MARMARA UNIVERSITY

FACULTY OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
DEPARTMENT

CSE4074
COMPUTER NETWORKS
Homework #1

A. Tunahan Cinsoy
150117062

1. The Basic HTTP GET/response interaction

Q1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

```
No.     Time              Source              Destination          Protocol Length Info
    70 18:29:05.805630    192.168.1.33        128.119.245.12       HTTP     584    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 70: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: Dell_bf:27:89 (50:9a:4c:bf:27:89), Dst: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b)
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52720, Dst Port: 80, Seq: 1, Ack: 1, Len: 530
Hypertext Transfer Protocol
No.     Time              Source              Destination          Protocol Length Info
    81 18:29:05.939825    128.119.245.12      192.168.1.33         HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 81: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b), Dst: Dell_bf:27:89 (50:9a:4c:bf:27:89)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.33
Transmission Control Protocol, Src Port: 80, Dst Port: 52720, Seq: 1, Ack: 531, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
```

My browser and server both run HTTP version of 1.1

Q2. What languages (if any) does your browser indicate that it can accept to the server?

```
No.     Time              Source              Destination          Protocol Length Info
    70 18:29:05.805630    192.168.1.33        128.119.245.12       HTTP     584    GET /wireshark-labs/HTTP-wireshark-file1.htm
HTTP/1.1
Frame 70: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: Dell_bf:27:89 (50:9a:4c:bf:27:89), Dst: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b)
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52720, Dst Port: 80, Seq: 1, Ack: 1, Len: 530
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/86.0.4240.198 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: tr-TR,tr;q=0.9,en-GB;q=0.8,en;q=0.7,de-DE;q=0.6,de;q=0.5,en-US;q=0.4\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 81]
```

My browser accepts Turkish, English (GB), German and English (US)

Q3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

```
No.     Time            Source              Destination         Protocol Length Info
    70 18:29:05.805630   192.168.1.33        128.119.245.12      HTTP     584    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 70: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: Dell_bf:27:89 (50:9a:4c:bf:27:89), Dst: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b)
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52720, Dst Port: 80, Seq: 1, Ack: 1, Len: 530
Hypertext Transfer Protocol
No.     Time            Source              Destination         Protocol Length Info
    81 18:29:05.939825   128.119.245.12      192.168.1.33        HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 81: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b), Dst: Dell_bf:27:89 (50:9a:4c:bf:27:89)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.33
Transmission Control Protocol, Src Port: 80, Dst Port: 52720, Seq: 1, Ack: 531, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
```

The IP address of my computer is 192.168.1.33 and the IP address of the server is 128.119.245.12

Q4. What is the status code returned from the server to your browser?

```
No.     Time            Source              Destination         Protocol Length Info
    70 18:29:05.805630   192.168.1.33        128.119.245.12      HTTP     584    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 70: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: Dell_bf:27:89 (50:9a:4c:bf:27:89), Dst: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b)
Internet Protocol Version 4, Src: 192.168.1.33, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52720, Dst Port: 80, Seq: 1, Ack: 1, Len: 530
Hypertext Transfer Protocol
No.     Time            Source              Destination         Protocol Length Info
    81 18:29:05.939825   128.119.245.12      192.168.1.33        HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 81: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b), Dst: Dell_bf:27:89 (50:9a:4c:bf:27:89)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.33
Transmission Control Protocol, Src Port: 80, Dst Port: 52720, Seq: 1, Ack: 531, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
```

The status code that has returned from server to my browser is 200 OK

Q5. When was the HTML file that you are retrieving last modified at the server?

```
No.     Time           Source               Destination          Protocol Length Info
     81 18:29:05.939825  128.119.245.12       192.168.1.33         HTTP     540   HTTP/1.1 200 OK  (text/html)
Frame 81: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b), Dst: Dell_bf:27:89 (50:9a:4c:bf:27:89)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.33
Transmission Control Protocol, Src Port: 80, Dst Port: 52720, Seq: 1, Ack: 531, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 16 Nov 2020 15:29:05 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 16 Nov 2020 06:59:02 GMT\r\n
    ETag: "80-5b433e9d02541"\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 1/1]
    [Time since request: 0.134195000 seconds]
    [Request in frame: 70]
    [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)
```

The file was last modified on Monday, 16 November 2020 06:59:02 GMT

Q6. How many bytes of content are being returned to your browser?

```
No.     Time           Source               Destination          Protocol Length Info
     81 18:29:05.939825  128.119.245.12       192.168.1.33         HTTP     540   HTTP/1.1 200 OK  (text/html)
Frame 81: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{47757726-300E-4107-
B849-4D6627335A75}, id 0
Ethernet II, Src: HuaweiTe_1d:33:5b (80:13:82:1d:33:5b), Dst: Dell_bf:27:89 (50:9a:4c:bf:27:89)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.33
Transmission Control Protocol, Src Port: 80, Dst Port: 52720, Seq: 1, Ack: 531, Len: 486
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Mon, 16 Nov 2020 15:29:05 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Mon, 16 Nov 2020 06:59:02 GMT\r\n
    ETag: "80-5b433e9d02541"\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 1/1]
    [Time since request: 0.134195000 seconds]
    [Request in frame: 70]
    [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)
```

128 bytes of content are being returned from server to my browser

Q7. 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.

