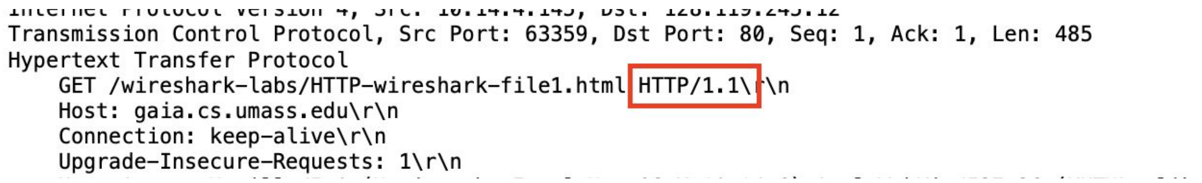
20132927_정재명_ wireshark_lab2_HTTP

1. The Basic HTTP GET/response interaction

1.Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

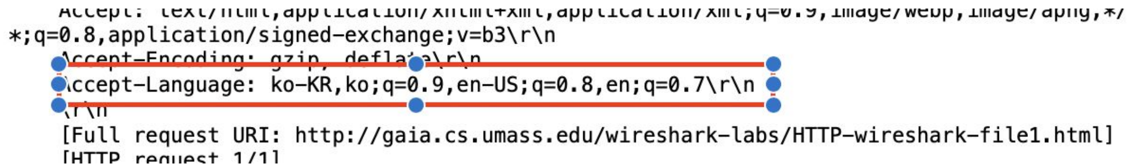
-> 1.1 version



```
Internet Protocol Version 4, Src: 10.14.4.145, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63359, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
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
```

2.What languages (if any) does your browser indicate that it can accept to the server?

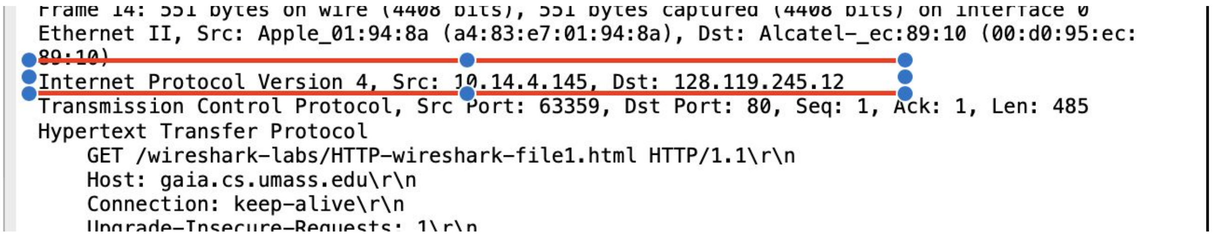
-> 한국어, 영어.



```
    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: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
```

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

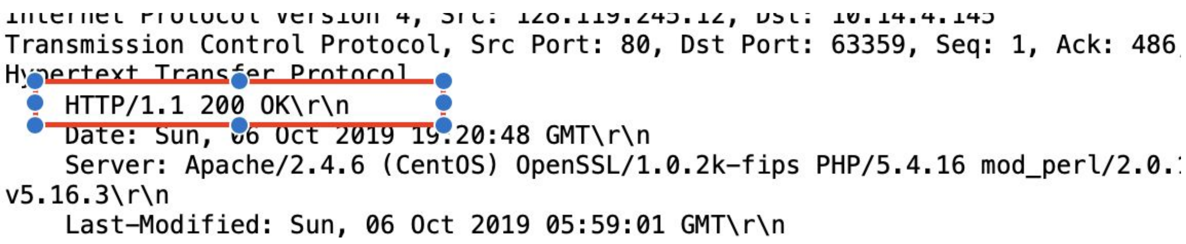
-> Me : 10.14.4.145 / gaia.cs.umass.edu : 128.119.245.12



```
Frame 14: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface 0
Ethernet II, Src: Apple_01:94:8a (a4:83:e7:01:94:8a), Dst: Alcatel-_ec:89:10 (00:d0:95:ec:
89:10)
Internet Protocol Version 4, Src: 10.14.4.145, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63359, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
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
```

