ECE361 – Computer Networks

Wireshark Lab 1: HTTP

First Name: Tianyi (Nora)   Last Name: Xu

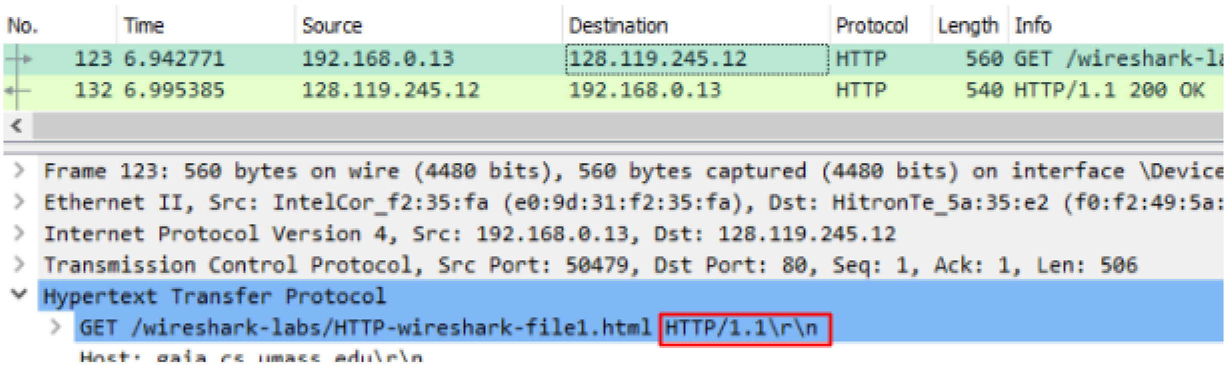
First Name: Yanyi (Will)   Last Name: Zhang

Group Details:

Student #: 1003130809 Student #: 1003327517

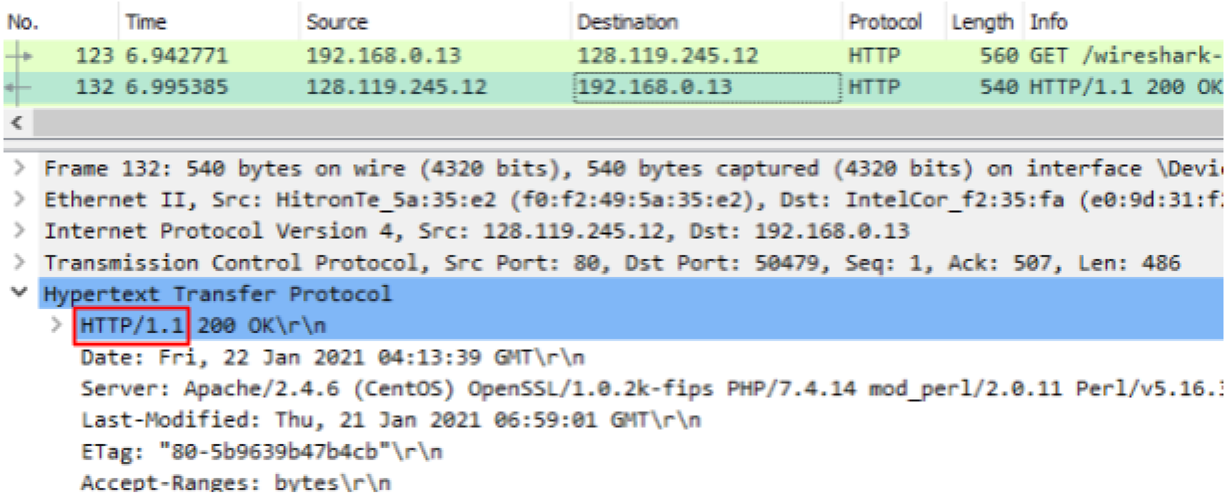
Mark:

	Question	Answer
1	Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?	My browser is running HTTP version 1.1 (Figure 1) The server is running HTTP version 1.1 (Figure 2)



```
No.    Time         Source          Destination      Protocol  Length  Info
  123  6.942771     192.168.0.13    128.119.245.12   HTTP         560  GET /wireshark-la
  132  6.995385     128.119.245.12  192.168.0.13     HTTP         540  HTTP/1.1 200 OK

> Frame 123: 560 bytes on wire (4480 bits), 560 bytes captured (4480 bits) on interface \Device
> Ethernet II, Src: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa), Dst: HitronTe_5a:35:e2 (f0:f2:49:5a:
> Internet Protocol Version 4, Src: 192.168.0.13, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50479, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
```

