

/var/folders/sv/92zc6xbs7r1_32n3m4_nsyv80000gn/T/wireshark_1000 LANY4GE00.pcapng 723 total packets, 4 shown

No.	Time	Source	Destination	Protocol	Length	Info
638	14:38:24.125155	192.168.1.210	128.119.245.12	HTTP	448	GET / wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Frame 638: 448 bytes on wire (3584 bits), 448 bytes captured (3584 bits) on interface en7, id 0

/var/folders/sv/92zc6xbs7r1_32n3m4_nsyv80000gn/T/wireshark_1000 LANY4GE00.pcapng 723 total packets, 4 shown

No.	Time	Source	Destination	Protocol	Length	Info
642	14:38:24.220309	128.119.245.12	192.168.1.210	HTTP	552	HTTP/1.1 200 OK (text/html)

Frame 642: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en7, id 0

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n
Date: Sun, 21 Mar 2021 21:38:24 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod_perl/2.0.11 Perl/v5.16.3\r\n
Last-Modified: Sun, 21 Mar 2021 05:59:01 GMT\r\n
ETag: "80-5be05a55baf1d"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
[Content length: 128]
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: 0.095154000 seconds]
[Request in frame: 638]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes

```
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
```

1. Browser is using HTTP version 1.1, and server is running HTTP version 1.1
2. Accept-Language: en-US,en;q=0.5 \r\n
3. My computer: 192.168.1.210, gaia.cs.umass.edu: 128.119.245.12
4. Status Code → 200 (OK)
5. Last-Modified: Sun, 21 Mar 2021 05:59:01 GMT \r\n
6. File Data: 128 bytes
7. None, I don't see any.

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.210
Transmission Control Protocol, Src Port: 80, Dst Port: 50576, Seq: 1, Ack: 383, Len: 730
Hypertext Transfer Protocol

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
```

Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.16; rv:86.0) Gecko/20100101 Firefox/86.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
If-Modified-Since: Sun, 21 Mar 2021 05:59:01 GMT\r\n
If-None-Match: "173-5be05a55ba74c"\r\n

No.	Time	Source	Destination	Protocol	Length	Info
646	16:00:34.733215	128.119.245.12	192.168.1.210	HTTP	306	HTTP/1.1

304 Not Modified

Frame 646: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface en7, id 0
Ethernet II, Src: ASUSTekC_e5:58:90 (70:4d:7b:e5:58:90), Dst: GopodGro_07:e3:5a (48:65:ee:17:e3:5a)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.210

Transmission Control Protocol, Src Port: 80, Dst Port: 50583, Seq: 1, Ack: 495, Len: 240

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Sun, 21 Mar 2021 23:00:34 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 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: "173-5be05a55ba74c"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.094881000 seconds]

[Request in frame: 643]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

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

9. The server did return contents of the file; I can tell by the Line-based text data field shown above.

10. If-Modified-Since: Sun, 21 Mar 2021 05:59:01 GMT\r\n

11. Status Code → 304 (Not Modified). The server did not return the contents of the file because nothing changed since it was last stored as cache. The If-Modified-Since line stored the date of when it was last modified, and the website would need to change its’ contents for it to return contents of the file.

Time	Source	Destination	Protocol	Length	Info
110	16:37:11...	192.168.1... 128.119.245.12	HTTP	448	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
115	16:37:11...	128.119.2... 192.168.1.210	HTTP	583	HTTP/1.1 200 OK (text/html)
135	16:37:12...	192.168.1... 128.119.245.12	HTTP	405	GET /favicon.ico HTTP/1.1
140	16:37:12...	128.119.2... 192.168.1.210	HTTP	551	HTTP/1.1 404 Not Found (text/html)

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: Sun, 21 Mar 2021 23:37:11 GMT\r\n

```
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.210
> Transmission Control Protocol, Src Port: 80, Dst Port: 50828, Seq: 4345, Ack: 383, Len: 517
> [4 Reassembled TCP Segments (4861 bytes): #112(1448), #113(1448), #114(1448), #115(517)]
  [Frame: 112, payload: 0-1447 (1448 bytes)]
  [Frame: 113, payload: 1448-2895 (1448 bytes)]
  [Frame: 114, payload: 2896-4343 (1448 bytes)]
  [Frame: 115, payload: 4344-4860 (517 bytes)]
  [Segment count: 4]
  [Reassembled TCP Length: 4861]
  [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a2053756e2c203231204d61722032...]
> Hypertext Transfer Protocol
```

12. My browser sent one HTTP GET request message. Packet number 115 contains the GET message for the Bill of Rights.

13. Packet 115

14. Status Code → 200, Status Phrase → OK

15. 4 TCP segments

350	19:08:33.619524	192.168.1... 178.79.137.164	HTTP	412	GET /8E_cover_small.jpg HTTP/1.1
353	19:08:33.637091	192.168.1... 128.119.245.12	HTTP	405	GET /pearson.png HTTP/1.1
357	19:08:33.729456	128.119.2... 192.168.1.210	HTTP	782	HTTP/1.1 200 OK (PNG)
361	19:08:33.771424	178.79.13... 192.168.1.210	HTTP	237	HTTP/1.1 301 Moved Permanently

16. There is a total of 3 HTTP Get request messages sent to Host: gaia.cs.umass.edu\r\n

17. The images were downloaded serially; we can tell by the time where they are different. If the images were downloaded in parallel they both of the images would have the same time.

```
Upgrade-Insecure-Requests: 1\r\n
Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
  Credentials: wireshark-students:network
\r\n
```

18. Status Code → 404, Status phrase → Unauthorized

19. The new field added was Authorization field