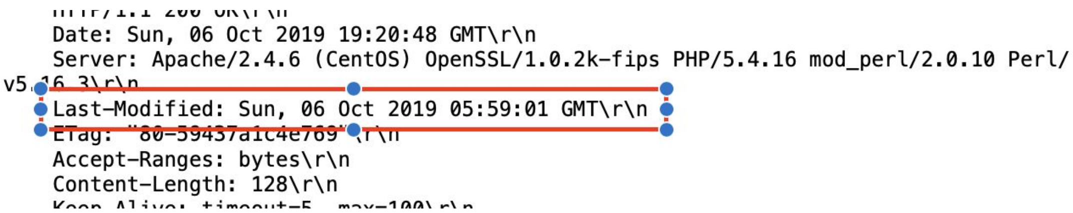
4.What is the status code returned from the server to your browser?

-> 200 / OK



```
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.14.4.145
Transmission Control Protocol, Src Port: 80, Dst Port: 63359, Seq: 1, Ack: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sun, 06 Oct 2019 19:20:48 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.
v5.16.3\r\n
    Last-Modified: Sun, 06 Oct 2019 05:59:01 GMT\r\n
```

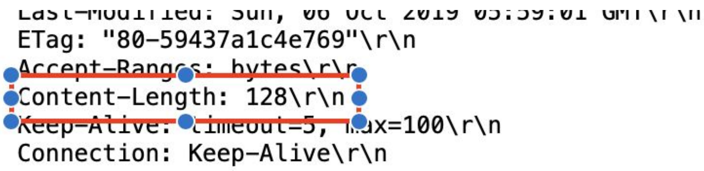
5.When was the HTML file that you are retrieving last modified at the server?



```
    HTTP/1.1 200 OK\r\n
    Date: Sun, 06 Oct 2019 19:20:48 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: Sun, 06 Oct 2019 05:59:01 GMT\r\n
    ETag: "80-59437a1c4e769"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
```

6.How many bytes of content are being returned to your browser?

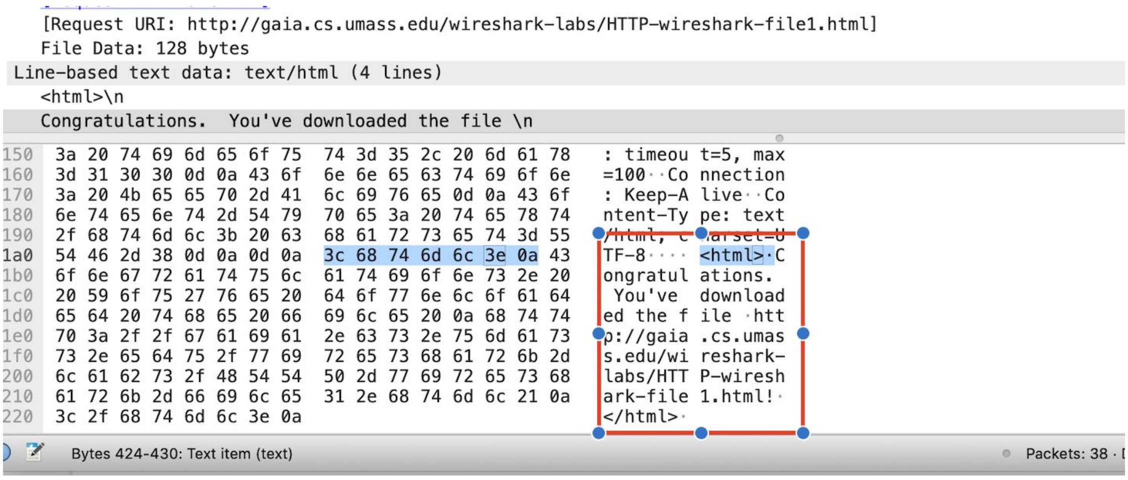
-> 128



```
Last-Modified: Sun, 06 Oct 2019 05:59:01 GMT\r\n
ETag: "80-59437a1c4e769"\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.

-> entity body

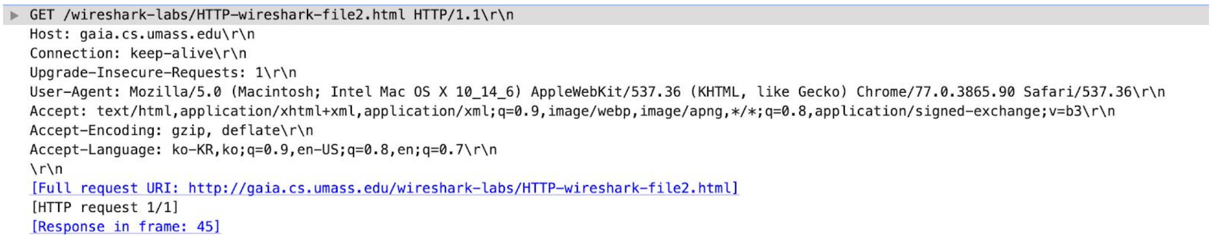