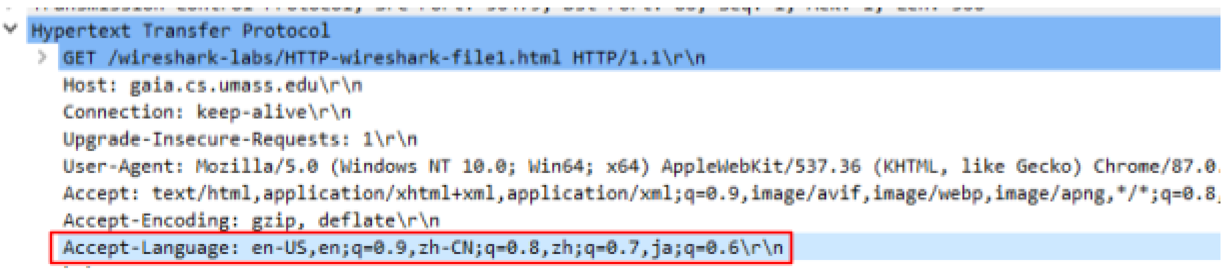
Figure 1



```
No.    Time         Source          Destination      Protocol  Length  Info
  123  6.942771     192.168.0.13    128.119.245.12   HTTP         560  GET /wireshark-
  132  6.995385     128.119.245.12  192.168.0.13     HTTP         540  HTTP/1.1 200 OK

> Frame 132: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Devi
> Ethernet II, Src: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2), Dst: IntelCor_f2:35:fa (e0:9d:31:f
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.13
> Transmission Control Protocol, Src Port: 80, Dst Port: 50479, Seq: 1, Ack: 507, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Fri, 22 Jan 2021 04:13:39 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.
    Last-Modified: Thu, 21 Jan 2021 06:59:01 GMT\r\n
    ETag: "80-5b9639b47b4cb"\r\n
    Accept-Ranges: bytes\r\n
```

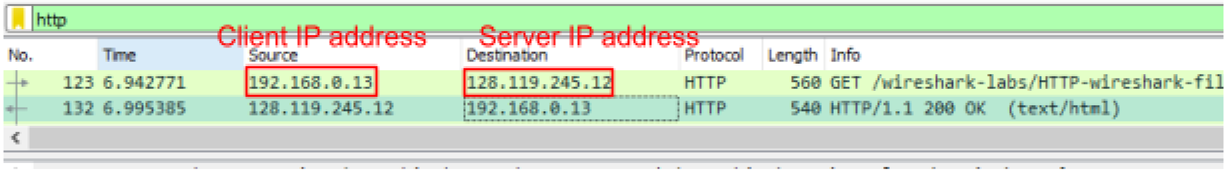
Figure 2

2	What languages (if any) does your browser indicate that it can accept to the server?	en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7, ja;q=0.6 English, Chinese, Japanese



```
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,ja;q=0.6\r\n
```

3	What is the IP address of your computer? Of the gaia.cs.umass.edu server?	IP address of my computer: 192.168.0.13 IP address of the server: 128.119.245.12

