Author: Jeremy Vuong
Course: CSC 138-03
Professor: Jun Dai
Date: 03/05/2023

Wireshark Lab 2-HTTP

1. My browser is running HTTP version 1.1.
   The server is running HTTP version 1.1.
2. My browser indicates that it can accept the language en-US.
3. The IP address of my computer is 10.0.0.96 and the IP address of the gaia.cs.umass.edu server is 128.119.245.12.
4. The status code returned from the server to my browser is Status Code: 200.
5. The HTML file was last modified Sun, 05 Mar 2023 03:59:01 GMT.
6. 128 bytes of content are being returned to my browser.
7. I do not see any headers within the data that are not displayed in the packet-listing window

```
No.     Time              Source                Destination           Protocol Length Info
    373 19:51:13.486174   10.0.0.96             128.119.245.12        HTTP     533    GET /wireshark-labs/HTTP-wireshark-file1.html
HTTP/1.1
Frame 373: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63278, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
Hypertext Transfer Protocol
    GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
        Request Method: GET
        Request URI: /wireshark-labs/HTTP-wireshark-file1.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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/
110.0.1587.63\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;q=0.7\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-file1.html]
    [HTTP request 1/2]
    [Response in frame: 380]
    [Next request in frame: 382]
```

```
No.     Time              Source                Destination           Protocol Length Info
    380 19:51:13.576435    128.119.245.12        10.0.0.96             HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 380: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 63278, Seq: 1, Ack: 480, Len: 486
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: Mon, 06 Mar 2023 03:51:13 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    ETag: "80-5f621b69a28c6"\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: 0.090261000 seconds]
    [Request in frame: 373]
    [Next request in frame: 382]
    [Next response in frame: 392]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    File Data: 128 bytes
Line-based text data: text/html (4 lines)
```

8. No, I do not see an “IF-MODIFIED-SINCE” line in the HTTP GET.

```
> Frame 204: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits) on interface \Device\NPF_{2748DDCA-E1DE-4281-80C4-430F4323F5A7}, id 0
> Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
> Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 63534, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
v Hypertext Transfer Protocol
  v 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
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/110.0.1587.63\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;q=0.7\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-file2.html]
    [HTTP request 1/1]
```

9. Yes, the server explicitly returned the contents of the file. The section named “Line-based text data” shows exactly what is displayed in my browser when I opened the webpage (gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html) into my browser.

```
No.     Time               Source                Destination           Protocol Length Info
    224 19:57:28.098106    128.119.245.12        10.0.0.96             HTTP     784    HTTP/1.1 200 OK  (text/html)
Frame 224: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 63534, Seq: 1, Ack: 480, Len: 730
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: Mon, 06 Mar 2023 03:57:28 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    ETag: "173-5f621b69a20f6"\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: 0.101599000 seconds]
    [Request in frame: 204]
    [Next request in frame: 227]
    [Next response in frame: 242]
    [Request URI: http://gaia.cs.umass.edu/favicon.ico]
    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
```

10. Yes, I see an “IF-MODIFIED-SINCE:” line in the HTTP GET. The information that follows the “IF-MODIFIED-SINCE:” header is the date and time that I last accessed the link/webpage.

```
No.     Time               Source                Destination           Protocol Length Info
   1405 19:57:44.422190    10.0.0.96             128.119.245.12        HTTP     645    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 1405: 645 bytes on wire (5160 bits), 645 bytes captured (5160 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 63535, Dst Port: 80, Seq: 1, Ack: 1, Len: 591
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36 Edg/
110.0.1587.63\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;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-5f621b69a20f6"\r\n
    If-Modified-Since: Sun, 05 Mar 2023 06:59:01 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: 1414]
```