```
   [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
   File Data: 128 bytes
 Line-based text data: text/html (4 lines)
   <html>\n
   Congratulations.  You've downloaded the file \n

150  3a 20 74 69 6d 65 6f 75  74 3d 35 2c 20 6d 61 78   : timeou t=5, max
160  3d 31 30 30 0d 0a 43 6f  6e 6e 65 63 74 69 6f 6e   =100··Co nnection
170  3a 20 4b 65 65 70 2d 41  6c 69 76 65 0d 0a 43 6f   : Keep-A live··Co
180  6e 74 65 6e 74 2d 54 79  70 65 3a 20 74 65 78 74   ntent-Ty pe: text
190  2f 68 74 6d 6c 3b 20 63  68 61 72 73 65 74 3d 55   /html; c harset=U
1a0  54 46 2d 38 0d 0a 0d 0a  3c 68 74 6d 6c 3e 0a 43   TF-8···· <html>·C
1b0  6f 6e 67 72 61 74 75 6c  61 74 69 6f 6e 73 2e 20   ongratul ations.
1c0  20 59 6f 75 27 76 65 20  64 6f 77 6e 6c 6f 61 64    You've  download
1d0  65 64 20 74 68 65 20 66  69 6c 65 20 0a 68 74 74   ed the f ile ·htt
1e0  70 3a 2f 2f 67 61 69 61  2e 63 73 2e 75 6d 61 73   p://gaia .cs.umas
1f0  73 2e 65 64 75 2f 77 69  72 65 73 68 61 72 6b 2d   s.edu/wi reshark-
200  6c 61 62 73 2f 48 54 54  50 2d 77 69 72 65 73 68   labs/HTT P-wiresh
210  61 72 6b 2d 66 69 6c 65  31 2e 68 74 6d 6c 21 0a   ark-file 1.html!·
220  3c 2f 68 74 6d 6c 3e 0a                            </html>·

Bytes 424-430: Text item (text)                                    Packets: 38 ·
```

2. The HTTP CONDITIONAL GET/response interaction

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?

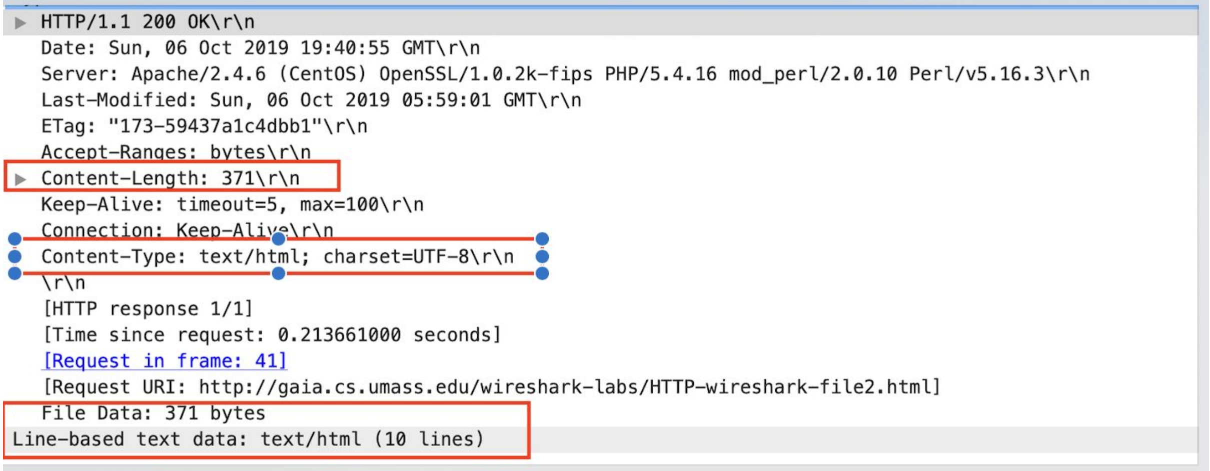
-> 찾을 수 없다.



