

No.	Time	Source	Destination	Protocol	Length	Info
32	19:59:14.155892000	10.36.40.181	128.119.245.12	HTTP	473	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
33	19:59:14.179788000	128.119.245.12	10.36.40.181	HTTP	457	HTTP/1.1 200 OK (text/html)
35	19:59:14.438582000	10.36.40.181	128.119.245.12	HTTP	384	GET /favicon.ico HTTP/1.1
36	19:59:14.452193000	128.119.245.12	10.36.40.181	HTTP	532	HTTP/1.1 404 Not Found (text/html)

HTTP protocol

File one

1)

```
Accept-Language: en-US,en;q=0.8\r\n
```

2) IP address = source : 10.36.40.181

Server = destination : 128.119.245.12

3)

```
If-Modified-Since: Fri, 10 Nov 2023 06:00:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wi
[HTTP request 1/1]
[Response in frame: 23]
```

4)

```
Content-Type: text/html; charset=UTF-8\r\n
Content-Length: 128\r\n
```

File 2

1) no there is no IF-MODIFIED-SINCE line

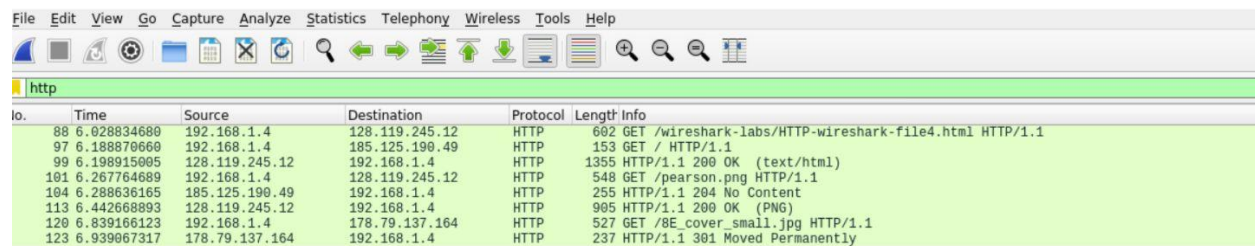
```
Frame 90: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface wlp2s0b1, id 0
Ethernet II, Src: GemtekTe_ac:87:57 (20:10:7a:ac:87:57), Dst: HuaweiTe_2d:15:54 (7c:11:cb:2d:15:54)
Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 43128, Dst Port: 80, Seq: 1, Ack: 1, Len: 548
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]
    [GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 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\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ar-EG;q=0.8,ar;q=0.7,es-US;q=0.6,es;q=0.5,fil-PH;q=0.4,fil;q=0.3,bn-BD;q=0.2,bn;q=0.1\r\n
    \r\n
```

2)

```
\r\n
ine-based text data: text/html
\r\n
<html>\r\n
\r\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\r\n
This file's last modification date will not change. <p>\r\n
Thus if you download this multiple times on your browser, a complete copy <br>\r\n
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\r\n
field in your browser's HTTP GET request to the server.\r\n
\r\n
```

File 3

1)



The screenshot shows the Wireshark interface with a packet capture of HTTP traffic. The packet list pane shows several GET requests. The packet details pane shows the selected packet (No. 88) with its structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

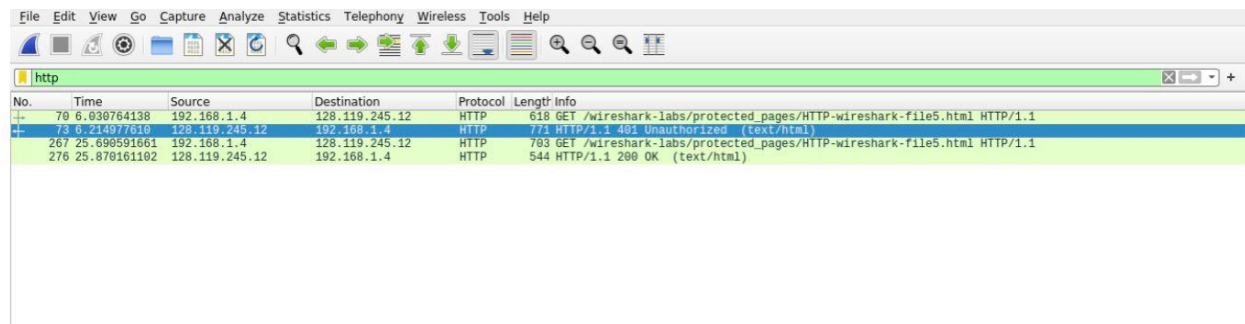
No.	Time	Source	Destination	Protocol	Length	Info
88	6.028834680	192.168.1.4	128.119.245.12	HTTP	602	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
97	6.188870660	192.168.1.4	185.125.190.49	HTTP	153	GET / HTTP/1.1
99	6.198915005	128.119.245.12	192.168.1.4	HTTP	1355	HTTP/1.1 200 OK (text/html)
101	6.267764689	192.168.1.4	128.119.245.12	HTTP	548	GET /pearson.png HTTP/1.1
104	6.288636165	185.125.190.49	192.168.1.4	HTTP	255	HTTP/1.1 204 No Content
113	6.442668893	128.119.245.12	192.168.1.4	HTTP	905	HTTP/1.1 200 OK (PNG)
120	6.839166123	192.168.1.4	178.79.137.164	HTTP	527	GET /8E_cover_small.jpg HTTP/1.1
123	6.939067317	178.79.137.164	192.168.1.4	HTTP	237	HTTP/1.1 301 Moved Permanently

3 GET for number 88, 97, 120

2) serially because they don't have the same time snippet

File 4

1) response was "401 Authentication Required"



The screenshot shows the Wireshark interface with a packet capture of HTTP traffic. The packet list pane shows a GET request (No. 73) and its response (No. 771). The packet details pane shows the selected packet (No. 771) with its structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The response status is 401 Unauthorized.

No.	Time	Source	Destination	Protocol	Length	Info
70	6.030764138	192.168.1.4	128.119.245.12	HTTP	618	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
73	6.214977610	128.119.245.12	192.168.1.4	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
267	25.690591661	192.168.1.4	128.119.245.12	HTTP	703	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
276	25.870161102	128.119.245.12	192.168.1.4	HTTP	544	HTTP/1.1 200 OK (text/html)

2) The new field that is now included is the authorization field

```
> Ethernet II, Src: GemtekTe_ac:87:57 (20:10:7a:ac:87:57), Dst: HuaweiTe_2d:15:54 (7c:11:cb:2d:15:54)
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 58858, Dst Port: 80, Seq: 1, Ack: 1, Len: 649
> Hypertext Transfer Protocol
  > GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.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 d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n
    Credentials: wireshark-students:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.0.0 Saf
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,ar-EG;q=0.8,ar;q=0.7,es-US;q=0.6,es;q=0.5,fil-PH;q=0.4,fil;q=0.3,bn-BD
    \r\n
```