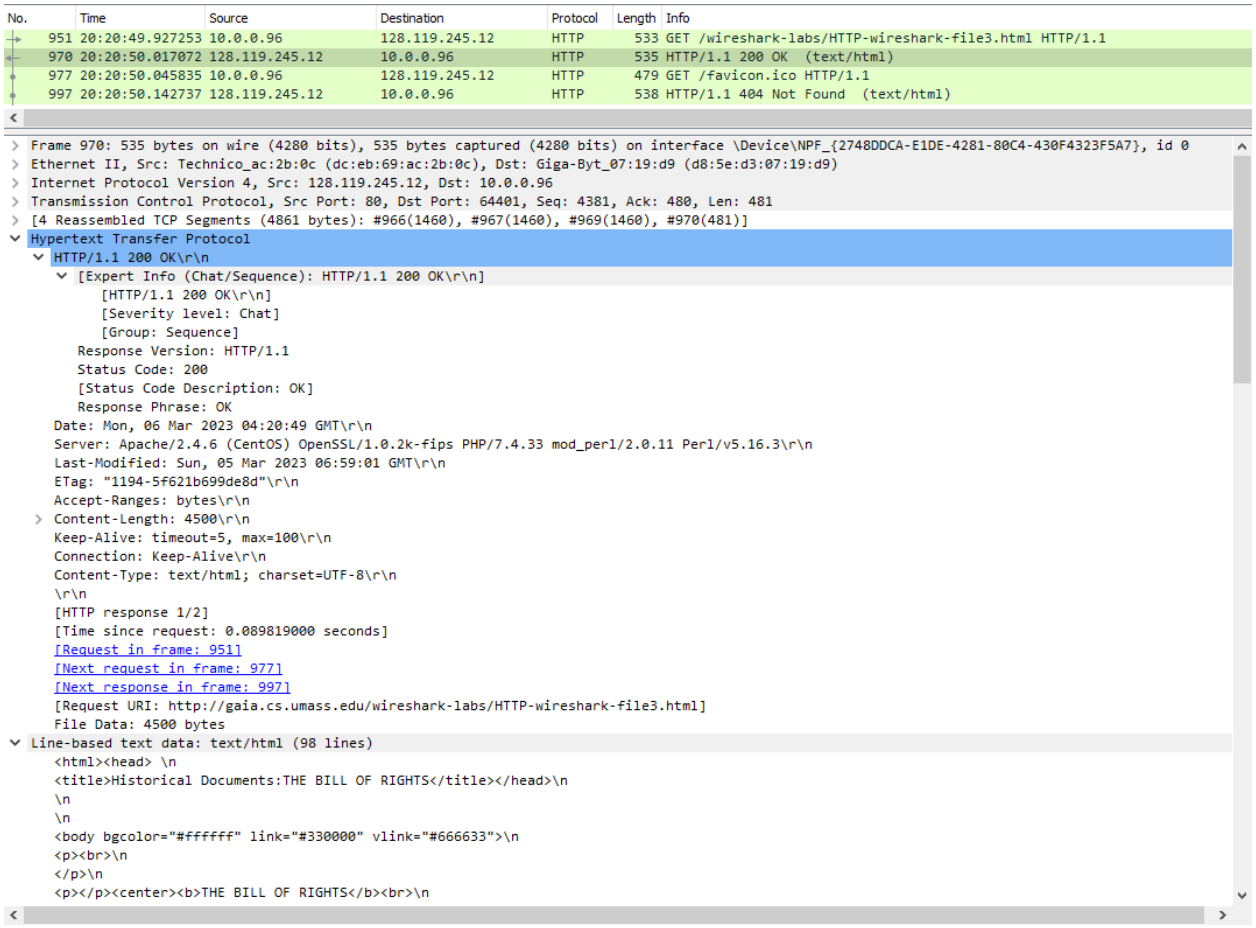
11. The HTTP status code is 304. No, the server did not explicitly return the contents of the file. Because the file had not been modified since it was last accessed, the browser retrieved the old file from its cached memory.

```
No.     Time              Source                Destination           Protocol Length Info
   1414 19:57:44.525108   128.119.245.12        10.0.0.96             HTTP     294    HTTP/1.1 304 Not Modified
Frame 1414: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 63535, Seq: 1, Ack: 592, Len: 240
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Mon, 06 Mar 2023 03:57:44 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 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: "173-5f621b69a20f6"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.102918000 seconds]
    [Request in frame: 1405]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

12. My browser sent 1 HTTP GET requests. The packet that contains the GET message for the Bill of Rights is packet number 951.

No.	Time	Source	Destination	Protocol	Length	Info
951	20:20:49.927253	10.0.0.96	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
970	20:20:50.017072	128.119.245.12	10.0.0.96	HTTP	535	HTTP/1.1 200 OK (text/html)
977	20:20:50.045835	10.0.0.96	128.119.245.12	HTTP	479	GET /favicon.ico HTTP/1.1
997	20:20:50.142737	128.119.245.12	10.0.0.96	HTTP	538	HTTP/1.1 404 Not Found (text/html)

13. The packet that contains the status code and phrase associated with the response to the HTTP GET request is packet number 970.



14. The status code is 200 and the phrase is OK in the response.

```
No.     Time               Source                Destination           Protocol Length Info
    970 20:20:50.017072    128.119.245.12        10.0.0.96             HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 970: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 64401, Seq: 4381, Ack: 480, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #966(1460), #967(1460), #969(1460), #970(481)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 06 Mar 2023 04:20:49 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    ETag: "1194-5f621b699de8d"\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 1/2]
    [Time since request: 0.089819000 seconds]
    [Request in frame: 951]
    [Next request in frame: 977]
    [Next response in frame: 997]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
```

15. There were 4 data-containing TCP segments needed to carry the single HTTP response and the text of the Bill of Rights.