I didn't see any header that is not displayed in the packet-listing window.

2. The HTTP CONDITONAL GET/response interaction

Q8. 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?

```
∨ 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/86.0.4240.198 Safari/537.36\r\
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-GB;q=0.8,en;q=0.7,de-DE;q=0.6,de;q=0.5,en-US;q=0.4\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: 36]
```

No, there isn't an "IF-MODIFED-SINCE" line in first HTTP GET Request.

Q9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

```
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.139844000 seconds]
    [Request in frame: 28]
    [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
```

Yes, the server explicitly returned the contents of the file under the section called "Line-based text data"

Q10. 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?

```
˅ 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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36\
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-GB;q=0.8,en;q=0.7,de-DE;q=0.6,de;q=0.5,en-US;q=0.4\r\n
    If-None-Match: "173-5b433e9d011b9"\r\n
    If-Modified-Since: Mon, 16 Nov 2020 06:59:02 GMT\r\n    ◂━━━━━
    \r\n
```

Yes, there is an "IF-MODIFIED-SINCE" line in the second HTTP GET request. Information that follows that header is the access date and time.

Q11. 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.

```
˅ Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n    ◂━━━━━
    Date: Mon, 16 Nov 2020 16:14:41 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.12 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: "173-5b433e9d011b9"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.150973000 seconds]
    [Request in frame: 446]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```
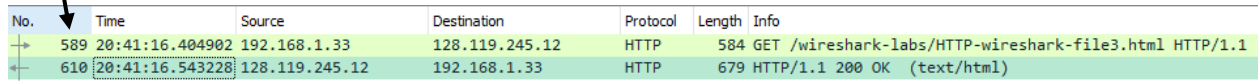
The returned HTTP status code is "304 Not Modified".

Server did not explicitly return the contents of the file because the browser has already cached the contents of the webpage. Server responded with "304 Not Modified", so the browser understood that the data is not changed, then the browser retrieved the contents of the webpage from its local cache.
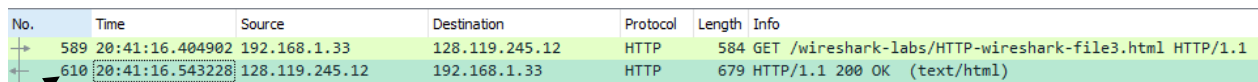
3. Retrieving Long Documents

Q12. 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?

No.	Time	Source	Destination	Protocol	Length	Info
589	20:41:16.404902	192.168.1.33	128.119.245.12	HTTP	584	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
610	20:41:16.543228	128.119.245.12	192.168.1.33	HTTP	679	HTTP/1.1 200 OK (text/html)

My browser sent only 1 HTTP GET request. Packet number of the GET message is 589
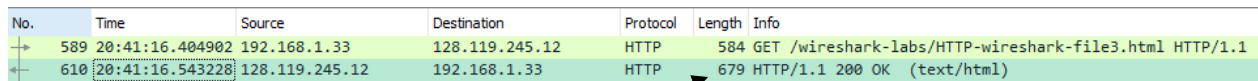
Q13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

No.	Time	Source	Destination	Protocol	Length	Info
589	20:41:16.404902	192.168.1.33	128.119.245.12	HTTP	584	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
610	20:41:16.543228	128.119.245.12	192.168.1.33	HTTP	679	HTTP/1.1 200 OK (text/html)

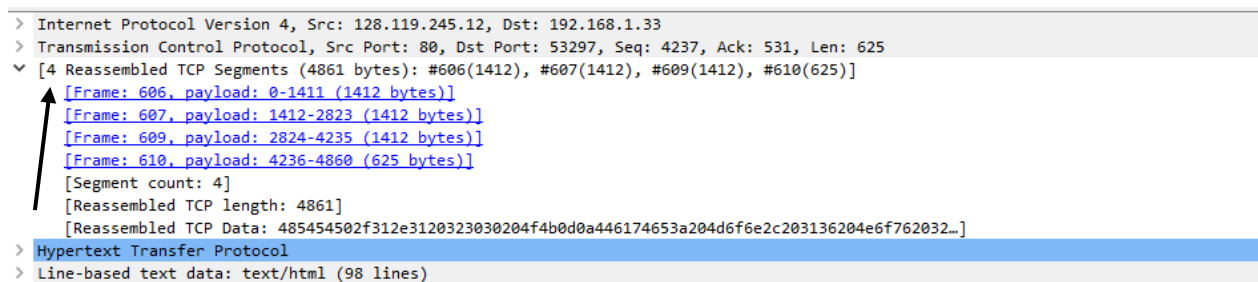The packet number that contains the status code and phrase associated with the response to the HTTP GET request is 610

Q14. What is the status code and phrase in the response?

No.	Time	Source	Destination	Protocol	Length	Info
589	20:41:16.404902	192.168.1.33	128.119.245.12	HTTP	584	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
610	20:41:16.543228	128.119.245.12	192.168.1.33	HTTP	679	HTTP/1.1 200 OK (text/html)

The status code is 200 and the phrase is OK

Q15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.33
> Transmission Control Protocol, Src Port: 80, Dst Port: 53297, Seq: 4237, Ack: 531, Len: 625
∨ [4 Reassembled TCP Segments (4861 bytes): #606(1412), #607(1412), #609(1412), #610(625)]
    [Frame: 606, payload: 0-1411 (1412 bytes)]
    [Frame: 607, payload: 1412-2823 (1412 bytes)]
    [Frame: 609, payload: 2824-4235 (1412 bytes)]
    [Frame: 610, payload: 4236-4860 (625 bytes)]
    [Segment count: 4]
    [Reassembled TCP length: 4861]
    [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a204d6f6e2c203136204e6f762032…]
> Hypertext Transfer Protocol
> Line-based text data: text/html (98 lines)
```