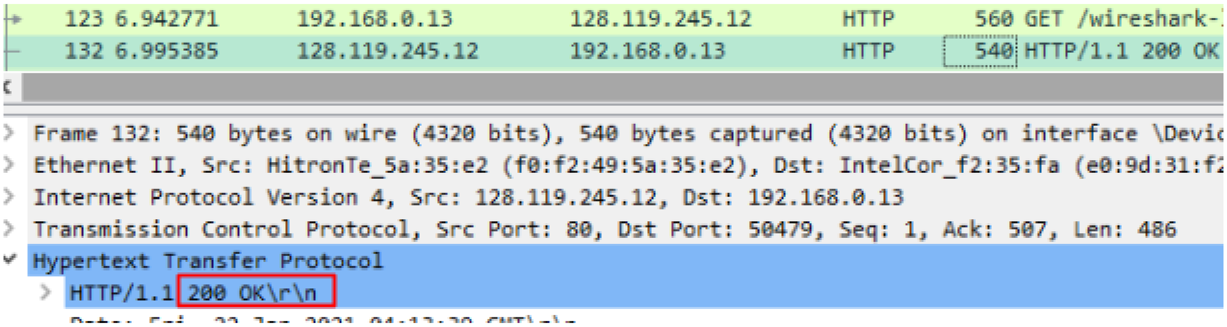


Client IP address

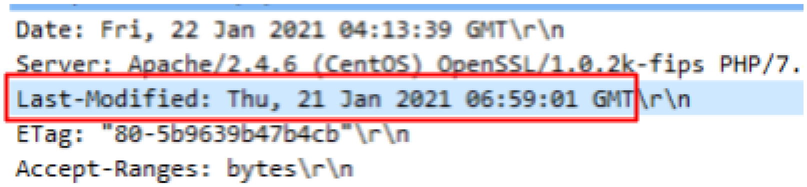
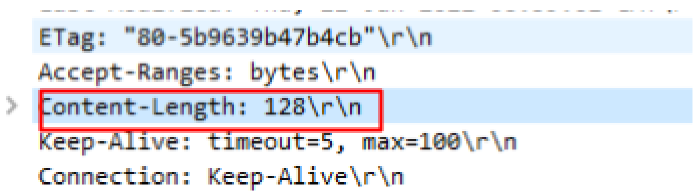
Server IP address

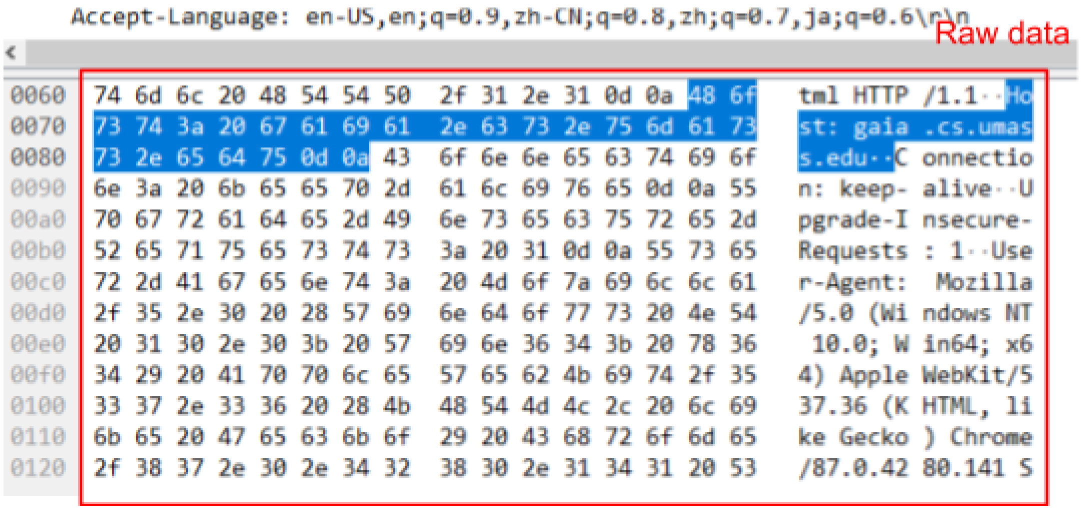
```
http
No.      Time       Source          Destination     Protocol  Length Info
   123 6.942771     192.168.0.13    128.119.245.12  HTTP         560 GET /wireshark-labs/HTTP-wireshark-fil
   132 6.995385     128.119.245.12  192.168.0.13    HTTP         540 HTTP/1.1 200 OK  (text/html)
```

