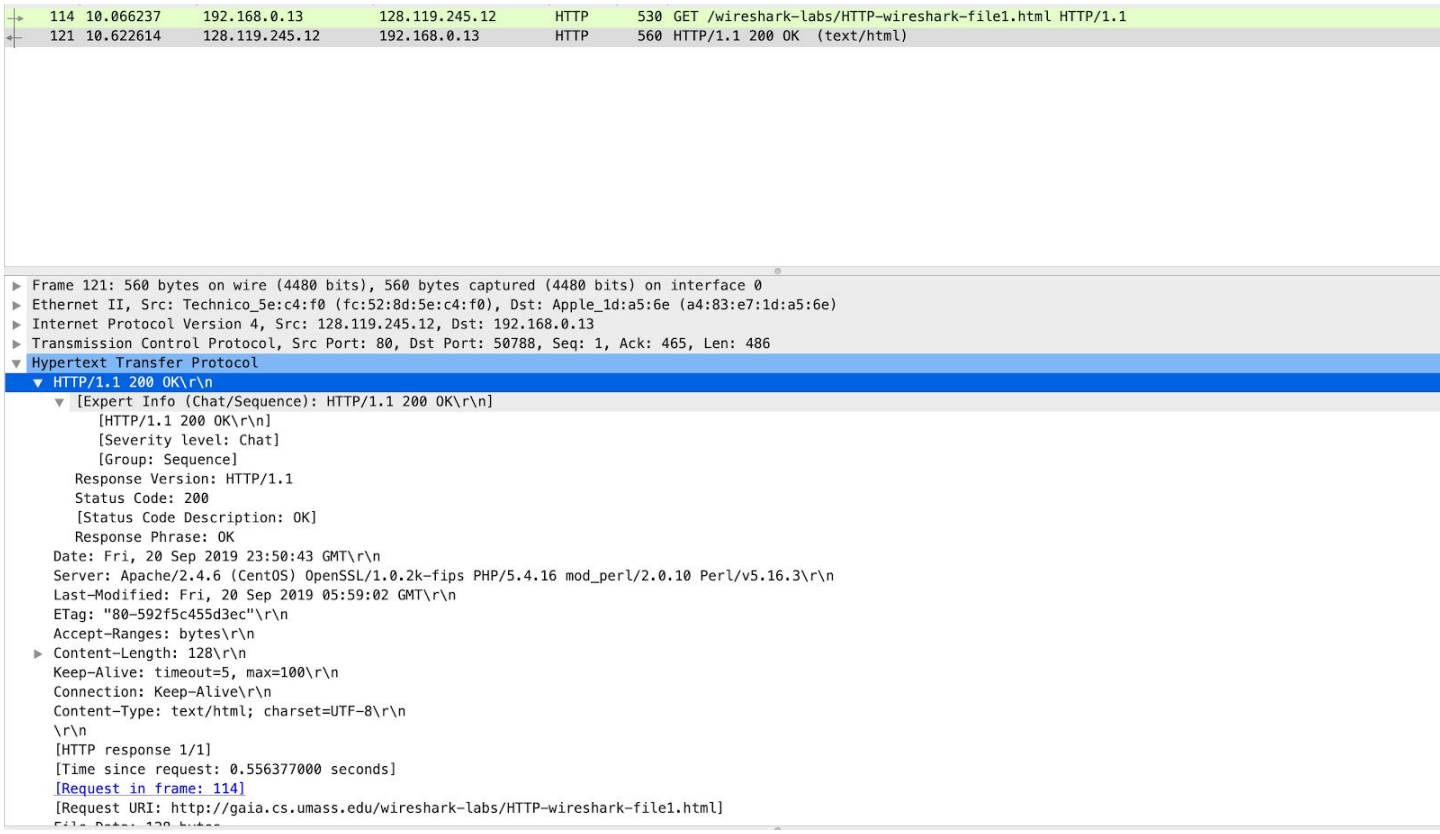
My computer : 192.168.0.13

Gaia.cs.umass.edu server : 128.119.245.12



