

Wireshark HTTP

The first screenshot shows a packet capture of an HTTP GET request. The packet list shows frame 517, which is a GET request to `/wireshark-labs/HTTP-wireshark-file1.html` from 192.168.1.10 to 128.119.245.12. The packet details pane shows the Hypertext Transfer Protocol section with the following information:

- Host: `gaia.cs.umass.edu`
- User-Agent: `Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0`
- Accept: `text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`
- Accept-Language: `en-US,en;q=0.5`
- Accept-Encoding: `gzip, deflate`
- Connection: `keep-alive`

The packet bytes pane shows the raw data of the request.

The second screenshot shows the details of the HTTP response (frame 528). The packet list shows frame 528, which is a 200 OK response from 128.119.245.12 to 192.168.1.10. The packet details pane shows the Hypertext Transfer Protocol section with the following information:

- Status Code: `200`
- Response Phrase: `OK`
- Date: `Thu, 08 Dec 2016 14:57:16 GMT`
- Server: `Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3`
- Last-Modified: `Thu, 06 Dec 2016 06:59:01 GMT`
- ETag: `"80-54326c1c15a1"`
- Accept-Ranges: `bytes`
- Content-Length: `128`
- Keep-Alive: `timeout=5, max=100`
- Connection: `Keep-Alive`
- Content-Type: `text/html; charset=UTF-8`

The packet bytes pane shows the raw data of the response.

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?
Browser and server are running HTTP 1.1
2. What languages (if any) does your browser indicate that it can accept to the server?
Accept-Language: en-US,en;q=0.5
3. What is the IP address of your computer? Of the `gaia.cs.umass.edu` server?
My computer: 192.168.1.10, `gaia.cs.umass.edu`: 128.119.245.12
4. What is the status code returned from the server to your browser?
200 OK

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

Last-Modified: Thu, 08 Dec 2016 06:59:01 GMT\r\n

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

128

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.

No

The image displays two screenshots of the Wireshark network protocol analyzer interface, illustrating the capture and analysis of HTTP traffic.

Screenshot 1 (Top):

- Filter:** http
- Packets List:** Shows four captured packets. Packet 67 is a GET request from 192.168.1.10 to 128.119.245.12 for /wireshark-labs/HTTP-wireshark-file2.html.
- Packet Details:** Expanded for packet 67, showing:
 - Frame 67: 386 bytes on wire (3088 bits), 386 bytes captured (3088 bits) on interface 0
 - Ethernet II, Src: LiteonTe_b5:42:55, Dst: ZlcomE_56:fd:9f
 - Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.245.12
 - 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]
 - [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
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv=45.0) Gecko/20100101 Firefox/45.0\r\n
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
 - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
 - [HTTP request 1/2]
 - [Response in frame: 71]
- Packet Bytes:** Hexadecimal and ASCII representation of the raw packet data.

Screenshot 2 (Bottom):

- Filter:** http
- Packets List:** Same as Screenshot 1, showing the same four packets.
- Packet Details:** Expanded for packet 71, showing:
 - > 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
 - [HTTP response 1/2]
 - [Time since request: 0.267667000 seconds]
 - [Request in frame: 67]
 - [Next request in frame: 92]
 - [Next response in frame: 93]
 - File Data: 371 bytes
 - Line-based text data: text/html
 - \n
 - <html>\n
 - \n
 - Congratulations again! Now you've downloaded the file lab2-2.html.
\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
\n
 - will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
\n
 - field in your browser's HTTP GET request to the server.\n
 - \n
 - </html>\n
- Packet Bytes:** Hexadecimal and ASCII representation of the raw packet data.

The top screenshot shows a packet capture of an HTTP GET request. The packet list shows a GET request from 192.168.1.10 to 128.119.245.12. The packet details pane shows the request structure, including the Host: gaia.cs.umass.edu, User-Agent: Mozilla/5.0, and various headers. The packet bytes pane shows the raw data of the request.