```
▶ 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/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: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\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: 45]
```

9.Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

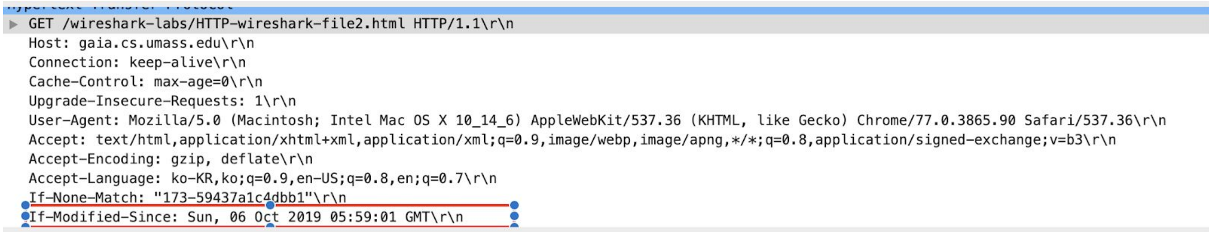
-> 파일을 보냈다. 아래와 같이 파일을 받았다는 정보가 함께 왔다.



```
▶ HTTP/1.1 200 OK\r\n
  Date: Sun, 06 Oct 2019 19:40:55 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: Sun, 06 Oct 2019 05:59:01 GMT\r\n
  ETag: "173-59437a1c4dbb1"\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: 0.213661000 seconds]
  [Request in frame: 41]
  [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)
```

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?

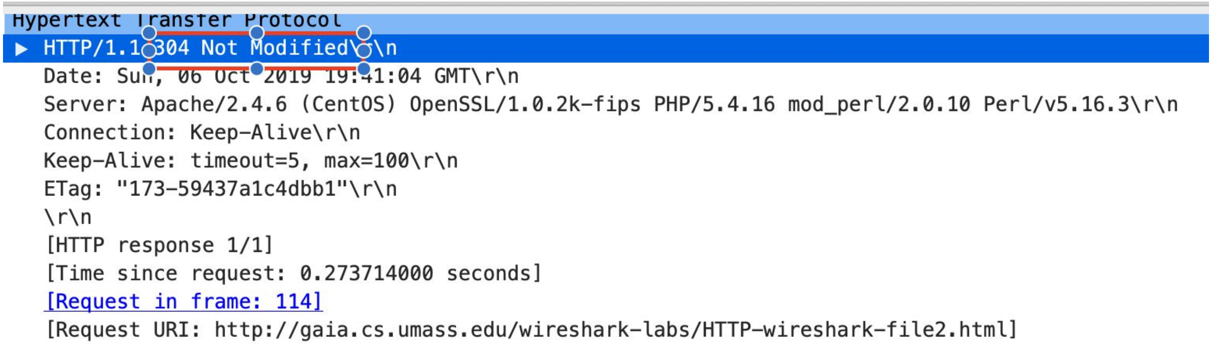
-> 처음에 서버가 보내준 객체가 수정된 날짜와 일치한다면 파일을 재전송하지 않아도 된다는 의미다.



```
▶ 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/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: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  If-None-Match: "173-59437a1c4dbb1"\r\n
  If-Modified-Since: Sun, 06 Oct 2019 05:59:01 GMT\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.

