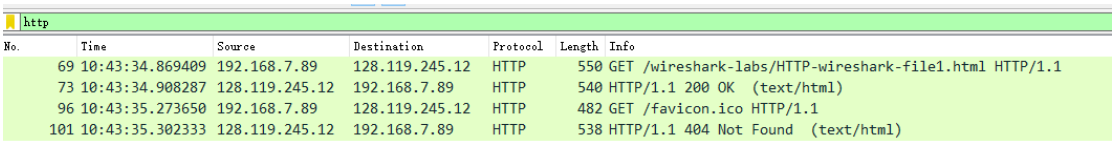
Lab HTTP

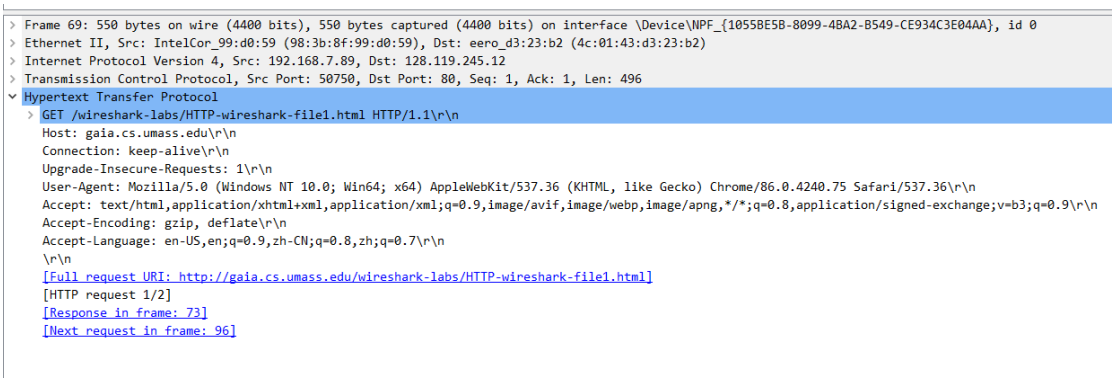
Ziqi Tan U 88387934

The Basic HTTP GET/response interaction

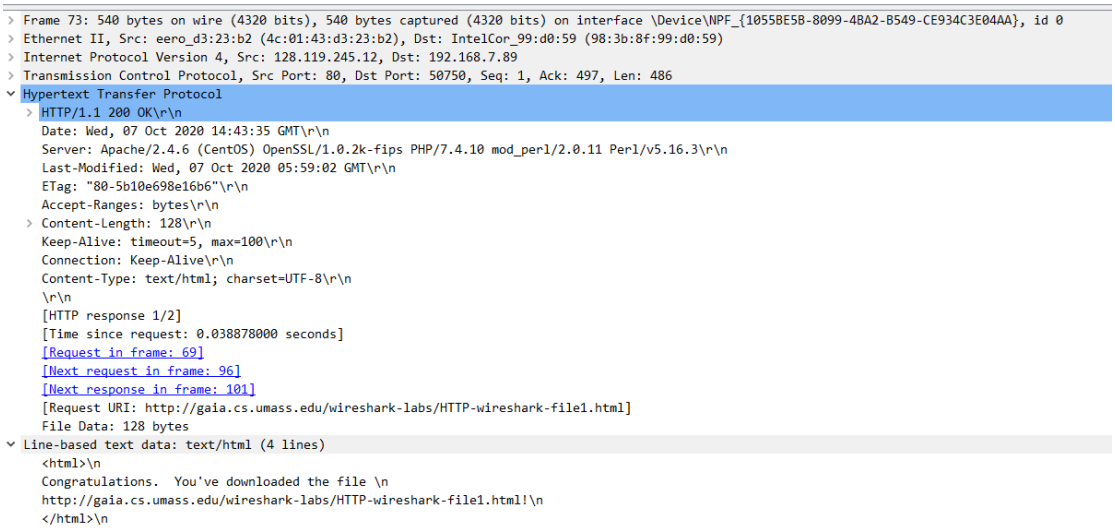


http

No.	Time	Source	Destination	Protocol	Length	Info
69	10:43:34.869409	192.168.7.89	128.119.245.12	HTTP	550	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
73	10:43:34.908287	128.119.245.12	192.168.7.89	HTTP	540	HTTP/1.1 200 OK (text/html)
96	10:43:35.273650	192.168.7.89	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
101	10:43:35.302333	128.119.245.12	192.168.7.89	HTTP	538	HTTP/1.1 404 Not Found (text/html)



```
> Frame 69: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
> Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: eero_d3:23:b2 (4c:01:43:d3:23:b2)
> Internet Protocol Version 4, Src: 192.168.7.89, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50750, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
v 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/86.0.4240.75 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 73]
    [Next request in frame: 96]
```



```
> Frame 73: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
> Ethernet II, Src: eero_d3:23:b2 (4c:01:43:d3:23:b2), Dst: IntelCor_99:d0:59 (98:3b:8f:99:d0:59)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.7.89