The bottom screenshot shows the corresponding HTTP response. The packet list shows a 304 Not Modified response from 128.119.245.12 to 192.168.1.10. The packet details pane shows the response structure, including the Status Code: 304, Response Phrase: Not Modified, and various headers. The packet bytes pane shows the raw data of the response.

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?

No

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

Yes. Because of the line base text data field

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?

Yes. If-Modified-Since: Thu, 08 Dec 2016 06:59:01 GMT\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.

HTTP/1.1 304 Not Modified. The server didn't return the contents of the file since the browser loaded it from its cache.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows several packets, with packet 72 being the first GET request and packet 79 being the response. The packet details pane for packet 79 shows the response status code 200 OK. The packet bytes pane shows the raw data of the response, which is a 304 Not Modified response.

No.	Time	Source	Destination	Protocol	Length	Info
72	9.369410	192.168.1.10	128.119.245.12	HTTP	386	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
79	9.626587	128.119.245.12	192.168.1.10	HTTP	711	HTTP/1.1 200 OK (text/html)

Frame 79: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface 0
> Ethernet II, Src: ZioncomE_56:fd:9f (78:44:76:56:fd:9f), Dst: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 1891, Seq: 4207, Ack: 333, Len: 657
✚ [4 Reassembled TCP Segments (4863 bytes): #75(1402), #76(1402), #78(1402), #79(657)]
[Frame 75, payload: 0-1401 (1402 bytes)]
[Frame 76, payload: 1402-2803 (1402 bytes)]
[Frame 78, payload: 2804-4205 (1402 bytes)]
[Frame 79, payload: 4206-4862 (657 bytes)]
[Segment count: 4]
[Reassembled TCP length: 4863]
[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a2054...]
✚ Hypertext Transfer Protocol
✚ HTTP/1.1 200 OK\r\n
 > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 Request Version: HTTP/1.1
 Status Code: 200
 Response Phrase: OK
 Date: Thu, 08 Dec 2016 15:52:00 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev Perl/v5.16.3\r\n
 Last-Modified: Thu, 08 Dec 2016 06:59:01 GMT\r\n
 Etag: "1194-543202c1bd339"\r\n
 Accept-Ranges: bytes\r\n
0000 c8 ff 28 b5 42 55 78 44 76 56 fd 9f 08 00 45 00 ...(.BUXD vV....E.
0010 02 b9 e6 12 40 00 28 06 32 f6 80 77 f5 0c c0 a8 ...@.(. 2..w....
0020 01 0a 00 50 07 63 eb cf 28 e8 29 1f ab b4 50 18 ...P.c.. (.)...P.
0030 00 ed 91 18 00 00 20 6c 61 77 2e 0a 0a 3c 2f 70 l aw...</p
0040 3e 3c 70 3e 3c 61 20 6e 61 6d 65 3d 22 38 22 3e ><p><a n ame="8">
0050 3c 73 74 72 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e <h3>Amen
0060 64 6d 65 6e 74 20 56 49 49 49 3c 2f 68 33 3e 3c dment VI II</h3><

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?

1 HTTP GET request sent. Packet 72

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

Packet 79

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

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?

4

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
719.799830		192.168.1.10	128.119.245.12	HTTP	386	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
7510.063782		128.119.245.12	192.168.1.10	HTTP	1129	HTTP/1.1 200 OK (text/html)
7610.082453		192.168.1.10	128.119.245.12	HTTP	403	GET /pearson.png HTTP/1.1
8210.350699		128.119.245.12	192.168.1.10	HTTP	863	HTTP/1.1 200 OK (PNG)
10010.881073		192.168.1.10	128.119.240.90	HTTP	417	GET /-kurose/cover_5th_ed.jpg HTTP/1.1
11111.139272		128.119.240.90	192.168.1.10	HTTP	510	HTTP/1.1 302 Found (text/html)
12511.666499		192.168.1.10	128.119.240.90	HTTP	417	GET /-kurose/cover_5th_ed.jpg HTTP/1.1

> Frame 125: 417 bytes on wire (3336 bits), 417 bytes captured (3336 bits) on interface 0