4	What is the status code returned from the server to your browser?	200 OK



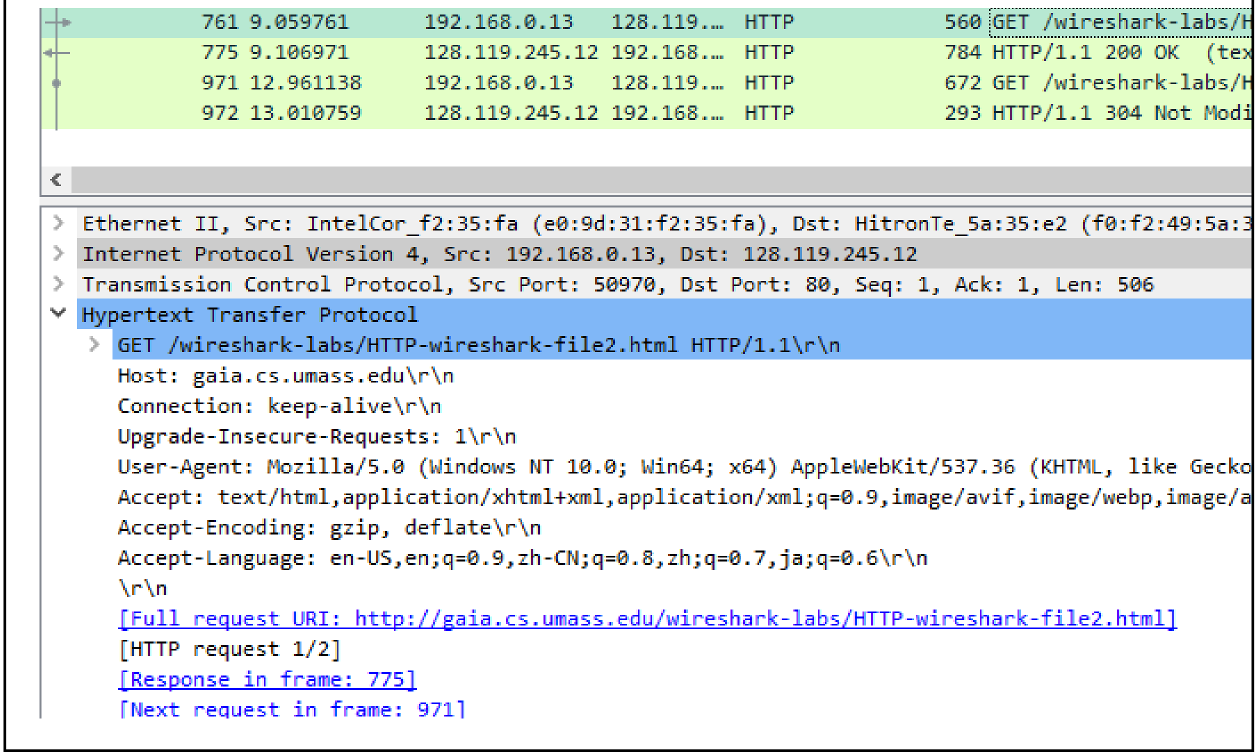
```
   123 6.942771     192.168.0.13     128.119.245.12    HTTP      560 GET /wireshark-
   132 6.995385     128.119.245.12   192.168.0.13      HTTP      540 HTTP/1.1 200 OK

> Frame 132: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Devic
> Ethernet II, Src: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2), Dst: IntelCor_f2:35:fa (e0:9d:31:f2
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.13
> Transmission Control Protocol, Src Port: 80, Dst Port: 50479, Seq: 1, Ack: 507, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
```

5	When was the HTML file that you are retrieving last modified at the server?	Thu, 21 Jan 2021 06:59:01 GMT
 Date: Fri, 22 Jan 2021 04:13:39 GMT\r\n Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7. Last-Modified: Thu, 21 Jan 2021 06:59:01 GMT\r\n ETag: "80-5b9639b47b4cb"\r\n Accept-Ranges: bytes\r\n		
6	How many bytes of content are being returned to your browser?	128 bytes
 ETag: "80-5b9639b47b4cb"\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		
7	By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.	No. all of the header can be found in raw data.