> Transmission Control Protocol, Src Port: 80, Dst Port: 50750, Seq: 1, Ack: 497, Len: 486
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 07 Oct 2020 14:43:35 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Oct 2020 05:59:02 GMT\r\n
    ETag: "80-5b10e698e16b6"\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 1/2]
    [Time since request: 0.038878000 seconds]
    [Request in frame: 69]
    [Next request in frame: 96]
    [Next response in frame: 101]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    File Data: 128 bytes
v Line-based text data: text/html (4 lines)
    <html>\n
    Congratulations.  You've downloaded the file \n
    http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
    </html>\n
```

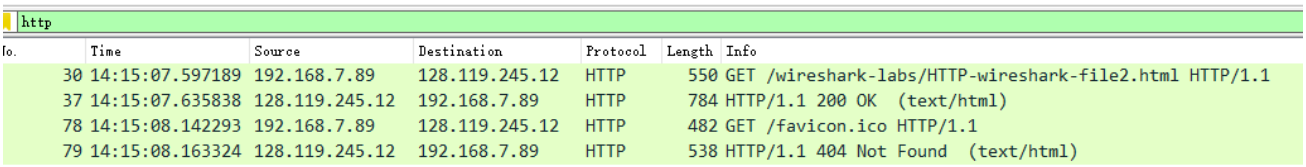
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

1. Browser: HTTP 1.1, Server: HTTP 1.1
2. Accepted language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
   English and Chinese.
   This is called a relative quality factor. It specifies what language the user would prefer, on a scale of 0 to 1.
3. IP address of my computer: 192.168.7.89, of the server: 128.119.245.12.
4. Status code returned from the server: 200.

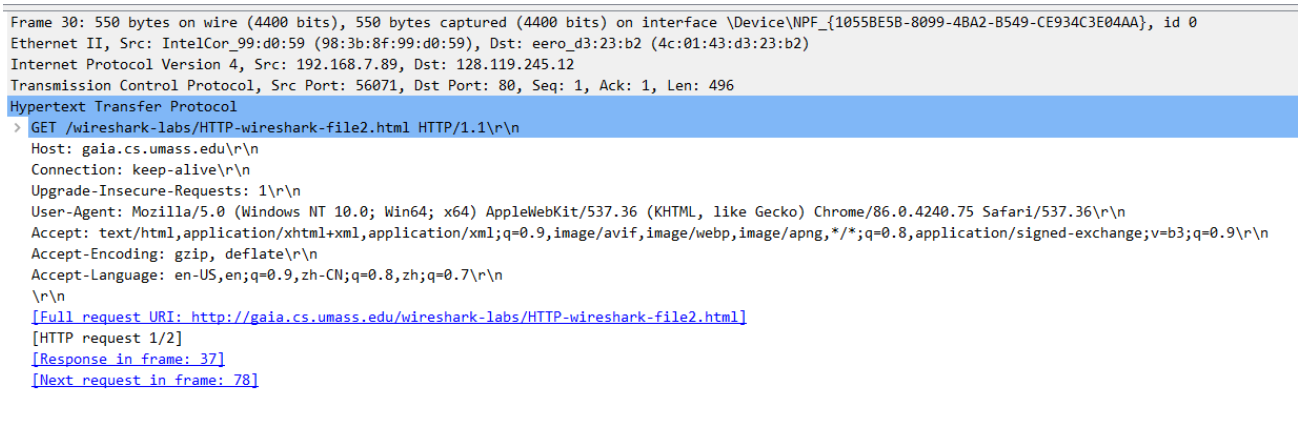
5. Last modified: Wed, 07 Oct 2020 05:59:02 GMT.
6. Content length: 128 bytes.
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
   For example: keep alive.