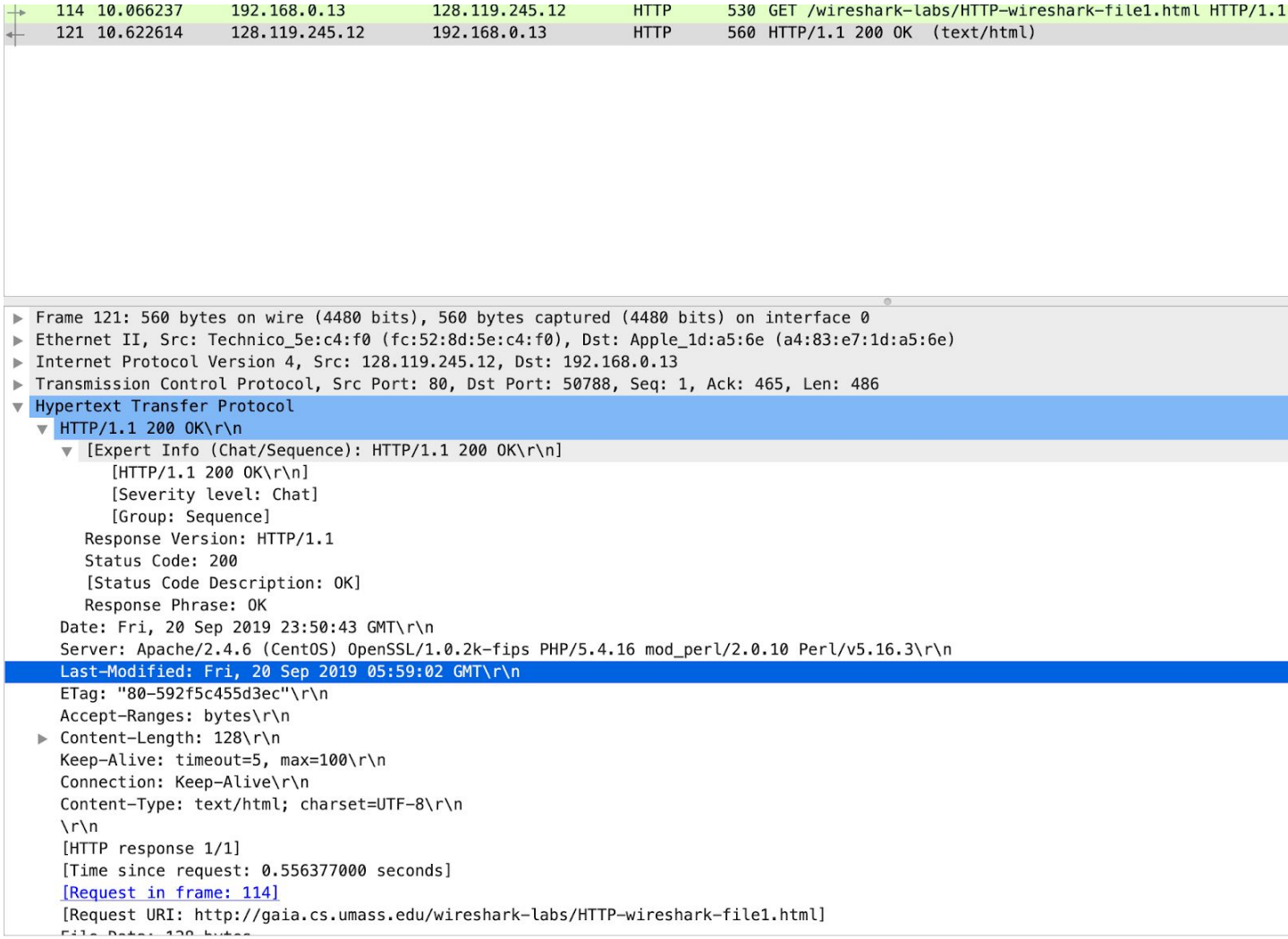
4.

Status code from the Server to the Browser : 200 OK



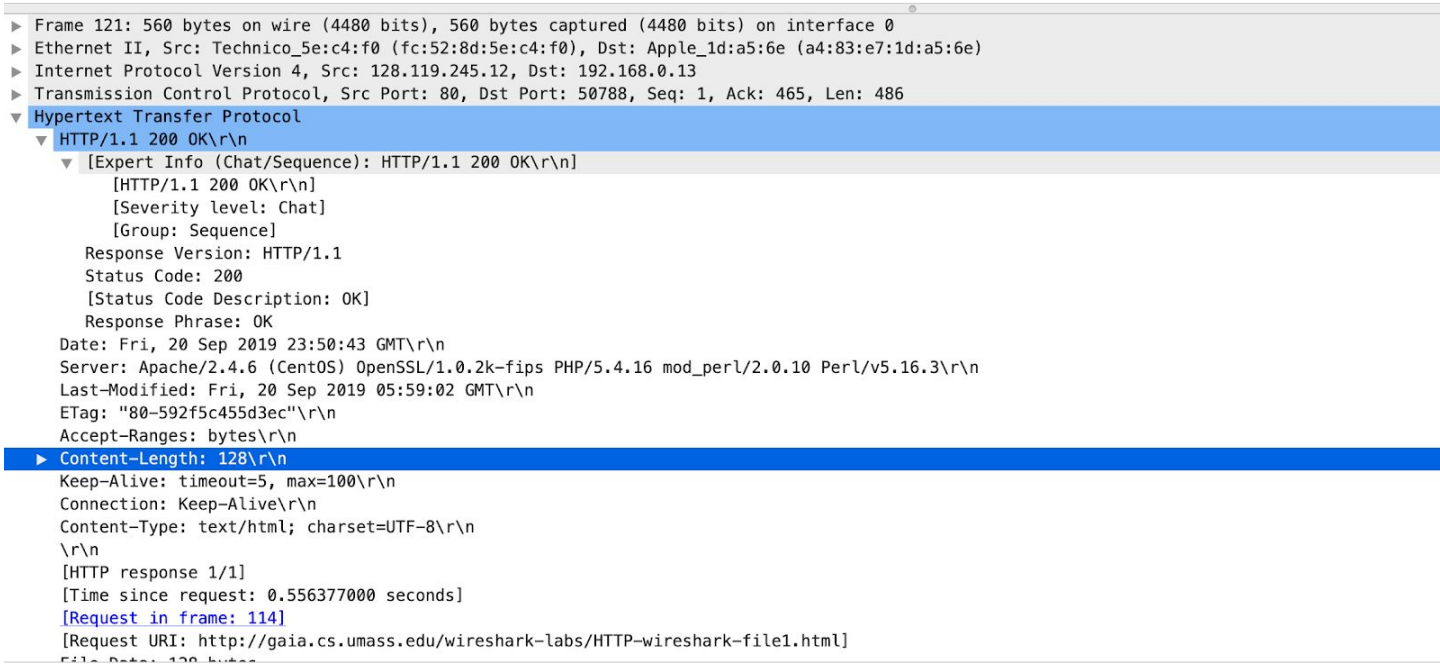
5.