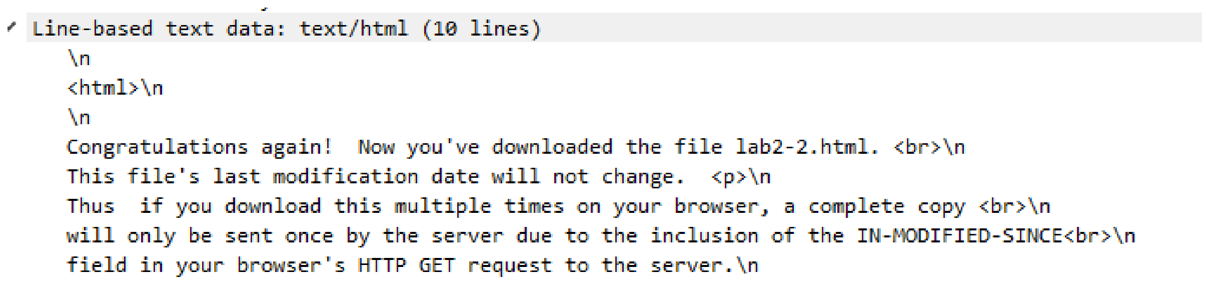
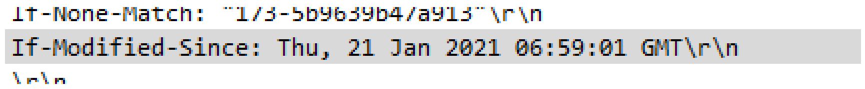


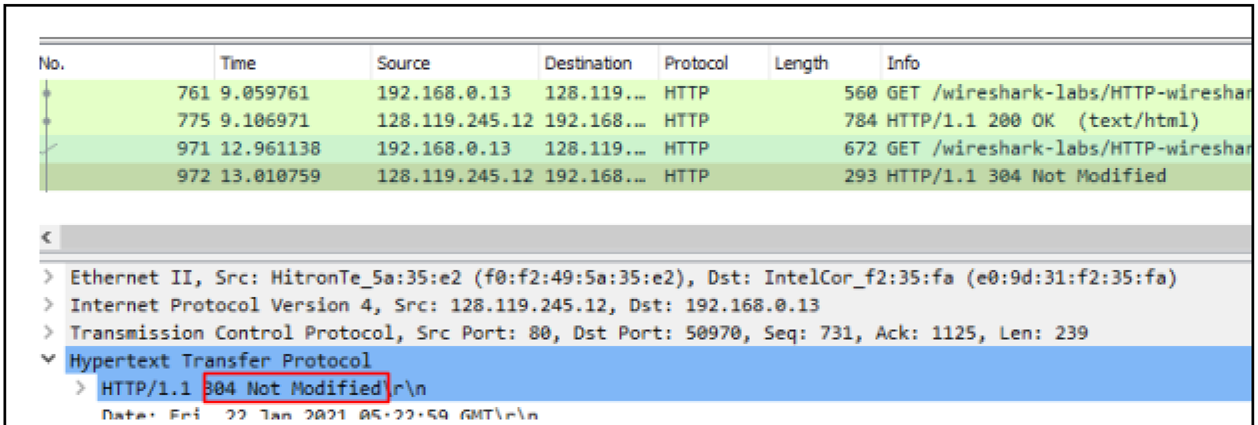
```
Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,ja;q=0.6\r\n
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00e0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00f0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
0100  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
0110  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
0120  2f 38 37 2e 30 2e 34 32  38 30 2e 31 34 31 20 53   /87.0.42 80.141 S
```

8	Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?	No.



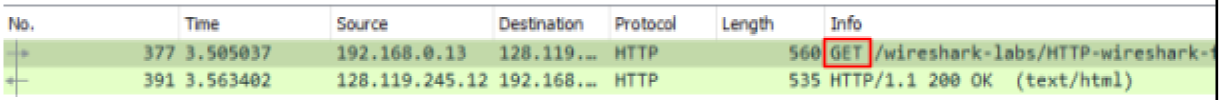
```
761 9.059761    192.168.0.13   128.119.…  HTTP   560 GET /wireshark-labs/H
775 9.106971    128.119.245.12 192.168.…  HTTP   784 HTTP/1.1 200 OK  (tex
971 12.961138   192.168.0.13   128.119.…  HTTP   672 GET /wireshark-labs/H
972 13.010759   128.119.245.12 192.168.…  HTTP   293 HTTP/1.1 304 Not Modi

> Ethernet II, Src: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa), Dst: HitronTe_5a:35:e2 (f0:f2:49:5a:3
> Internet Protocol Version 4, Src: 192.168.0.13, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50970, Dst Port: 80, Seq: 1, Ack: 1, Len: 506
v 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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7,ja;q=0.6\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: 775]
    [Next request in frame: 971]
```