The HTTP CONDITIONAL GET/response interaction

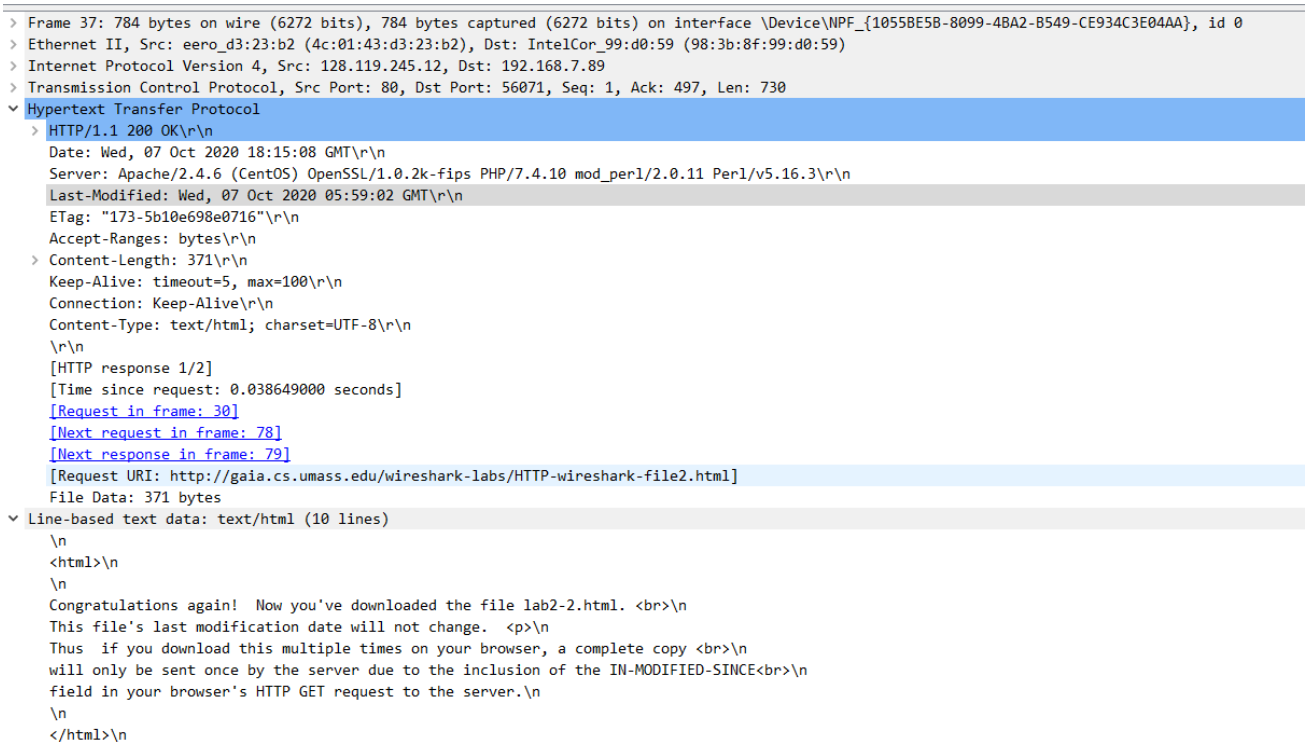
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html