-> 이 때 서버는 응답 코드 304 / Not Modified를 보낸다. 이것은 파일이 수정되지 않았으니 재전송 하지 않았음을 의미한다. 실제로 아무것도 보내준 파일이 없다.



```
Hypertext Transfer Protocol
▶ HTTP/1.1 304 Not Modified\r\n
  Date: Sun, 06 Oct 2019 19:41:04 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
  Connection: Keep-Alive\r\n
  Keep-Alive: timeout=5, max=100\r\n
  ETag: "173-59437a1c4dbb1"\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.273714000 seconds]
  [Request in frame: 114]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

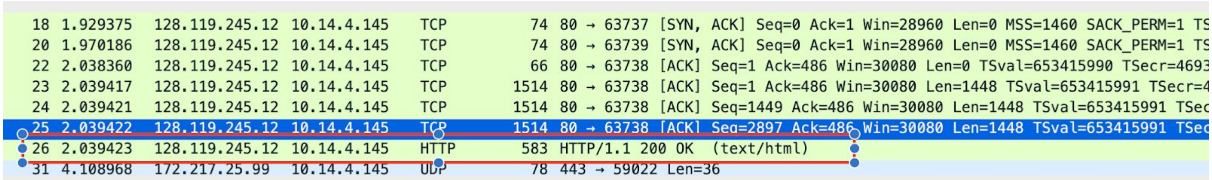
3. Retrieving Long Documents

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

-> 1개의 GET 메세지를 보냈다. 이 안에 the Bill or Rights에 대한 요청도 함께 담겨 있다.

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

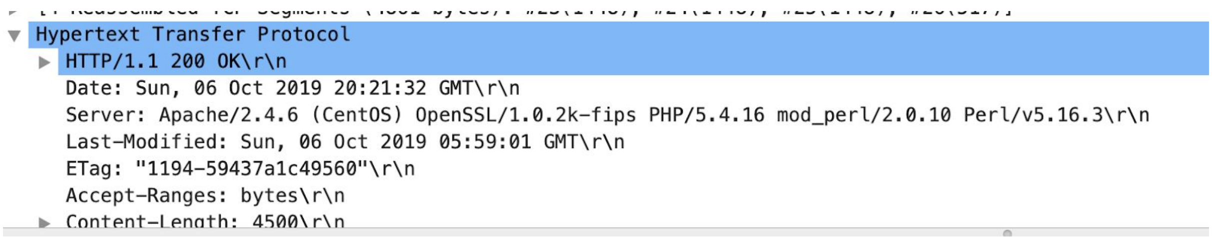
-> 사진 상에서 26번째 패킷에 해당 정보가 담겨 있다.



```
 18 1.929375   128.119.245.12 10.14.4.145    TCP         74 80 → 63737 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
 20 1.970186   128.119.245.12 10.14.4.145    TCP         74 80 → 63739 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TS
 22 2.038360   128.119.245.12 10.14.4.145    TCP         66 80 → 63738 [ACK] Seq=1 Ack=486 Win=30080 Len=0 TSval=653415990 TSecr=4693
 23 2.039417   128.119.245.12 10.14.4.145    TCP       1514 80 → 63738 [ACK] Seq=1 Ack=486 Win=30080 Len=1448 TSval=653415991 TSecr=4
 24 2.039421   128.119.245.12 10.14.4.145    TCP       1514 80 → 63738 [ACK] Seq=1449 Ack=486 Win=30080 Len=1448 TSval=653415991 TSec
 25 2.039422   128.119.245.12 10.14.4.145    TCP       1514 80 → 63738 [ACK] Seq=2897 Ack=486 Win=30080 Len=1448 TSval=653415991 TSec
 26 2.039423   128.119.245.12 10.14.4.145    HTTP       583 HTTP/1.1 200 OK  (text/html)
 31 4.108968   172.217.25.99  10.14.4.145    UDP         78 443 → 59022 Len=36
```

14. What is the status code and phrase in the response?

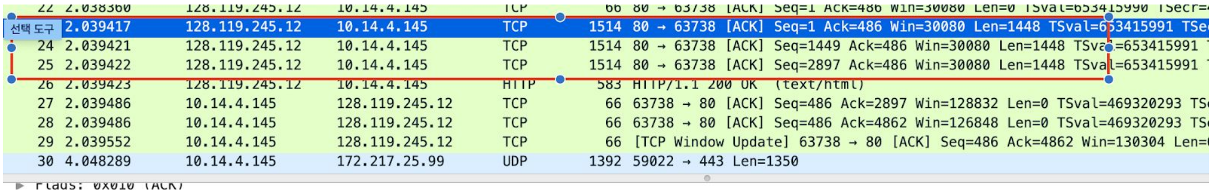
-> 200 / OK