4 reassembled TCP Segments were needed to carry the single HTTP response and the text of the Bill of Rights

4. HTML Documents with Embedded Objects

Q16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

```
284 20:56:44.524174 192.168.1.33      128.119.245.12    HTTP    584 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
292 20:56:44.662796 128.119.245.12     192.168.1.33      HTTP   1127 HTTP/1.1 200 OK  (text/html)
294 20:56:44.725922 192.168.1.33       128.119.245.12    HTTP    516 GET /pearson.png HTTP/1.1
299 20:56:44.859001 128.119.245.12     192.168.1.33      HTTP    841 HTTP/1.1 200 OK  (PNG)
320 20:56:45.091573 192.168.1.33       128.119.245.12    HTTP    490 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
502 20:56:45.654582 128.119.245.12     192.168.1.33      HTTP   1120 HTTP/1.1 200 OK  (JPEG JFIF image)
```

My browser sent 3 HTTP GET request messages. All of these messages sent to same address which is 128.119.245.12

Q17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

```
284 20:56:44.524174 192.168.1.33      128.119.245.12    HTTP    584 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
292 20:56:44.662796 128.119.245.12     192.168.1.33      HTTP   1127 HTTP/1.1 200 OK  (text/html)
294 20:56:44.725922 192.168.1.33       128.119.245.12    HTTP    516 GET /pearson.png HTTP/1.1
299 20:56:44.859001 128.119.245.12     192.168.1.33      HTTP    841 HTTP/1.1 200 OK  (PNG)
320 20:56:45.091573 192.168.1.33       128.119.245.12    HTTP    490 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
502 20:56:45.654582 128.119.245.12     192.168.1.33      HTTP   1120 HTTP/1.1 200 OK  (JPEG JFIF image)
```

My browser downloaded two images serially. We can understand that from the implementation time of these two requests. One of the images started at 20:56:44.725922 and ended at 20:56:44.859001, the other one has started at 20:56:45.091573 and ended at 20:56:45.654582.
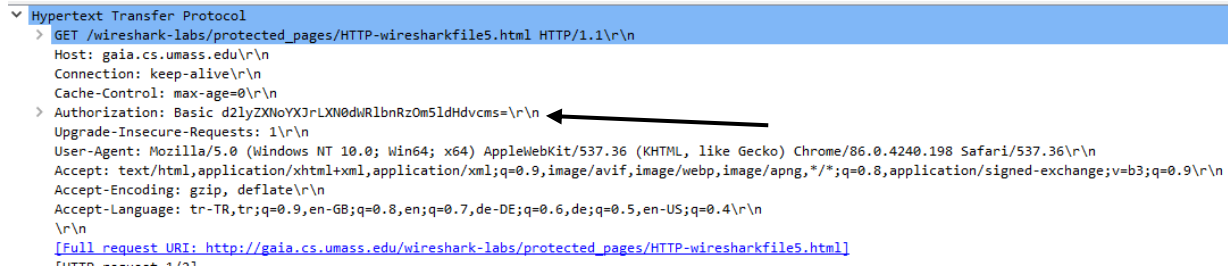
5. HTTP Authentication

Q18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

```
103 21:10:22.159160 192.168.1.33      128.119.245.12    HTTP    599 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
109 21:10:22.311188 128.119.245.12     192.168.1.33      HTTP    771 HTTP/1.1 401 Unauthorized  (text/html)
480 21:10:41.123960 192.168.1.33      128.119.245.12    HTTP    684 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
484 21:10:41.280342 128.119.245.12     192.168.1.33      HTTP    583 HTTP/1.1 404 Not Found  (text/html)
487 21:10:41.518346 192.168.1.33      128.119.245.12    HTTP    574 GET /favicon.ico HTTP/1.1
490 21:10:41.657673 128.119.245.12     192.168.1.33      HTTP    538 HTTP/1.1 404 Not Found  (text/html)
```

Initial response of the server is "401 Unauthorized"

Q19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

```
✓ Hypertext Transfer Protocol
  › GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.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
  › Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\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/86.0.4240.198 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: tr-TR,tr;q=0.9,en-GB;q=0.8,en;q=0.7,de-DE;q=0.6,de;q=0.5,en-US;q=0.4\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]
```

The new field that is included in second HTTP GET message is "Authorization"