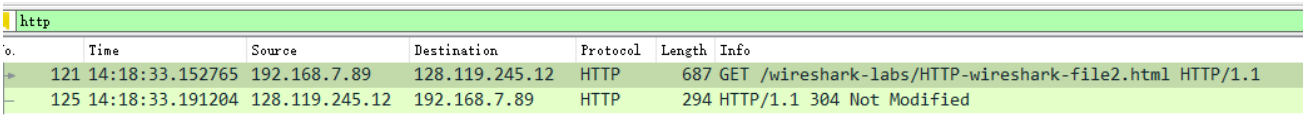
```
http
No.     Time           Source          Destination     Protocol Length Info
     30 14:15:07.597189 192.168.7.89    128.119.245.12  HTTP      550 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
     37 14:15:07.635838 128.119.245.12  192.168.7.89    HTTP      784 HTTP/1.1 200 OK  (text/html)
     78 14:15:08.142293 192.168.7.89    128.119.245.12  HTTP      482 GET /favicon.ico HTTP/1.1
     79 14:15:08.163324 128.119.245.12  192.168.7.89    HTTP      538 HTTP/1.1 404 Not Found  (text/html)
```



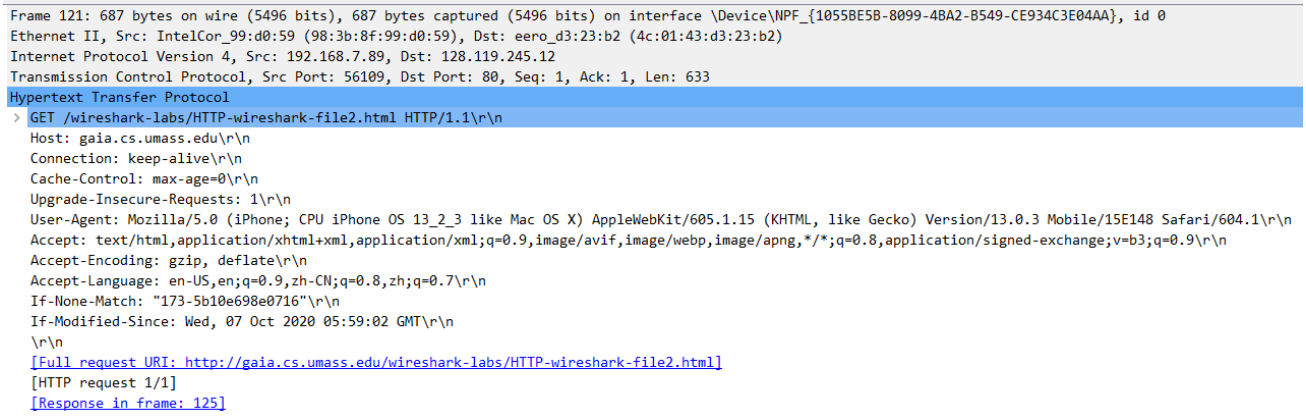
```
Frame 30: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: eero_d3:23:b2 (4c:01:43:d3:23:b2)
Internet Protocol Version 4, Src: 192.168.7.89, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56071, Dst Port: 80, Seq: 1, Ack: 1, Len: 496
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) Chrome/86.0.4240.75 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\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: 37]
  [Next request in frame: 78]
```