The HTML file that I am retrieving was last modified by the server: Fri, 20 Sep 2019 5:59:02 GMT



6.

The length of content returned by the Browser is 128 as in the below picture:



7.
The raw data is exactly the same as the data in the packet listing window.

8.
There is no “IF-MODIFIED-SINCE” line in the first HTTP GET request.

9.
Yes the server does explicitly returns the contents of the File. The response sent by the server is 200 OK and also it can be seen in the below figure that the content of the file is present in the response.

No.	Time	Source	Destination	Protocol	Length	Info
55	7.782153	192.168.0.13	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
58	7.948532	128.119.245.12	192.168.0.13	HTTP	804	HTTP/1.1 200 OK (text/html)
132	26.760697	192.168.0.13	128.119.245.12	HTTP	642	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
135	26.809414	128.119.245.12	192.168.0.13	HTTP	314	HTTP/1.1 304 Not Modified

```
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Sat, 21 Sep 2019 01:24:02 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, 20 Sep 2019 05:59:02 GMT\r\n
  ETag: "173-592f5c455cc1c"\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 1/1]
  [Time since request: 0.166379000 seconds]
  [Request in frame: 55]
  [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
```

10.

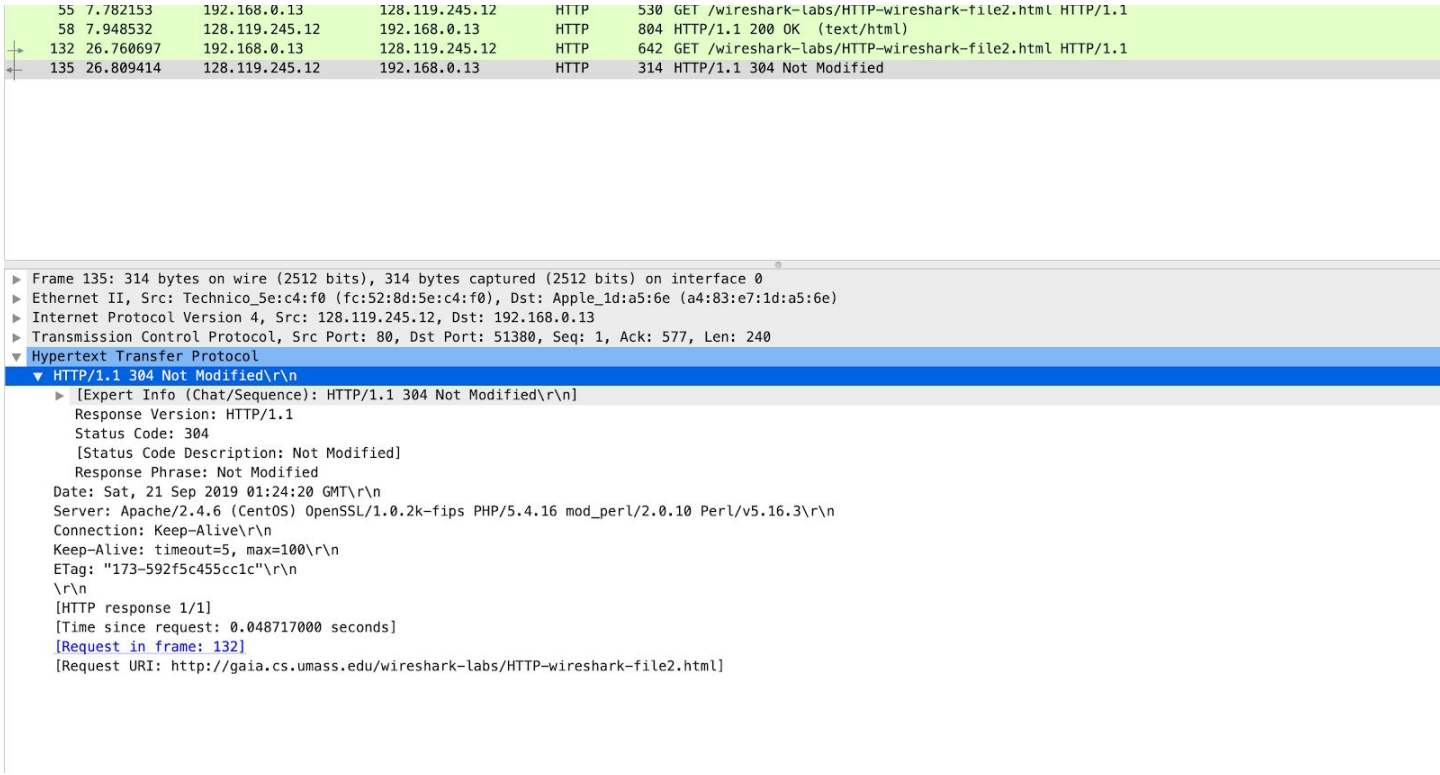
Yes, there is an IF-MODIFIED-HEADER field in the second GET request.