9	Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?	Yes. The status code is 200 and we can see the content in line-based text data field.
 Line-based text data: text/html (10 lines) \n <html>\n \n Congratulations again! Now you've downloaded the file lab2-2.html.
\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
\n will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n field in your browser's HTTP GET request to the server.\n		
10	Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET? If so, what information follows the "IF-MODIFIED-SINCE:" header?	Yes. The information follows is "Thu, 21 Jan 2021 06:59:01 GMT", which is the last modification of the file from the previous get request
 If-None-Match: "173-5b9639b47a913"\r\n If-Modified-Since: Thu, 21 Jan 2021 06:59:01 GMT\r\n \r\n		
11	What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.	304 Not Modified. The server does not explicitly return the contents of the file since the web browser loaded it from its cache.



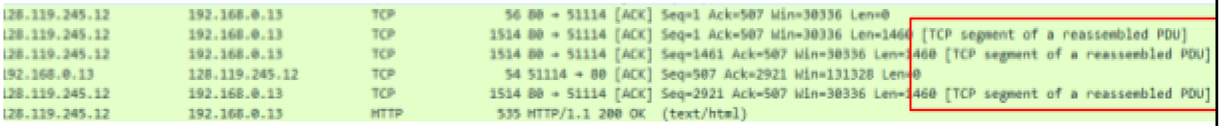
```
No.      Time          Source          Destination  Protocol  Length  Info
    761 9.059761      192.168.0.13    128.119...   HTTP         560 GET /wireshark-labs/HTTP-wireshar
    775 9.106971      128.119.245.12  192.168...   HTTP         784 HTTP/1.1 200 OK  (text/html)
    971 12.961138     192.168.0.13    128.119...   HTTP         672 GET /wireshark-labs/HTTP-wireshar
    972 13.010759     128.119.245.12  192.168...   HTTP         293 HTTP/1.1 304 Not Modified

> Ethernet II, Src: HitronTe_5a:35:e2 (f0:f2:49:5a:35:e2), Dst: IntelCor_f2:35:fa (e0:9d:31:f2:35:fa)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.0.13
> Transmission Control Protocol, Src Port: 80, Dst Port: 50970, Seq: 731, Ack: 1125, Len: 239
v Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 22 Jan 2021 05:22:59 GMT\r\n
```

12	How many HTTP GET request messages were sent by your browser?	1



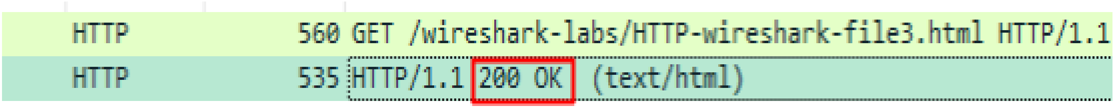
```
No.      Time          Source          Destination  Protocol  Length  Info
    377 3.505037      192.168.0.13    128.119...   HTTP         560 GET /wireshark-labs/HTTP-wireshark-f
    391 3.563402      128.119.245.12  192.168...   HTTP         535 HTTP/1.1 200 OK  (text/html)
```

13	How many data-containing TCP segments were needed to carry the single HTTP response?	3. Because we see 3 “[TCP segment of a reassembled PDU]” between the client’s GET request and the response from the server.



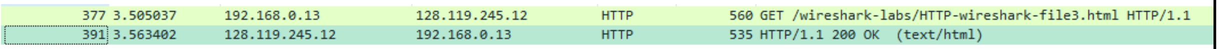
```
128.119.245.12   192.168.0.13     TCP     56 80 → 51114 [ACK] Seq=1 Ack=507 Win=30336 Len=0
128.119.245.12   192.168.0.13     TCP   1514 80 → 51114 [ACK] Seq=1 Ack=507 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
128.119.245.12   192.168.0.13     TCP   1514 80 → 51114 [ACK] Seq=1461 Ack=507 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
192.168.0.13     128.119.245.12   TCP     54 51114 → 80 [ACK] Seq=507 Ack=2921 Win=131328 Len=0
128.119.245.12   192.168.0.13     TCP   1514 80 → 51114 [ACK] Seq=2921 Ack=507 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
128.119.245.12   192.168.0.13     HTTP   535 HTTP/1.1 200 OK  (text/html)
```