```
▶ [4 Reassembled TCP Segments (4861 bytes): #23(1448), #24(1448), #25(1448), #26(517)]
▼ Hypertext Transfer Protocol
  ▶ HTTP/1.1 200 OK\r\n
    Date: Sun, 06 Oct 2019 20:21:32 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: Sun, 06 Oct 2019 05:59:01 GMT\r\n
    ETag: "1194-59437a1c49560"\r\n
    Accept-Ranges: bytes\r\n
  ▶ Content-Length: 4500\r\n
```

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

-> 각각 1448 바이트 씩, 3개의 TCP 세그먼트로 나눠서 전송되었다.

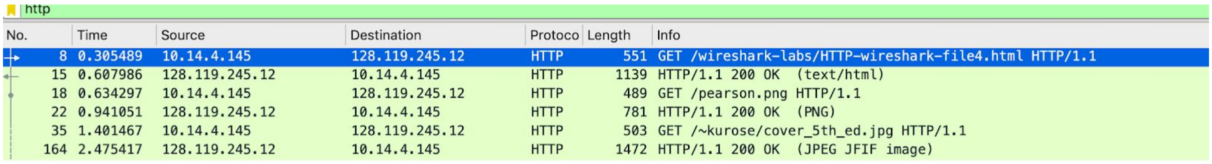


```
 22 2.038360   128.119.245.12   10.14.4.145      TCP       66 80 → 63738 [ACK] Seq=1 Ack=486 Win=30080 Len=0 TSval=653415990 TSecr=
선택 도구 2.039417   128.119.245.12   10.14.4.145      TCP     1514 80 → 63738 [ACK] Seq=1 Ack=486 Win=30080 Len=1448 TSval=653415991 TSe
 24 2.039421   128.119.245.12   10.14.4.145      TCP     1514 80 → 63738 [ACK] Seq=1449 Ack=486 Win=30080 Len=1448 TSval=653415991
 25 2.039422   128.119.245.12   10.14.4.145      TCP     1514 80 → 63738 [ACK] Seq=2897 Ack=486 Win=30080 Len=1448 TSval=653415991
 26 2.039423   128.119.245.12   10.14.4.145      HTTP     583 HTTP/1.1 200 OK  (text/html)
 27 2.039486   10.14.4.145      128.119.245.12   TCP       66 63738 → 80 [ACK] Seq=486 Ack=2897 Win=128832 Len=0 TSval=469320293 TS
 28 2.039486   10.14.4.145      128.119.245.12   TCP       66 63738 → 80 [ACK] Seq=486 Ack=4862 Win=126848 Len=0 TSval=469320293 TS
 29 2.039552   10.14.4.145      128.119.245.12   TCP       66 [TCP Window Update] 63738 → 80 [ACK] Seq=486 Ack=4862 Win=130304 Len=
 30 4.048289   10.14.4.145      172.217.25.99    UDP     1392 59022 → 443 Len=1350
▶ Flags: 0x010 (ACK)
```

4. HTML Documents with Embedded Objects

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

-> 세 개의 GET 요청 메세지를 보냈다. 모두 128.245.12로 요청을 보냈다.

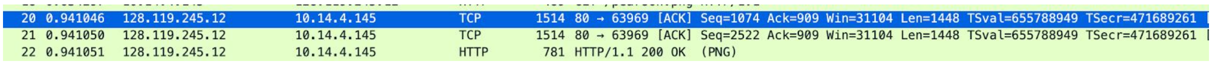