> Ethernet II, Src: LiteonTe_b5:42:55 (c8:ff:28:b5:42:55), Dst: ZioncomE_56:fd:9f (78:44:76:56:fd:9f)

> Internet Protocol Version 4, Src: 192.168.1.10, Dst: 128.119.240.90

> Transmission Control Protocol, Src Port: 24218, Dst Port: 80, Seq: 1, Ack: 1, Len: 363

> Hypertext Transfer Protocol

> GET /-kurose/cover_5th_ed.jpg HTTP/1.1\r\n

Host: caite.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0\r\n

Accept: image/png,image/*;q=0.8,*/*;q=0.5\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n

Connection: keep-alive\r\n

\r\n

[Full request URI: http://caite.cs.umass.edu/-kurose/cover_5th_ed.jpg]

[HTTP request 1/1]

[Response in frame: 248]

0000 78 44 76 56 fd 9f c8 ff 28 b5 42 55 08 00 45 00 xDv....(.BU..E.

0010 01 93 6e c7 40 00 80 06 57 f9 c0 a8 01 0a 80 77 .n.0...W.....

0020 70 5a 5e 9a 00 50 f6 12 01 12 64 b5 71 4a 50 18 .Z'.P...d.GJP.

0030 01 01 90 e6 00 00 47 45 54 20 2f 7e 6b 75 72 6fGE T /-kur

0040 73 65 2f 63 6f 76 65 72 5f 35 74 68 5f 65 64 2a se/cover_5th_ed

0050 6a 70 67 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f jpg HTTP /1.1..H

0060 73 74 3a 20 63 61 69 74 65 2e 63 73 2e 75 6d 61 st: caite.cs.uma

0070 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ss.edu.. User-Age

Frame (frame), 417 bytes

Packets: 340 · Displayed: 12 (3.5%) · Dropped: 0 (0.0%)

Profile: Default

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

4. Initial page: 128.119.245.12, Pearson's logo: 128.119.245.12, Cover 5th ed:128.119.240.90, 128.119.240.90

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

Yes, by checking the TCP ports we can see if our files were downloaded serially or in parallel.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
397.2.175350		125.234.51.41	192.168.1.10	HTTP	1428	HTTP/1.1 206 Partial Content (application/octet-stream)
445.10.560344		192.168.1.10	128.119.245.12	HTTP	401	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
449.10.824765		128.119.245.12	192.168.1.10	HTTP	773	HTTP/1.1 401 Unauthorized (text/html)
486.16.412722		192.168.1.10	128.119.245.12	HTTP	460	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
492.16.669430		128.119.245.12	192.168.1.10	HTTP	585	HTTP/1.1 404 Not Found (text/html)
904.33.732009		192.168.1.10	123.30.175.52	HTTP	1361	GET /show?show=_0Zra50vdaveYq3oIXBe3Jsg0cI6wR5Q-UxIwmB1sxp8P1WmQYZXTpuAc3*XoDEGo92Ar8t*ppChS3eHzWnX1KDpCZ3f-VGbY...

Checksum: 0x9dc7 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [SEQ/ACK analysis]

> Hypertext Transfer Protocol

> GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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

> Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm0=\r\n

Credentials: wireshark-students:network

\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wiresharkfile5.html]

[HTTP request 1/1]

[Response in frame: 492]

2150 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e q=0.5..A ccept-En

2160 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 coding: gzip, de

2170 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f late..C connectio

2180 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 n: keep-alive..A

2190 75 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 uthoriza tion: Ba

21a0 73 69 63 20 64 32 6c 79 5a 58 4e 6f 59 58 4a 72 sic d2ly ZXNoYXJr

21b0 4c 58 4e 30 64 57 52 6c 62 6e 52 7a 4f 6d 35 6c LXN0dWRl bnRzOm5l

21c0 64 48 64 76 63 6d 73 3d 0d 0a 0d 0a dHdvcm0=...

HTTP Authorization header (http.authorization), 59 bytes

Packets: 911 · Displayed: 7 (0.8%)

Profile: Default

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

401 Unauthorized

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

The HTTP GET includes the Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n