The value is : Fri, 20 Sep 2019 05:59:02 GMT

55	7.782153	192.168.0.13	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
58	7.948532	128.119.245.12	192.168.0.13	HTTP	804	HTTP/1.1 200 OK (text/html)
132	26.760697	192.168.0.13	128.119.245.12	HTTP	642	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
135	26.809414	128.119.245.12	192.168.0.13	HTTP	314	HTTP/1.1 304 Not Modified

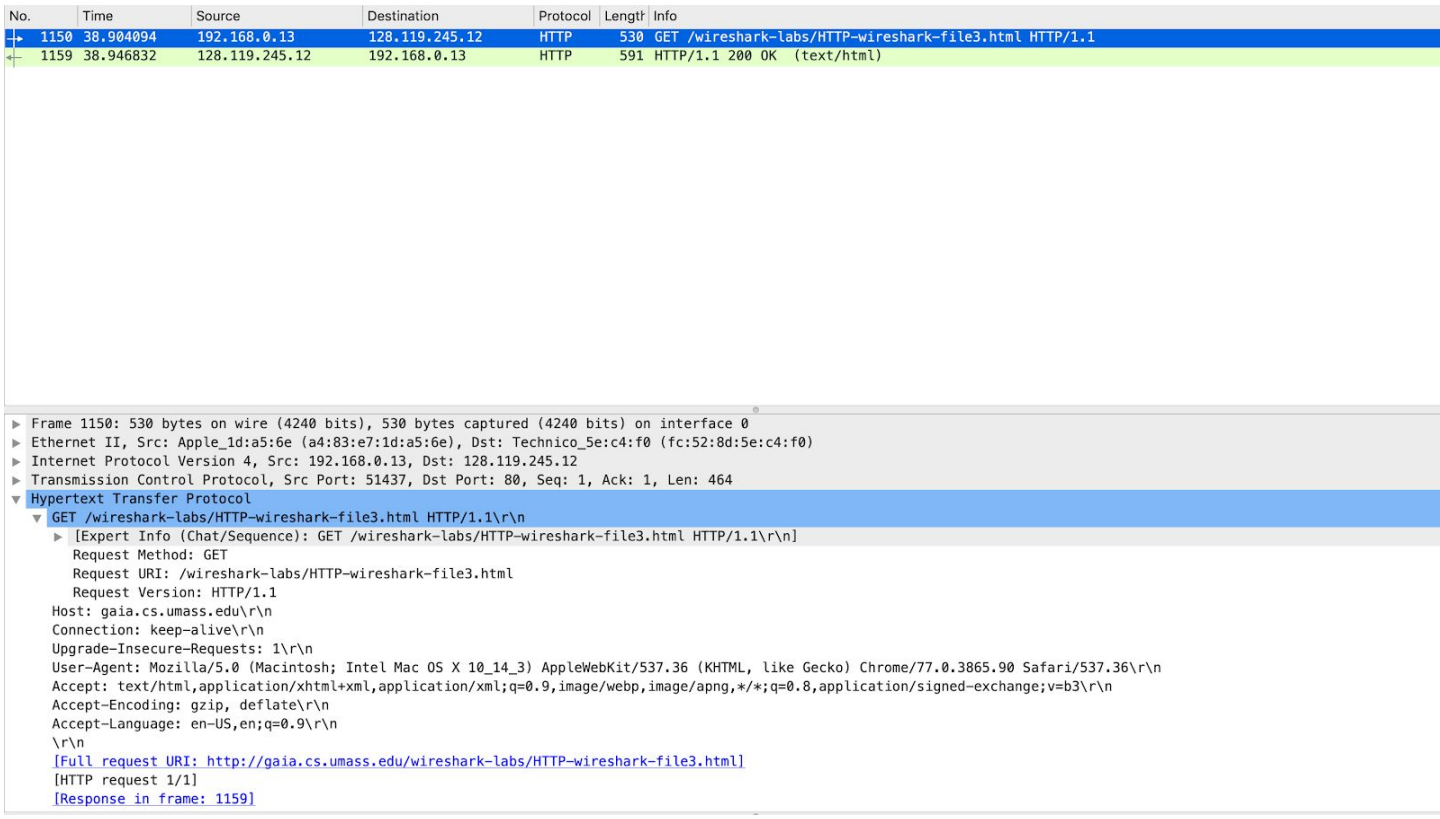
```
▶ Frame 132: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface 0
▶ Ethernet II, Src: Apple_1d:a5:6e (a4:83:e7:1d:a5:6e), Dst: Technico_5e:c4:f0 (fc:52:8d:5e:c4:f0)
▶ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 51380, Dst Port: 80, Seq: 1, Ack: 1, Len: 576
▼ 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
  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_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 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\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9\r\n
  If-None-Match: "173-592f5c455cc1c"\r\n
  If-Modified-Since: Fri, 20 Sep 2019 05:59:02 GMT\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  [HTTP request 1/1]
  [Response in frame: 135]
```

11.