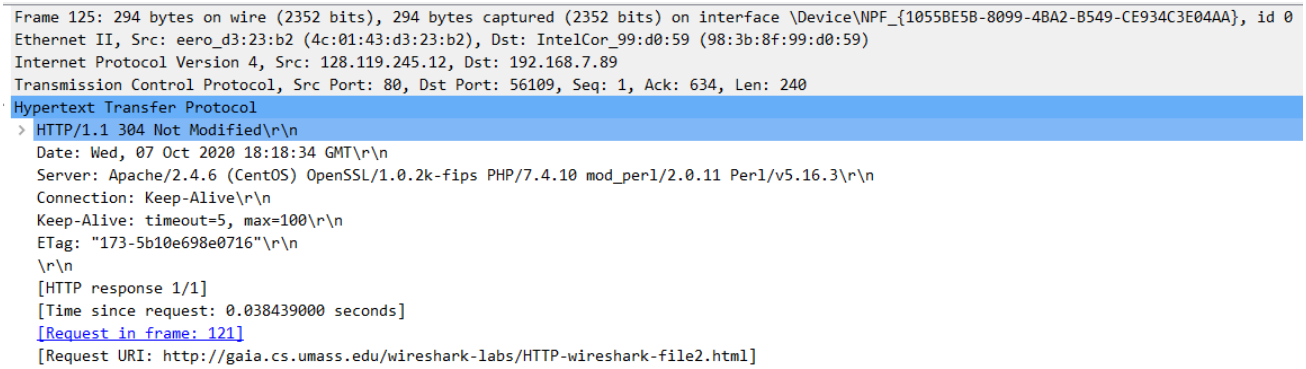
```
Frame 37: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: eero_d3:23:b2 (4c:01:43:d3:23:b2), Dst: IntelCor_99:d0:59 (98:3b:8f:99:d0:59)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.7.89
Transmission Control Protocol, Src Port: 80, Dst Port: 56071, Seq: 1, Ack: 497, Len: 730
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Wed, 07 Oct 2020 18:15:08 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Last-Modified: Wed, 07 Oct 2020 05:59:02 GMT\r\n
  ETag: "173-5b10e698e0716"\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: 0.038649000 seconds]
  [Request in frame: 30]
  [Next request in frame: 78]
  [Next response in frame: 79]
  [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
  \n
  </html>\n
```



No.	Time	Source	Destination	Protocol	Length	Info
121	14:18:33.152765	192.168.7.89	128.119.245.12	HTTP	687	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
125	14:18:33.191204	128.119.245.12	192.168.7.89	HTTP	294	HTTP/1.1 304 Not Modified



```
Frame 121: 687 bytes on wire (5496 bits), 687 bytes captured (5496 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: eero_d3:23:b2 (4c:01:43:d3:23:b2)
Internet Protocol Version 4, Src: 192.168.7.89, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56109, Dst Port: 80, Seq: 1, Ack: 1, Len: 633
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 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
  If-None-Match: "173-5b10e698e0716"\r\n
  If-Modified-Since: Wed, 07 Oct 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 1/1]
  [Response in frame: 125]
```

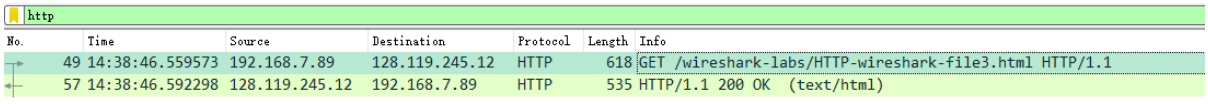


```
Frame 125: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: eero_d3:23:b2 (4c:01:43:d3:23:b2), Dst: IntelCor_99:d0:59 (98:3b:8f:99:d0:59)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.7.89
Transmission Control Protocol, Src Port: 80, Dst Port: 56109, Seq: 1, Ack: 634, Len: 240
Hypertext Transfer Protocol
> HTTP/1.1 304 Not Modified\r\n
  Date: Wed, 07 Oct 2020 18:18:34 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-5b10e698e0716"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.038439000 seconds]
  [Request in frame: 121]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

8. No “IF-MODIFIED-SINCE” line in the first http get request.
9. In the first http response, the server explicitly returned the contents of the file. We can see the line-base text data in the packet.
10. If-Modified-Since: Wed, 07 Oct 2020 05:59:02 GMT
11. 304 Not Modified. The server didn’t explicitly return the contents of the file. The server told the browser that the content was not modified and please use the cache content.

Retrieving Long Documents

http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html



No.	Time	Source	Destination	Protocol	Length	Info
49	14:38:46.559573	192.168.7.89	128.119.245.12	HTTP	618	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
57	14:38:46.592298	128.119.245.12	192.168.7.89	HTTP	535	HTTP/1.1 200 OK (text/html)