```
http
No.   Time       Source           Destination      Protoco Length Info
    8 0.305489   10.14.4.145      128.119.245.12   HTTP     551 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
   15 0.607986   128.119.245.12   10.14.4.145      HTTP    1139 HTTP/1.1 200 OK  (text/html)
   18 0.634297   10.14.4.145      128.119.245.12   HTTP     489 GET /pearson.png HTTP/1.1
   22 0.941051   128.119.245.12   10.14.4.145      HTTP     781 HTTP/1.1 200 OK  (PNG)
   35 1.401467   10.14.4.145      128.119.245.12   HTTP     503 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
  164 2.475417   128.119.245.12   10.14.4.145      HTTP    1472 HTTP/1.1 200 OK  (JPEG JFIF image)
```

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

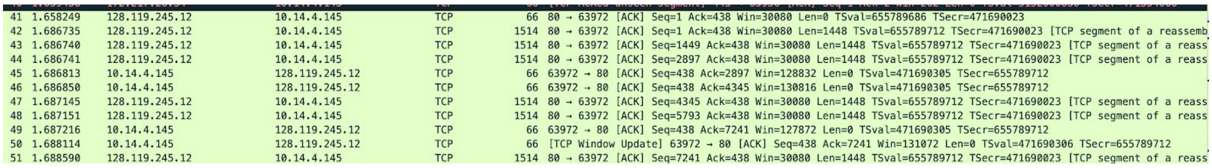
-> 순서대로 받았다. 포트 번호를 보면, 첫번째 사진을 전송하는 프로세스와 두번째 사진을 전송하는 프로세스가 다른 것을 알 수 있다.

-> 첫 번째 사진파일



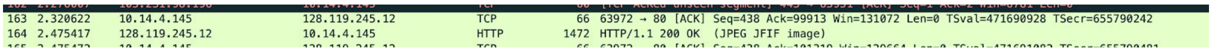
```
20 0.941046   128.119.245.12   10.14.4.145   TCP    1514 80 → 63969 [ACK] Seq=1074 Ack=909 Win=31104 Len=1448 TSval=655788949 TSecr=471689261 [
21 0.941050   128.119.245.12   10.14.4.145   TCP    1514 80 → 63969 [ACK] Seq=2522 Ack=909 Win=31104 Len=1448 TSval=655788949 TSecr=471689261 [
22 0.941051   128.119.245.12   10.14.4.145   HTTP    781 HTTP/1.1 200 OK  (PNG)
```

-> 두 번째 사진파일



```
41 1.658249   128.119.245.12   10.14.4.145      TCP     66 80 → 63972 [ACK] Seq=1 Ack=438 Win=30080 Len=0 TSval=655789686 TSecr=471690023
42 1.686735   128.119.245.12   10.14.4.145      TCP   1514 80 → 63972 [ACK] Seq=1 Ack=438 Win=30080 Len=1448 TSval=655789712 TSecr=471690023 [TCP segment of a reassemb
43 1.686740   128.119.245.12   10.14.4.145      TCP   1514 80 → 63972 [ACK] Seq=1449 Ack=438 Win=30080 Len=1448 TSval=655789712 TSecr=471690023 [TCP segment of a reass
44 1.686741   128.119.245.12   10.14.4.145      TCP   1514 80 → 63972 [ACK] Seq=2897 Ack=438 Win=30080 Len=1448 TSval=655789712 TSecr=471690023 [TCP segment of a reass
45 1.686813   10.14.4.145      128.119.245.12   TCP     66 63972 → 80 [ACK] Seq=438 Ack=2897 Win=128832 Len=0 TSval=471690305 TSecr=655789712
46 1.686850   10.14.4.145      128.119.245.12   TCP     66 63972 → 80 [ACK] Seq=438 Ack=4345 Win=130816 Len=0 TSval=471690305 TSecr=655789712
47 1.687145   128.119.245.12   10.14.4.145      TCP   1514 80 → 63972 [ACK] Seq=4345 Ack=438 Win=30080 Len=1448 TSval=655789712 TSecr=471690023 [TCP segment of a reass
48 1.687151   128.119.245.12   10.14.4.145      TCP   1514 80 → 63972 [ACK] Seq=5793 Ack=438 Win=30080 Len=1448 TSval=655789712 TSecr=471690023 [TCP segment of a reass
49 1.687216   10.14.4.145      128.119.245.12   TCP     66 63972 → 80 [ACK] Seq=438 Ack=7241 Win=127872 Len=0 TSval=471690305 TSecr=655789712
50 1.688114   10.14.4.145      128.119.245.12   TCP     66 [TCP Window Update] 63972 → 80 [ACK] Seq=438 Ack=7241 Win=131072 Len=0 TSval=471690306 TSecr=655789712
51 1.688590   128.119.245.12   10.14.4.145      TCP   1514 80 → 63972 [ACK] Seq=7241 Ack=438 Win=30080 Len=1448 TSval=655789712 TSecr=471690023 [TCP segment of a reass
```

- 생략 -

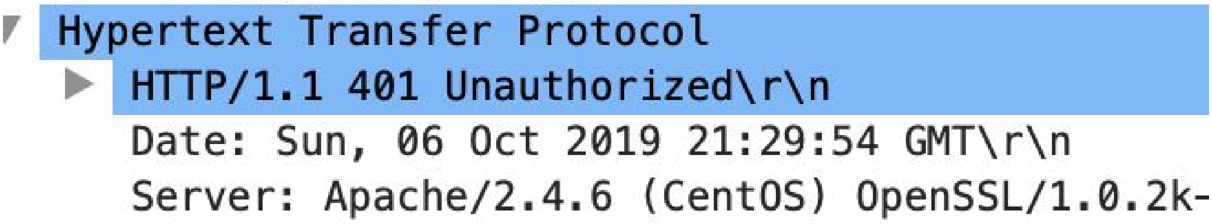