It can be seen that the server responds with a 304 Not Modified response.
The previous GET request told the server to give the body of the response if it is modified since the time given in the GET request sent.
Since in this case the local copy stored at the machine in the cache was not modified since then the server responded with a 304 NOT MODIFIED message.
The 304 NOT MODIFIED message tells the cache to go ahead and forward the objects requested to the browser.

12.
The Browser sends only one GET request.
You can check the Message number 1150

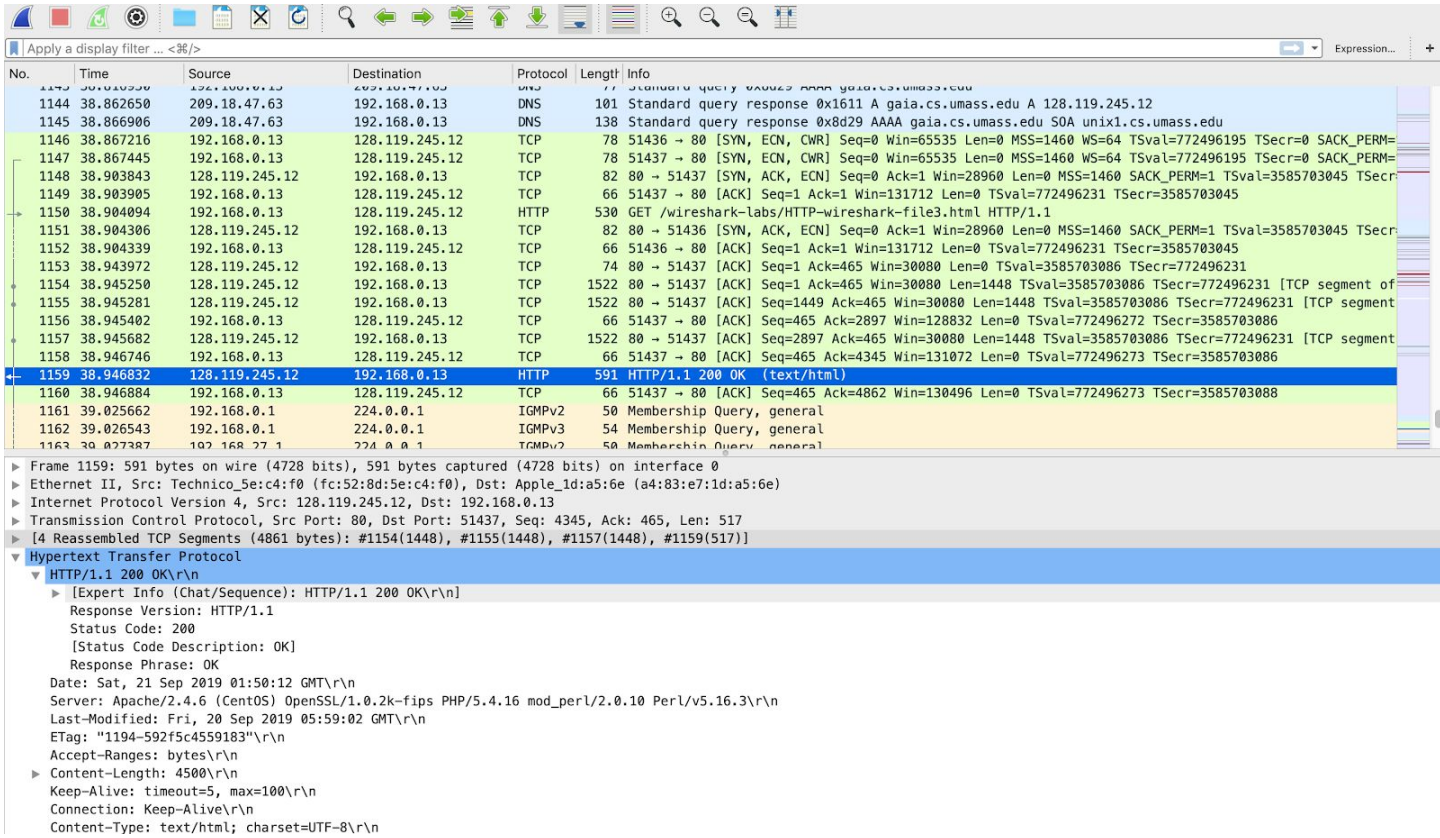


No.	Time	Source	Destination	Protocol	Length	Info
1150	38.904094	192.168.0.13	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1159	38.946832	128.119.245.12	192.168.0.13	HTTP	591	HTTP/1.1 200 OK (text/html)

```
▶ Frame 1150: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface 0
▶ Ethernet II, Src: Apple_1d:a5:6e (a4:83:e7:1d:a5:6e), Dst: Technico_5e:c4:f0 (fc:52:8d:5e:c4:f0)
▶ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 51437, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
▼ Hypertext Transfer Protocol
  ▼ GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file3.html
      Request Version: HTTP/1.1
    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_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 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\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-file3.html]
    [HTTP request 1/1]
    [Response in frame: 1159]
```

13.

The response 200 OK message is in the Packet 1159.