```
Frame 49: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: eero_d3:23:b2 (4c:01:43:d3:23:b2)
Internet Protocol Version 4, Src: 192.168.7.89, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56894, Dst Port: 80, Seq: 1, Ack: 1, Len: 564
Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\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: 57]
```

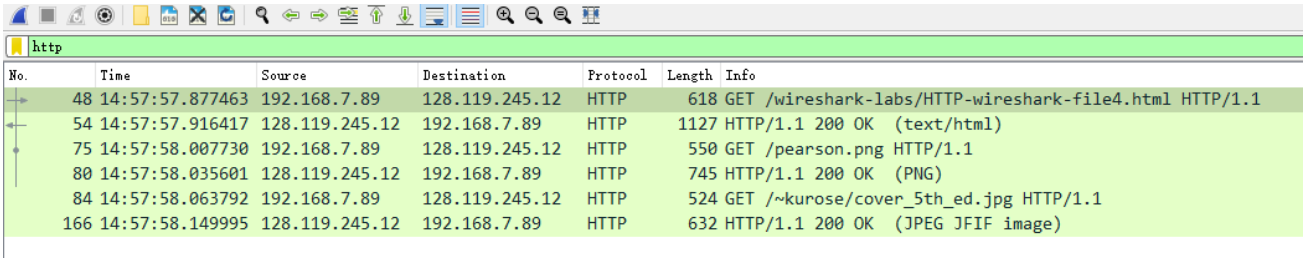
```
Frame 57: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: eero_d3:23:b2 (4c:01:43:d3:23:b2), Dst: IntelCor_99:d0:59 (98:3b:8f:99:d0:59)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.7.89
Transmission Control Protocol, Src Port: 80, Dst Port: 56894, Seq: 4381, Ack: 565, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #54(1460), #55(1460), #56(1460), #57(481)]
Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Wed, 07 Oct 2020 18:38:47 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.10 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Wed, 07 Oct 2020 05:59:02 GMT\r\n
    ETag: "1194-5b10e698dad3d"\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]
    [Time since request: 0.032725000 seconds]
    [Request in frame: 49]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
Line-based text data: text/html (98 lines)
    <html><head> \n
    <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
    \n
    \n
    <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
    <p><br>\n
    </p>\n
    <p></p><center><b>THE BILL OF RIGHTS</b><br>\n
      <em>Amendments 1-10 of the Constitution</em>\n
    </center>\n
    \n
    <p>The Conventions of a number of the States having, at the time of adopting\n
    the Constitution, expressed a desire, in order to prevent misconstruction\n
```

12. Only one http request was sent by my browser. Packet number is 49.
13. Number 57.
14. 200 OK.
15. 4 TCP segments were needed.