14	What is the status code and phrase associated with the response to the HTTP GET request?	200 OK.

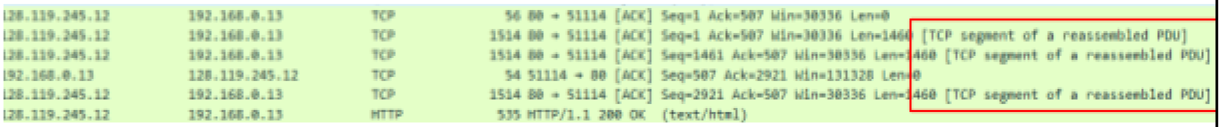


```
HTTP      560 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
HTTP      535 HTTP/1.1 200 OK  (text/html)
```

15	Are there any HTTP status lines in the transmitted data associated with a TCP induced “Continuation”?	No. It existed in the earlier version of wireshark and has been replaced by “TCP segment of reassembled PDU”

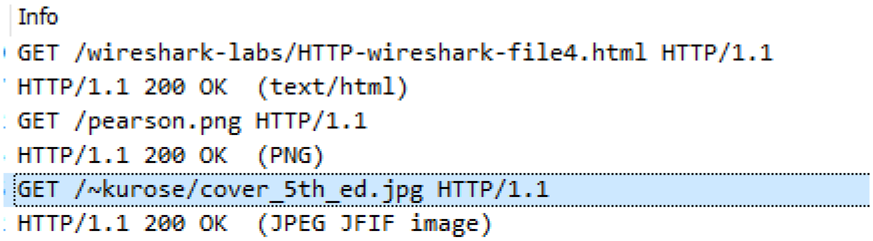


```
377 3.505037   192.168.0.13     128.119.245.12   HTTP   560 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
391 3.563402   128.119.245.12   192.168.0.13     HTTP   535 HTTP/1.1 200 OK  (text/html)
```

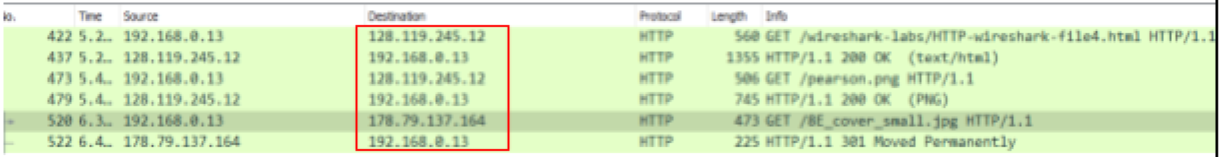


```
128.119.245.12   192.168.0.13     TCP     56 80 → 51114 [ACK] Seq=1 Ack=507 Win=30336 Len=0
128.119.245.12   192.168.0.13     TCP   1514 80 → 51114 [ACK] Seq=1 Ack=507 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
128.119.245.12   192.168.0.13     TCP   1514 80 → 51114 [ACK] Seq=1461 Ack=507 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
192.168.0.13     128.119.245.12   TCP     54 51114 → 80 [ACK] Seq=507 Ack=2921 Win=131328 Len=0
128.119.245.12   192.168.0.13     TCP   1514 80 → 51114 [ACK] Seq=2921 Ack=507 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
128.119.245.12   192.168.0.13     HTTP   535 HTTP/1.1 200 OK  (text/html)
```

16	How many HTTP GET request messages were sent by your browser? To which Internet addresses were these GET requests sent?	3 GET request messages are sent to the following addresses: 1. http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html (128.119.245.12) 2. http://gaia.cs.umass.edu/pearson.png (128.119.245.12) 3. http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg (178.79.137.164)

