

No.	Time	Source	Destination	Protocol	Length	Info
124	3.951189	172.17.125.190	128.119.245.12	HTTP	653	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
141	4.256532	128.119.245.12	172.17.125.190	HTTP	305	HTTP/1.1 304 Not Modified
232	32.096295	172.17.125.190	203.205.232.66	HTTP	213	GET /mcrhead/evp0NfXE64IUtSbGqADTOegcIhMh5yAHGjcy7mEWgQvMefnDYfNB8TR0eRGYnVzrEp4JIRa3seNicsiaY8c8ncvIgg-
237	32.143186	172.17.125.190	203.205.254.220	HTTP	802	POST /mmtls/00002ec0 HTTP/1.1
247	32.147106	203.205.232.66	172.17.125.190	HTTP	204	HTTP/1.1 200 OK (JPEG 3FIF image)
253	32.272453	203.205.254.220	172.17.125.190	HTTP	624	HTTP/1.1 200 OK
260	32.392602	172.17.125.190	49.51.89.155	HTTP	792	POST /mmtls/00002ec0 HTTP/1.1
263	32.666499	49.51.89.155	172.17.125.190	HTTP	1063	HTTP/1.1 200 OK
8625	308.713273	172.17.125.190	203.205.254.220	HTTP	841	POST /mmtls/00003245 HTTP/1.1
8628	308.723355	172.17.125.190	203.205.254.220	HTTP	841	POST /mmtls/00003245 HTTP/1.1
8631	308.726978	172.17.125.190	203.205.254.220	HTTP	801	POST /mmtls/00003245 HTTP/1.1

> Frame 124: 653 bytes on wire (5224 bits), 653 bytes captured (5224 bits) on interface \Device\NPF_{05902488-473A-46E5-8229-98F0E39007DA}, id 0
 > Ethernet II, Src: TendaTec_d8:1c:cd (50:2b:73:dd:1c:cd), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
 > Internet Protocol Version 4, Src: 172.17.125.190, Dst: 128.119.245.12
 > Transmission Control Protocol, Src Port: 2264, Dst Port: 80, Seq: 1, Ack: 1, Len: 587

▼ 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

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/88.0.4324.190 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: zh-CN,zh;q=0.9\r\n

If-None-Match: "80-5bd0070156e16"\r\n

If-Modified-Since: Mon, 08 Mar 2021 06:21:01 GMT\r\n

\r\n

No.	Time	Source	Destination	Protocol	Length	Info
124	3.951189	172.17.125.190	128.119.245.12	HTTP	653	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
141	4.256532	128.119.245.12	172.17.125.190	HTTP	305	HTTP/1.1 304 Not Modified
232	32.096295	172.17.125.190	203.205.232.66	HTTP	213	GET /mcrhead/evp0NfXE64IUtSbGqADTOegcIhMh5yAHGjcy7mEWgQvMefnDYfNB8TR0eRGYnVzrEp4JIRa3seNicsiaY8c8ncvIgg-
237	32.143186	172.17.125.190	203.205.254.220	HTTP	802	POST /mmtls/00002ec0 HTTP/1.1
247	32.147106	203.205.232.66	172.17.125.190	HTTP	204	HTTP/1.1 200 OK (JPEG 3FIF image)
253	32.272453	203.205.254.220	172.17.125.190	HTTP	624	HTTP/1.1 200 OK
260	32.392602	172.17.125.190	49.51.89.155	HTTP	792	POST /mmtls/00002ec0 HTTP/1.1
263	32.666499	49.51.89.155	172.17.125.190	HTTP	1063	HTTP/1.1 200 OK
8625	308.713273	172.17.125.190	203.205.254.220	HTTP	841	POST /mmtls/00003245 HTTP/1.1
8628	308.723355	172.17.125.190	203.205.254.220	HTTP	841	POST /mmtls/00003245 HTTP/1.1
8631	308.726978	172.17.125.190	203.205.254.220	HTTP	801	POST /mmtls/00003245 HTTP/1.1

> Frame 141: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface \Device\NPF_{05902488-473A-46E5-8229-98F0E39007DA}, id 0
 > Ethernet II, Src: Cisco_04:14:00 (a0:e0:af:04:14:00), Dst: TendaTec_d8:1c:cd (50:2b:73:dd:1c:cd)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.17.125.190
 > Transmission Control Protocol, Src Port: 80, Dst Port: 2264, Seq: 1, Ack: 588, Len: 239

▼ 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, 08 Mar 2021 06:21:44 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: "80-5bd0070156e16"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.305343000 seconds]

[Request in frame: 124]

[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

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

Answer: They are both running HTTP 1.1

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

Answer: Accept-Language: zh-CN

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

Answer: My IP address is 172.17.125.190 and the server's is 128.119.245.12

No.	Time	Source	Destination	Protocol	Length	Info
124	3.951189	172.17.125.190	128.119.245.12	HTTP	653	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
141	4.256532	128.119.245.12	172.17.125.190	HTTP	305	HTTP/1.1 304 Not Modified

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

Answer: 304; Not Modified

No.	Time	Source	Destination	Protocol	Length	Info
141	4.256532	128.119.245.12	172.17.125.190	HTTP	305	HTTP/1.1 304 Not Modified

▼ 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

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

Answer: Mon, 08 Mar 2021 06:21:44 GMT\r\n

```
-----
[Status Code Description: Not Modified]
Response Phrase: Not Modified
Date: Mon, 08 Mar 2021 06:21:44 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
```

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

Answer: 128 bytes

```
ETag: "80-5bd00def68207"\r\n
Accept-Ranges: bytes\r\n
> Content-Length: 128\r\n
```

7. 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.

Answer: No all of the headers can be found in the raw data.

8. 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?

Answer: No

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

Answer: Yes, we can find this information from Line-based text data field.

```
▼ Line-based text data: text/html (4 lines)
<html>\n
Congratulations. You've downloaded the file \n
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!\n
</html>\n
```

10. 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?

Answer: Yes

```
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9\r\n
If-None-Match: "80-5bd0070156e16"\r\n
If-Modified-Since: Mon, 08 Mar 2021 06:21:01 GMT\r\n
\r\n
```

11. 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.

Answer: status code: 200

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill of Rights?

Answer: one HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
180	6.118413	172.17.125.190	128.119.245.12	HTTP	542	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
187	6.384366	128.119.245.12	172.17.125.190	HTTP	1213	HTTP/1.1 200 OK (text/html)

13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

```
Transmission Control Protocol, Src Port: 80, Dst Port: 2804, Seq: 1, Ack: 590, Len: 241
  Source Port: 80
  Destination Port: 2804
  [Stream index: 6]
  [TCP Segment Len: 241]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 186363198
  [Next Sequence Number: 242 (relative sequence number)]
  Acknowledgment Number: 590 (relative ack number)
  Acknowledgment number (raw): 3507330885
  1000 .... = Header Length: 32 bytes (8)
```

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

Answer: 200 OK

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

Answer: according to the author's trace file, we can find there are 4 TCP segments.

```
[4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]
  [Frame: 10, payload: 0-1459 (1460 bytes)]
  [Frame: 11, payload: 1460-2919 (1460 bytes)]
  [Frame: 13, payload: 2920-4379 (1460 bytes)]
  [Frame: 14, payload: 4380-4815 (436 bytes)]
```