```
No.     Time               Source                Destination           Protocol Length Info
    970 20:20:50.017072    128.119.245.12        10.0.0.96             HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 970: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 64401, Seq: 4381, Ack: 480, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #966(1460), #967(1460), #969(1460), #970(481)]
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
            [HTTP/1.1 200 OK\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 200
        [Status Code Description: OK]
        Response Phrase: OK
    Date: Mon, 06 Mar 2023 04:20:49 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sun, 05 Mar 2023 06:59:01 GMT\r\n
    ETag: "1194-5f621b699de8d"\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 1/2]
    [Time since request: 0.089819000 seconds]
    [Request in frame: 951]
    [Next request in frame: 977]
    [Next response in frame: 997]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
    File Data: 4500 bytes
```

16. My browser sent 3 HTTP GET request messages.
    - 128.119.245.12 (wireshark-labs/HTTP-wireshark-file4.html)
    - 128.119.245.12 (pearson.png)
    - 178.79.137.164 (/8E_cover_small.jpg)

No.	Time	Source	Destination	Protocol	Length	Info
471	20:44:35.937157	10.0.0.96	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
496	20:44:36.035012	128.119.245.12	10.0.0.96	HTTP	1355	HTTP/1.1 200 OK (text/html)
497	20:44:36.040604	10.0.0.96	128.119.245.12	HTTP	479	GET /pearson.png HTTP/1.1
523	20:44:36.139623	128.119.245.12	10.0.0.96	HTTP	745	HTTP/1.1 200 OK (PNG)
718	20:44:36.712402	10.0.0.96	178.79.137.164	HTTP	446	GET /8E_cover_small.jpg HTTP/1.1
730	20:44:36.869442	178.79.137.164	10.0.0.96	HTTP	225	HTTP/1.1 301 Moved Permanently

17. Yes, the two images were downloaded serially. The first image's HTTP GET request was completed before the second image's HTTP GET request was sent.

No.	Time	Source	Destination	Protocol	Length	Info
471	20:44:35.937157	10.0.0.96	128.119.245.12	HTTP	533	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
496	20:44:36.035012	128.119.245.12	10.0.0.96	HTTP	1355	HTTP/1.1 200 OK (text/html)
497	20:44:36.040604	10.0.0.96	128.119.245.12	HTTP	479	GET /pearson.png HTTP/1.1
523	20:44:36.139623	128.119.245.12	10.0.0.96	HTTP	745	HTTP/1.1 200 OK (PNG)
718	20:44:36.712402	10.0.0.96	178.79.137.164	HTTP	446	GET /8E_cover_small.jpg HTTP/1.1
730	20:44:36.869442	178.79.137.164	10.0.0.96	HTTP	225	HTTP/1.1 301 Moved Permanently

18. The server's response code is 401 Unauthorized.

```
No.     Time              Source                Destination           Protocol Length Info
   8557 21:02:54.715512   128.119.245.12        10.0.0.96             HTTP     771    HTTP/1.1 401 Unauthorized  (text/html)
Frame 8557: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c), Dst: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.96
Transmission Control Protocol, Src Port: 80, Dst Port: 49891, Seq: 1, Ack: 496, Len: 717
Hypertext Transfer Protocol
    HTTP/1.1 401 Unauthorized\r\n
        [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
            [HTTP/1.1 401 Unauthorized\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Response Version: HTTP/1.1
        Status Code: 401
        [Status Code Description: Unauthorized]
        Response Phrase: Unauthorized
    Date: Mon, 06 Mar 2023 05:02:54 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.087438000 seconds]
    [Request in frame: 8540]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 381 bytes
Line-based text data: text/html (12 lines)
```

19. The new field that is included is the authorization field.

```
No.     Time              Source                Destination           Protocol Length Info
   9142 21:03:11.260688   10.0.0.96             128.119.245.12        HTTP     634    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 9142: 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits) on interface \Device\NPF_{2748DDCA-
E1DE-4281-80C4-430F4323F5A7}, id 0
Ethernet II, Src: Giga-Byt_07:19:d9 (d8:5e:d3:07:19:d9), Dst: Technico_ac:2b:0c (dc:eb:69:ac:2b:0c)
Internet Protocol Version 4, Src: 10.0.0.96, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 49890, Dst Port: 80, Seq: 1, Ack: 1, Len: 580
Hypertext Transfer Protocol
    GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
        [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
            [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
            [Severity level: Chat]
            [Group: Sequence]
        Request Method: GET
        Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.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
    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/110.0.0.0 Safari/537.36 Edg/
110.0.1587.63\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;q=0.7\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-wireshark-file5.html]
    [HTTP request 1/2]
    [Response in frame: 9151]
    [Next request in frame: 9152]
```