Apply a display filter ... <⌘/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1144	38.862650	209.18.47.63	192.168.0.13	DNS	101	Standard query response 0x1611 A gaia.cs.umass.edu A 128.119.245.12
1145	38.866906	209.18.47.63	192.168.0.13	DNS	138	Standard query response 0x8d29 AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
1146	38.867216	192.168.0.13	128.119.245.12	TCP	78	51436 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=772496195 TSecr=0 SACK_PERM=
1147	38.867445	192.168.0.13	128.119.245.12	TCP	78	51437 → 80 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=772496195 TSecr=0 SACK_PERM=
1148	38.903843	128.119.245.12	192.168.0.13	TCP	82	80 → 51437 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3585703045 TSecr
1149	38.903905	192.168.0.13	128.119.245.12	TCP	66	51437 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=772496231 TSecr=3585703045
1150	38.904094	192.168.0.13	128.119.245.12	HTTP	530	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1151	38.904306	128.119.245.12	192.168.0.13	TCP	82	80 → 51436 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3585703045 TSecr
1152	38.904339	192.168.0.13	128.119.245.12	TCP	66	51436 → 80 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=772496231 TSecr=3585703045
1153	38.943972	128.119.245.12	192.168.0.13	TCP	74	80 → 51437 [ACK] Seq=1 Ack=465 Win=30080 Len=0 TSval=3585703086 TSecr=772496231
1154	38.945250	128.119.245.12	192.168.0.13	TCP	1522	80 → 51437 [ACK] Seq=1 Ack=465 Win=30080 Len=1448 TSval=3585703086 TSecr=772496231 [TCP segment of
1155	38.945281	128.119.245.12	192.168.0.13	TCP	1522	80 → 51437 [ACK] Seq=1449 Ack=465 Win=30080 Len=1448 TSval=3585703086 TSecr=772496231 [TCP segment
1156	38.945402	192.168.0.13	128.119.245.12	TCP	66	51437 → 80 [ACK] Seq=465 Ack=2897 Win=128832 Len=0 TSval=772496272 TSecr=3585703086
1157	38.945682	128.119.245.12	192.168.0.13	TCP	1522	80 → 51437 [ACK] Seq=2897 Ack=465 Win=30080 Len=1448 TSval=3585703086 TSecr=772496231 [TCP segment
1158	38.946746	192.168.0.13	128.119.245.12	TCP	66	51437 → 80 [ACK] Seq=465 Ack=4345 Win=131072 Len=0 TSval=772496273 TSecr=3585703086
1159	38.946832	128.119.245.12	192.168.0.13	HTTP	591	HTTP/1.1 200 OK (text/html)
1160	38.946884	192.168.0.13	128.119.245.12	TCP	66	51437 → 80 [ACK] Seq=465 Ack=4862 Win=130496 Len=0 TSval=772496273 TSecr=3585703088
1161	39.025662	192.168.0.1	224.0.0.1	IGMPv2	50	Membership Query, general
1162	39.026543	192.168.0.1	224.0.0.1	IGMPv3	54	Membership Query, general

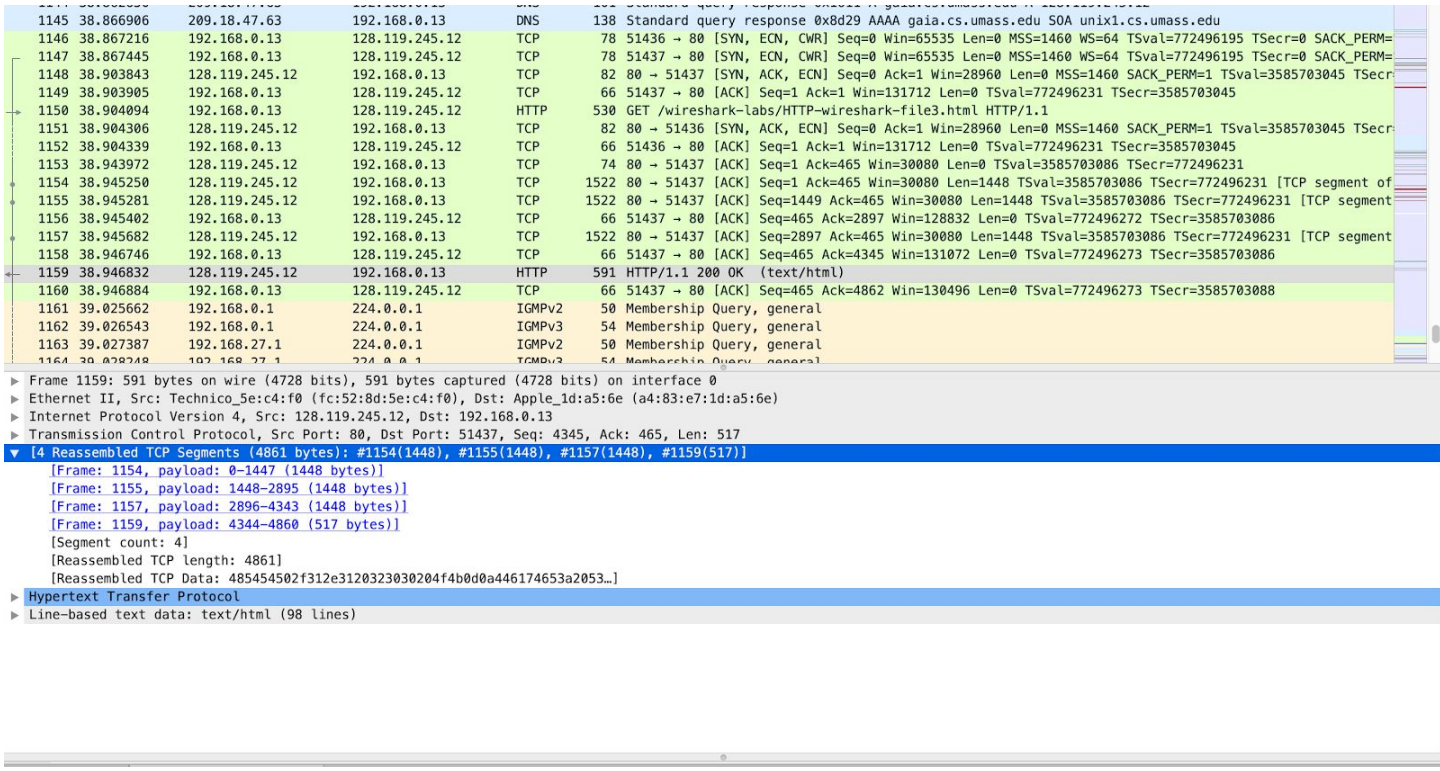
```
▶ Frame 1159: 591 bytes on wire (4728 bits), 591 bytes captured (4728 bits) on interface 0
▶ Ethernet II, Src: Technico_5e:c4:f0 (fc:52:8d:5e:c4:f0), Dst: Apple_1d:a5:6e (a4:83:e7:1d:a5:6e)
▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.13
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 51437, Seq: 4345, Ack: 465, Len: 517
▶ [4 Reassembled TCP Segments (4861 bytes): #1154(1448), #1155(1448), #1157(1448), #1159(517)]
▼ 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: Sat, 21 Sep 2019 01:50:12 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, 20 Sep 2019 05:59:02 GMT\r\n
    ETag: "1194-592f5c4559183"\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
```

