

Lab2

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

- My browser is running HTTP version 1.1.

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

- en-US, en; q=0.8\r\n. I don't know what half of that means, but the first part has to mean "United States English."

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

- My IP address is 192.168.1.249, and gaia.cs.umass server is 128.199.245.12.

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

- The status code is 200.

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

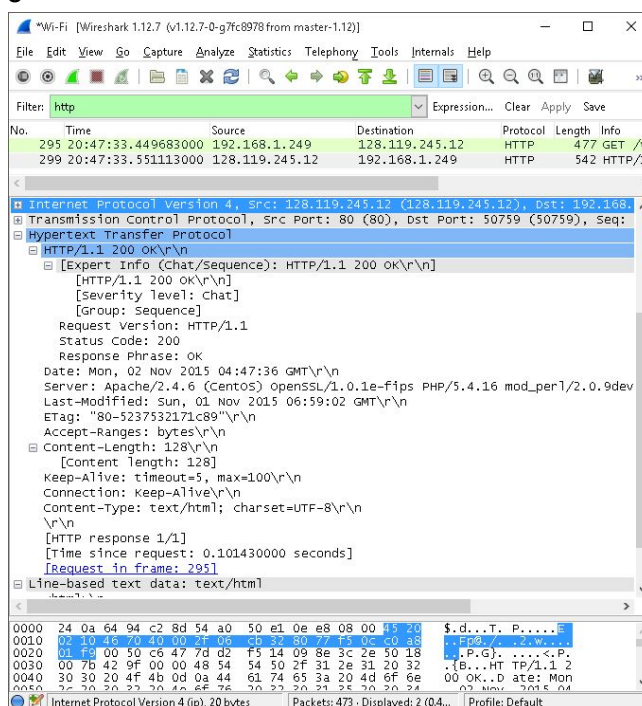
- The HTML file was last modified Sunday, 01 Nov 2015 06:59:02 GMT

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

- 128 bytes were returned to my browser.

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.

- Nothing that I could find. I couldn't find anything in the raw data window that wasn't in the packet-listing window.



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, I do not.

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

- Yes, the server return the contents of the file. It is under “Line-based text data:”

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 I do. It says, “Sun, 01 Nov 2015 06:59:02 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.

- Status code is 304. Response phrase is “Not modified”, and there are no contents of the file because nothing has changed since the last request.

*Wi-Fi [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
204	21:20:30.273336000	192.168.1.249	128.119.245.12	HTTP	477	GET /w...
208	21:20:30.378339000	128.119.245.12	192.168.1.249	HTTP	786	HTTP/1...
687	21:20:47.014389000	192.168.1.249	128.119.245.12	HTTP	589	GET /w...
692	21:20:47.122452000	128.119.245.12	192.168.1.249	HTTP	296	HTTP/1...

< >

Frame 692: 296 bytes on wire (2368 bits), 296 bytes captured (2368 bits) on interf.

Ethernet II, Src: AsustekC_e1:0e:e8 (54:a0:50:e1:0e:e8), Dst: Azurewav_94:c2:8d (2...

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1...

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 50966 (50966), Seq: 1,

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]

[HTTP/1.1 304 Not Modified\r\n]

[Severity level: chat]

[Group: sequence]

Request Version: HTTP/1.1

Status Code: 304

Response Phrase: Not Modified

Date: Mon, 02 Nov 2015 05:20:47 GMT\r\n

Server: Apache/2.4.6 (Centos) openssl/1.0.1e-fips PHP/5.4.16 mod_perl/2.0.9dev P...

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=100\r\n

ETag: "173-52375321714b9"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.108063000 seconds]

[Request in frame: 687]

< >

0000 24 0a 64 94 c2 8d 54 a0 50 e1 0e e8 08 00 45 20 \$.d...T. P....E

0010 01 1a 16 e4 40 00 2f 06 fb b4 80 77 f5 0c c0 a8 ...@./...w....

0020 01 f9 00 50 c7 16 d9 60 05 c2 e7 74 10 85 50 18 ...P... ..t..P.

0030 00 7b df b3 00 00 48 54 54 50 2f 31 2e 31 20 33 .{....HT TP/1.1 3

0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not M odified.

0050 02 44 61 74 65 20 20 4d 6f 62 2c 20 20 22 20 4d 02 M odified.

File: "C:\Users\josep\AppData\Local\Temp\..." Packets: 951 · Displayed: 4 (0.4... Profile: Default

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?

- My browser only sent 1 HTTP GET request. The first packet that has the request has the GET message for the Bill of Rights.

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

- The first response packet contains the status code and phrase for the HTTP GET request.

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

- The status code is 200, and the phrase is "OK"

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

- There were four segments.

The image shows a Wireshark network traffic capture. The top pane displays a list of packets. Packet 147 is an HTTP GET request from 192.168.1.249 to 128.119.245.12. Packet 155 is the corresponding HTTP 200 OK response from 128.119.245.12 to 192.168.1.249. The middle pane shows the details of the selected packet (155), including the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
147	21:41:56.046353000	192.168.1.249	128.119.245.12	HTTP	477	GET /wireshark-labs/HTTP-wireshark-file
155	21:41:56.159409000	128.119.245.12	192.168.1.249	HTTP	537	HTTP/1.1 200 OK (text/html)

[4 Reassembled TCP Segments (4863 bytes): #152(1460), #153(1460), #154(1460), #155(483)]

- [Frame: 152, payload: 0-1459 (1460 bytes)]
- [Frame: 153, payload: 1460-2919 (1460 bytes)]
- [Frame: 154, payload: 2920-4379 (1460 bytes)]
- [Frame: 155, payload: 4380-4862 (483 bytes)]

[Segment count: 4]
[Reassembled TCP length: 4863]
[Reassembled TCP data: 485454502f312e3120323030204f4b0d0a446174653a204d...]