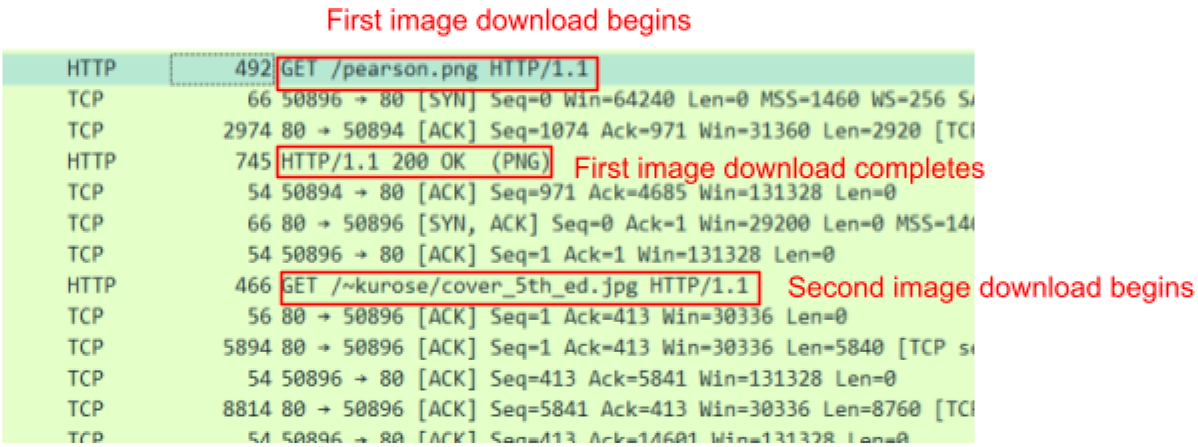


```
Info
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
HTTP/1.1 200 OK  (text/html)
GET /pearson.png HTTP/1.1
HTTP/1.1 200 OK  (PNG)
GET /~kurose/cover_5th_ed.jpg HTTP/1.1
HTTP/1.1 200 OK  (JPEG JFIF image)
```



```
No.  Time    Source            Destination       Protocol  Length  Info
422  5.2..   192.168.0.13      128.119.245.12    HTTP       560 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
437  5.2..   128.119.245.12    192.168.0.13      HTTP      1355 HTTP/1.1 200 OK  (text/html)
473  5.4..   192.168.0.13      128.119.245.12    HTTP       506 GET /pearson.png HTTP/1.1
479  5.4..   128.119.245.12    192.168.0.13      HTTP       745 HTTP/1.1 200 OK  (PNG)
520  6.3..   192.168.0.13      178.79.137.164    HTTP       473 GET /8E_cover_small.jpg HTTP/1.1
522  6.4..   178.79.137.164    192.168.0.13      HTTP       225 HTTP/1.1 301 Moved Permanently
```

17	Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.	The two images were downloaded serially. Because the second image’s GET request happened after the first image finished downloading.



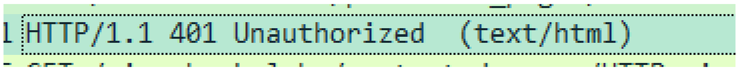
First image download begins

First image download completes

Second image download begins

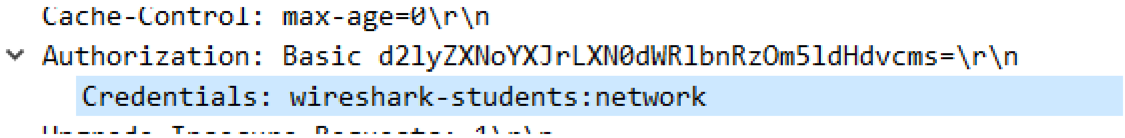
```
HTTP       492 GET /pearson.png HTTP/1.1
TCP         66 50896 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
TCP       2974 80 → 50894 [ACK] Seq=1074 Ack=971 Win=31360 Len=2920 [TC
HTTP       745 HTTP/1.1 200 OK  (PNG)
TCP         54 50894 → 80 [ACK] Seq=971 Ack=4685 Win=131328 Len=0
TCP         66 80 → 50896 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=14
TCP         54 50896 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
HTTP       466 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
TCP         56 80 → 50896 [ACK] Seq=1 Ack=413 Win=30336 Len=0
TCP       5894 80 → 50896 [ACK] Seq=1 Ack=413 Win=30336 Len=5840 [TCP s
TCP         54 50896 → 80 [ACK] Seq=413 Ack=5841 Win=131328 Len=0
TCP       8814 80 → 50896 [ACK] Seq=5841 Ack=413 Win=30336 Len=8760 [TC
TCP         54 50896 → 80 [ACK] Seq=413 Ack=14601 Win=131328 Len=0
```

18 (optional)	What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?	401 Unauthorized.



```
1 HTTP/1.1 401 Unauthorized  (text/html)
```

19 (optional)	When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?	Authorization and credentials



```
    Cache-Control: max-age=0\r\n
  ⌄ Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcms=\r\n
        Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
```