```
[4 Reassembled TCP Segments (4861 bytes): #54(1460), #55(1460), #56(1460), #57(481)]
  [Frame: 54, payload: 0-1459 (1460 bytes)]
  [Frame: 55, payload: 1460-2919 (1460 bytes)]
  [Frame: 56, payload: 2920-4379 (1460 bytes)]
  [Frame: 57, payload: 4380-4860 (481 bytes)]
  [Segment count: 4]
  [Reassembled TCP length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2057…]
```

HTML Documents with Embedded Objects

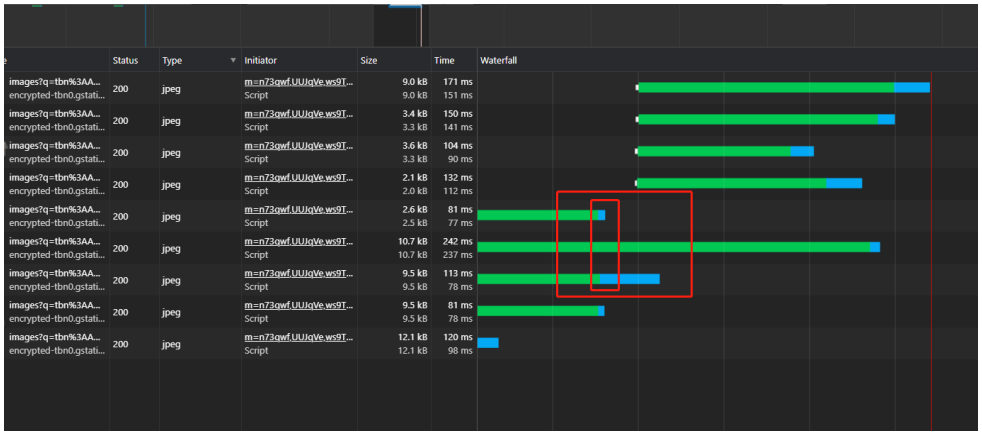
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html



http

No.	Time	Source	Destination	Protocol	Length	Info
48	14:57:57.877463	192.168.7.89	128.119.245.12	HTTP	618	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
54	14:57:57.916417	128.119.245.12	192.168.7.89	HTTP	1127	HTTP/1.1 200 OK (text/html)
75	14:57:58.007730	192.168.7.89	128.119.245.12	HTTP	550	GET /pearson.png HTTP/1.1
80	14:57:58.035601	128.119.245.12	192.168.7.89	HTTP	745	HTTP/1.1 200 OK (PNG)
84	14:57:58.063792	192.168.7.89	128.119.245.12	HTTP	524	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
166	14:57:58.149995	128.119.245.12	192.168.7.89	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)

16. The browser sent 3 http request.
    They were sent to 192.119.245.12.
17. They were downloaded in serial, but actually they may download in parallel (See the second waterfall image). Let's see the waterfall in Chrome developer tool. The blue part represents content download. The blue part of these two images didn't overlap. They may overlap sometimes.