14.

Status Code and phase in response is 200 OK.

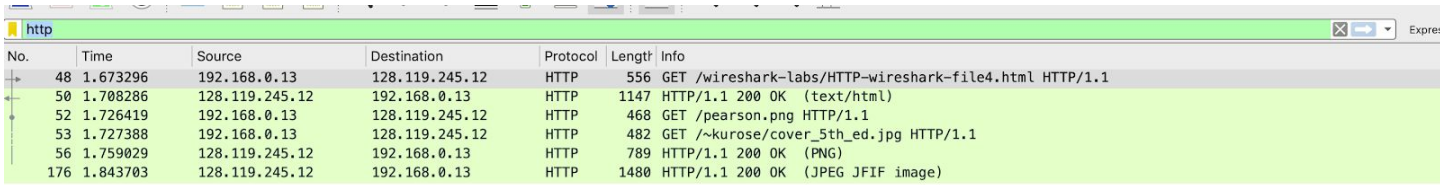
15.

4 TCP segments were needed to carry the data in the file.



16.

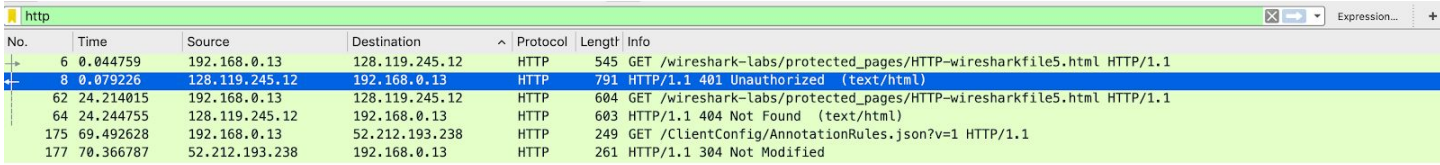
This time there are 3 GET requests. They are sent to addresses :
128.119.245.12
128.119.245.12
128.119.245.12



17.

I believe the 2 images are requested simultaneously as the images are requested together and then the 200 OK response comes one by one.