```
163 2.320622   10.14.4.145      128.119.245.12   TCP     66 63972 → 80 [ACK] Seq=438 Ack=99913 Win=131072 Len=0 TSval=471690928 TSecr=655790242
164 2.475417   128.119.245.12   10.14.4.145      HTTP  1472 HTTP/1.1 200 OK  (JPEG JFIF image)
```

5 HTTP Authentication

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

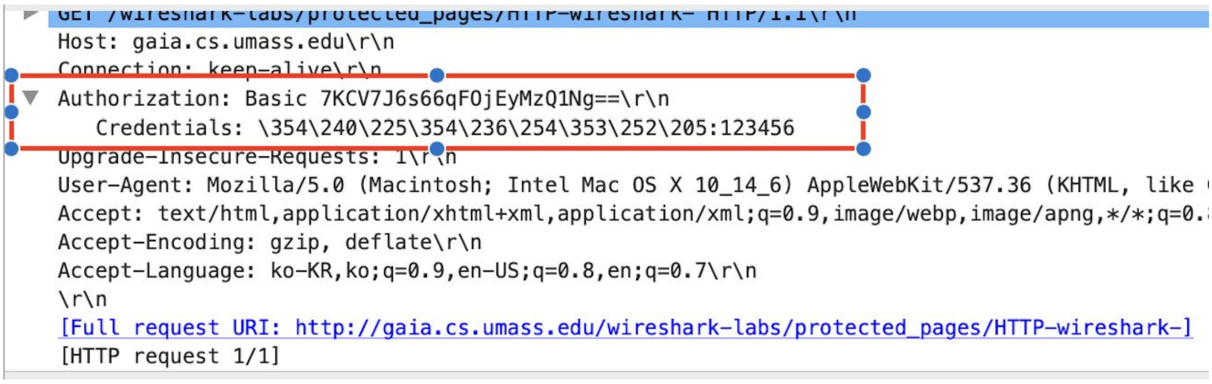
-> 401 / Unauthorized



```
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
  Date: Sun, 06 Oct 2019 21:29:54 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-
```

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

-> Authorization 항목이 추가 되었다.



```
▶ GET /wireshark-labs/protected_pages/HTTP-wireshark- HTTP/1.1\r\n
  Host: gaia.cs.umass.edu\r\n
  Connection: keep-alive\r\n
▼ Authorization: Basic 7KCV7J6s66qFOjEyMzQ1Ng==\r\n
     Credentials: \354\240\225\354\236\254\353\252\205:123456
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-]
  [HTTP request 1/1]
```