```
> Frame 48: 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
> Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: eero_d3:23:b2 (4c:01:43:d3:23:b2)
> Internet Protocol Version 4, Src: 192.168.7.89, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 57851, Dst Port: 80, Seq: 1, Ack: 1, Len: 564
v 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
    Pragma: no-cache\r\n
    Cache-Control: no-cache\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_2_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.3 Mobile/15E148 Safari/604.1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\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: 54]
    [Next request in frame: 75]
```

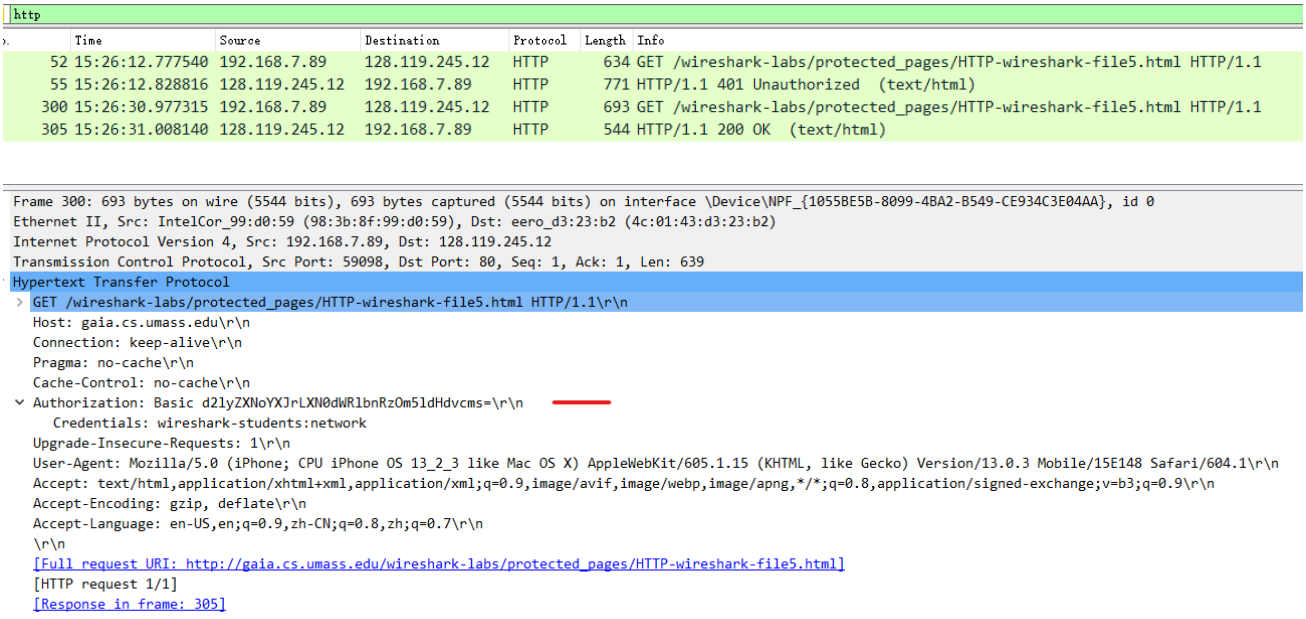
```
Frame 75: 550 bytes on wire (4400 bits), 550 bytes captured (4400 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: eero_d3:23:b2 (4c:01:43:d3:23:b2)
Internet Protocol Version 4, Src: 192.168.7.89, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57851, Dst Port: 80, Seq: 565, Ack: 1074, Len: 496
  Source Port: 57851
  Destination Port: 80
  [Stream index: 6]
  [TCP Segment Len: 496]
  Sequence number: 565    (relative sequence number)
  Sequence number (raw): 3459306576
  [Next sequence number: 1061    (relative sequence number)]
  Acknowledgment number: 1074    (relative ack number)
  Acknowledgment number (raw): 1236301743
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
  Window size value: 509
  [Calculated window size: 130304]
  [Window size scaling factor: 256]
  Checksum: 0x3f90 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
  TCP payload (496 bytes)
Hypertext Transfer Protocol
```

```
Frame 84: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface \Device\NPF_{1055BE5B-8099-4BA2-B549-CE934C3E04AA}, id 0
Ethernet II, Src: IntelCor_99:d0:59 (98:3b:8f:99:d0:59), Dst: eero_d3:23:b2 (4c:01:43:d3:23:b2)
Internet Protocol Version 4, Src: 192.168.7.89, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57853, Dst Port: 80, Seq: 1, Ack: 1, Len: 470
  Source Port: 57853
  Destination Port: 80
  [Stream index: 8]
  [TCP Segment Len: 470]
  Sequence number: 1    (relative sequence number)
  Sequence number (raw): 1883010655
  [Next sequence number: 471    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  Acknowledgment number (raw): 2274468219
  0101 .... = Header Length: 20 bytes (5)
> Flags: 0x018 (PSH, ACK)
  Window size value: 513
  [Calculated window size: 131328]
  [Window size scaling factor: 256]
  Checksum: 0x3f76 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
> [SEQ/ACK analysis]
> [Timestamps]
  TCP payload (470 bytes)
Hypertext Transfer Protocol
```

HTTP Authentication

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

The username is “wireshark-students” (without the quotes), and the password is “network” (again, without the quotes).



18. Firstly, the server tells us 401 Unauthroized.
19. The second request includes the Authorization field.

Note:

The username (wireshark-students) and password (network) that you entered are encoded in the string of characters (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=) following the “Authorization: Basic” header in the client’s HTTP GET message. While it may appear that your username and password are encrypted, they are simply encoded in a format known as Base64 format. The username and password are not encrypted!