18. The server's response to the initial GET request is 401 Unauthorized.

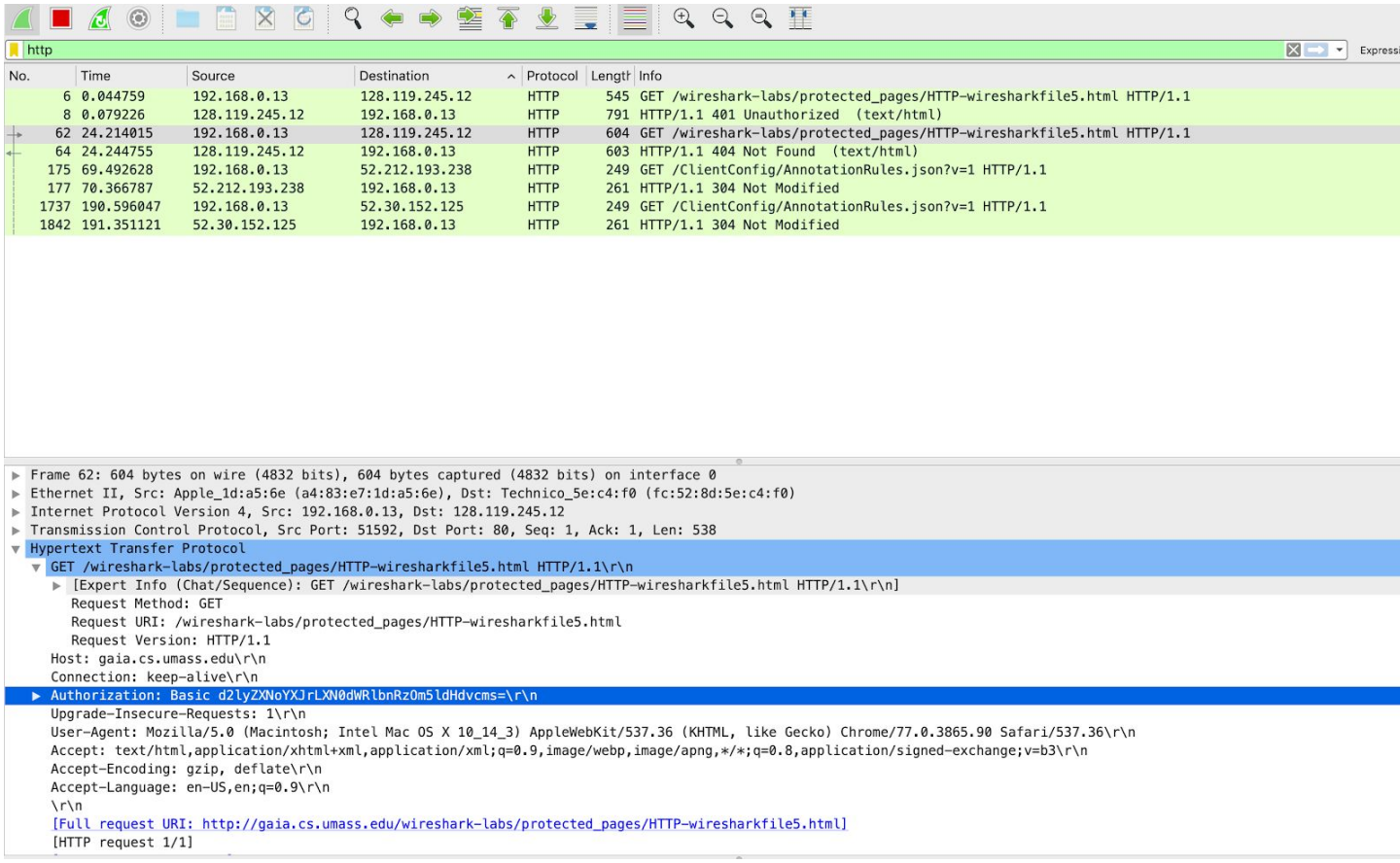


No.	Time	Source	Destination	Protocol	Length	Info
6	0.044759	192.168.0.13	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
8	0.079226	128.119.245.12	192.168.0.13	HTTP	791	HTTP/1.1 401 Unauthorized (text/html)
62	24.214015	192.168.0.13	128.119.245.12	HTTP	604	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
64	24.244755	128.119.245.12	192.168.0.13	HTTP	603	HTTP/1.1 404 Not Found (text/html)
175	69.492628	192.168.0.13	52.212.193.238	HTTP	249	GET /ClientConfig/AnnotationRules.json?v=1 HTTP/1.1
177	70.366787	52.212.193.238	192.168.0.13	HTTP	261	HTTP/1.1 304 Not Modified

19.

A new field that is requested in the next GET request:

Authorization Field



No.	Time	Source	Destination	Protocol	Length	Info
6	0.044759	192.168.0.13	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
8	0.079226	128.119.245.12	192.168.0.13	HTTP	791	HTTP/1.1 401 Unauthorized (text/html)
62	24.214015	192.168.0.13	128.119.245.12	HTTP	604	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
64	24.244755	128.119.245.12	192.168.0.13	HTTP	603	HTTP/1.1 404 Not Found (text/html)
175	69.492628	192.168.0.13	52.212.193.238	HTTP	249	GET /ClientConfig/AnnotationRules.json?v=1 HTTP/1.1
177	70.366787	52.212.193.238	192.168.0.13	HTTP	261	HTTP/1.1 304 Not Modified
1737	190.596047	192.168.0.13	52.30.152.125	HTTP	249	GET /ClientConfig/AnnotationRules.json?v=1 HTTP/1.1
1842	191.351121	52.30.152.125	192.168.0.13	HTTP	261	HTTP/1.1 304 Not Modified

```
▶ Frame 62: 604 bytes on wire (4832 bits), 604 bytes captured (4832 bits) on interface 0
▶ Ethernet II, Src: Apple_1d:a5:6e (a4:83:e7:1d:a5:6e), Dst: Technico_5e:c4:f0 (fc:52:8d:5e:c4:f0)
▶ Internet Protocol Version 4, Src: 192.168.0.13, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 51592, Dst Port: 80, Seq: 1, Ack: 1, Len: 538
▼ Hypertext Transfer Protocol
  ▼ GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 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\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/protected_pages/HTTP-wiresharkfile5.html]
    [HTTP request 1/1]
```