

Wireshark Lab: HTTP

1- HTTP 1.1

2- en-US , en, and tr

3- Source Address: 10.22.77.113

(my computer),

Destination Address: 128.119.245.12 (the gaia.cs.umass.edu server)

4- 200

5- Tue, 24 Oct 2023 05:59:02 GMT

6- 128

7- No, I do not see.

8- No, I do not see

9- Yes, it did. Line-Based Text Data section is the same as what I saw on the browser.

10- Yes, it is included. The information is the date and time that I last modified the webpage. If-Modified-Since: Tue, 24 Oct 2023 05:59:02 GMT

```

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]
  [GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
  [Severity Level: Chat]
  [Group: Sequence]
  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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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;q=0.8\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
  If-None-Match: "80-60832af8f455"\r\n
  If-Modified-Since: Sat, 21 Oct 2023 05:59:01 GMT\r\n
  Source Address: 10.22.77.113
  Destination Address: 128.119.245.12

```

```

[Severity Level: Chat]
[Group: Sequence]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Tue, 24 Oct 2023 13:33:35 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: Tue, 24 Oct 2023 05:59:02 GMT\r\n
ETag: "80-60870091f2caa"\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]

```

```

Frame 75: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits)
Ethernet II, Src: Apple23:4c:62 (94:f6:06:23:4c:62), Dst: Fortinet80:00:12 (08:00:07:00:00:12)
Internet Protocol Version 4, Src: 10.22.77.113, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 48888, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,tr;q=0.8\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: 85]

```

```

Frame 80: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits)
Ethernet II, Src: Fortinet80:00:12 (08:00:07:00:00:12), Dst: Apple23:4c:62 (94:f6:06:23:4c:62)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.22.77.113
Transmission Control Protocol, Src Port: 80, Dst Port: 48888, Seq: 1, Ack: 488, Len: 728
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Tue, 24 Oct 2023 15:43:41 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: Tue, 24 Oct 2023 05:59:02 GMT\r\n
  ETag: "173-60870091f24aa"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 373\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: 0.147021088 seconds]
  [Request in frame: 75]
  [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
  File Data: 373 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. <br>\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 If-Modified-Since <br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n

```

```

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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
  If-None-Match: "173-60870091f24aa"\n
  If-Modified-Since: Tue, 24 Oct 2023 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: 279]

```

11- The HTTP status code is “304: Not Modified”. The server didn't provide the file's contents because the browser had stored a cached copy, and since the file hadn't changed since the last access, it instructed the browser to fetch the old cached version.

```
> Frame 270: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
> Ethernet II, Src: Fortinet_09:00:12 (00:09:0f:09:00:12), Dst: Apple_23:4c:62 (94:f6:d6:23:4c:62)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.22.77.113
> Transmission Control Protocol, Src Port: 80, Dst Port: 49897, Seq: 1, Ack: 600, 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\r\n
    Date: Tue, 24 Oct 2023 15:43:57 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: "173-68070091f24da"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.150890000 seconds]
    [Request in frame: 266]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

12- My browser sent 1 HTTP GET request to the server. The packet number was 207.

13- It was 222.

No.	Time	Source	Destination	Protocol	Length	Info
207	3.860383	10.22.77.113	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
222	4.059097	128.119.245.12	10.22.77.113	HTTP	1165	HTTP/1.1 200 OK (text/html)

14- Status Code: 200
Response Phrase: OK

```
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  > 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: Tue, 24 Oct 2023 15:58:28 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: Tue, 24 Oct 2023 05:59:02 GMT\r\n
    ETag: "1194-68070091e65a"\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: 0.190790000 seconds]
    [Request in frame: 207]
    [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)]
```

15- 4 TCP segments

```
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
  > 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: Tue, 24 Oct 2023 15:58:28 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: Tue, 24 Oct 2023 05:59:02 GMT\r\n
    ETag: "1194-68070091e65a"\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]
```

16- 3 http GET message requests

No.	Time	Source	Destination	Protocol	Length	Info
84	3.132532	10.22.77.113	128.119.245.12	HTTP	541	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
99	3.283148	128.119.245.12	10.22.77.113	HTTP	105	HTTP/1.1 200 OK (text/html)
103	3.315585	10.22.77.113	128.119.245.12	HTTP	487	GET /pearson.png HTTP/1.1
109	3.400972	10.22.77.113	178.79.137.164	HTTP	466	GET /8E_cover_small.jpg HTTP/1.1
112	3.464770	128.119.245.12	10.22.77.113	HTTP	1165	HTTP/1.1 200 OK (PNG)
116	3.474212	178.79.137.164	10.22.77.113	HTTP	237	HTTP/1.1 301 Moved Permanently

1- [Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>]

Destination Address: 128.119.245.12

```

[Header check status: Unverified]
Source Address: 10.22.77.113
Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 49967, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
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
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]
[Response in frame: 132]

```

2- [Full request URI: <http://gaia.cs.umass.edu/pearson.png>]

Destination Address: 128.119.245.12

```

[Expert Info (Chat/Sequence): GET /pearson.png HTTP/1.1\r\n]
Request Method: GET
Request URI: /pearson.png
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*;q=0.8\r\n
Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/pearson.png]
[HTTP request 542]
[Prev request in frame: 84]
[Response in frame: 132]

```

3- [Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]

Destination Address: 178.79.137.164

```

Source Address: 10.22.77.113
Destination Address: 178.79.137.164
Transmission Control Protocol, Src Port: 49969, Dst Port: 80, Seq: 1, Ack: 1, Len: 480
Hypertext Transfer Protocol
GET /8E_cover_small.jpg HTTP/1.1\r\n
Host: kurose.cslash.net\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36\r\n
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*;q=0.8\r\n
Referer: http://gaia.cs.umass.edu\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
\r\n
[Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
[HTTP request 542]
[Response in frame: 136]

```

17- The two image object file were downloaded in parallel. This is evidenced by the fact that two GET request messages (for the image objects) are made before either of the image objects are received.

18- Status Code: 401

Response Phrase: Unauthorized

```

Hypertext Transfer Protocol
HTTP/1.1 401 Unauthorized\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
Response Version: HTTP/1.1
Status Code: 401
Response Phrase: Unauthorized
Date: Tue, 24 Oct 2023 20:28:48 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: 0.14591800 seconds]
[Request in frame: 208]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
File Data: 301 bytes
[Line-based text data: text/html (12 lines)]

```

19. Authorization field

```

Transmission Control Protocol, Src Port: 50161, 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]
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 d2lyZWNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n
Credentials: wireshark-students:network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 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;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9,tr;q=0.8\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 1417]

```