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
- Date: Mon, 02 Nov 2015 05:41:56 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: Sun, 01 Nov 2015 06:59:02 GMT\r\n
- ETag: "1194-523753216e1f0"\r\n
- Accept-Ranges: bytes\r\n

0000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
0010 0a 44 61 74 65 3a 20 4d 6f 6e 2c 20 30 32 20 4e .Date: M on, 02 N
0020 6f 76 20 32 30 31 35 20 30 35 3a 34 31 3a 35 36 ov 2015 05:41:56
0030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap
0040 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/2.4 .6 (Cent
0050 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) open SSL/1.0.
0060 31 65 2d 66 69 70 73 20 50 48 50 2f 35 2e 34 2e le-fips PHP/5.4.
0070 31 36 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 16 mod_p erl/2.0.
0080 39 64 65 76 20 50 65 72 6c 2f 76 35 2e 31 36 2e 9dev Per l/v5.16.
0090 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64 3..Last- Modified
00a0 3a 20 53 75 6e 2c 20 30 31 20 4e 6f 76 20 32 30 : Sun, 0 1 Nov 20
00b0 31 35 20 30 36 3a 35 39 3a 30 32 20 47 4d 54 0d 15 06:59 :02 GMT.
00c0 0a 45 54 61 67 3a 20 22 31 31 39 34 2d 35 32 33 ETag: " 1194-523

Frame (537 bytes): Reassembled TCP (4863 bytes)

TCP Segment (tcp.segment), 1460 bytes

Packets: 416 · Displayed: 2 (0.5%) · 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?

- There were 4 GET requests.
 - a. /wireshark-labs/HTTP-wireshark-file4.html
 - b. /~kurose/cover_5th_ed.jpg
 - c. /assets/hip/us/hip_us_pearsonhighered/images/pearson_logo.gif
 - d. /~kurose/cover_5th_ed.jpg

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.

- Chrome downloaded the images serially. I know that because the second image didn't start to load until the first one was completely done.

Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)

Filter: http

No.	Time	Source	Destination	Protocol	Length	Info
119	21:50:36.153008000	192.168.1.249	128.119.245.12	HTTP	477	GET /wireshark-labs/HTTP-wireshark-f
124	21:50:36.266354000	128.119.245.12	192.168.1.249	HTTP	1156	HTTP/1.1 200 OK (text/html)
137	21:50:36.510224000	192.168.1.249	128.119.240.90	HTTP	462	GET /~kurose/cover_5th_ed.jpg HTTP/1
140	21:50:36.512283000	192.168.1.249	165.193.140.14	HTTP	503	GET /assets/hip/us/hip_us_pearsonhigh
146	21:50:36.619281000	128.119.240.90	192.168.1.249	HTTP	510	HTTP/1.1 302 Found (text/html)
160	21:50:36.744764000	192.168.1.249	128.119.240.90	HTTP	462	GET /~kurose/cover_5th_ed.jpg HTTP/1
161	21:50:36.756007000	165.193.140.14	192.168.1.249	HTTP	998	HTTP/1.1 200 OK (GIF89a)
281	21:50:37.357851000	128.119.240.90	192.168.1.249	HTTP	526	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 119: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface 0

Ethernet II, Src: Azureway_94:c2:8d (24:0a:64:94:c2:8d), Dst: AsustekC_e1:0e:e8 (54:a0:50:e1:0e:e8)

Internet Protocol Version 4, Src: 192.168.1.249 (192.168.1.249), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 51101 (51101), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 423

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

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Sa

DNT: 1\r\n

Accept-Encoding: gzip, deflate, sdch\r\n

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

\r\n

0000 54 a0 50 e1 0e e8 24 0a 64 94 c2 8d 08 00 45 00 T.P...\$. d....E.

0010 01 cf 27 8b 40 00 80 06 99 78 c0 a8 01 f9 80 77 ...@... .x....w

0020 05 0c c7 9d 00 50 9a 8b 93 2b 2e ac 8e 53 50 18P...+.SP.

0030 f1 00 cc 8b 00 00 47 45 54 20 2f 77 69 72 65 73GE T/wires

0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w

0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 34 2e 68 reshark -file4.h

0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1..Ho

0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas

0080 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu..C onnectio

0090 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 n: keep- alive..A

00a0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html

00b0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 ,applica tion/xht

00c0 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 63 61 74 69 ml+xml.a nnlicati

File: "C:\Users\josep\AppData\Local\Temp\..." Packets: 411 · Displayed: 8 (1.9%) · Dropped: 0 (0.0%) Profile: Default

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

- The status code was 401 and the phrase was "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 new field is "Authorization", and it contains the username and password that I typed in.

The image shows a Wireshark 1.12.7 capture of network traffic. The filter is set to 'http'. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
182	22:02:29.036467000	192.168.1.249	128.119.245.12	HTTP	493	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
186	22:02:29.161660000	128.119.245.12	192.168.1.249	HTTP	773	HTTP/1.1 401 Unauthorized (text/html)
1068	22:02:58.934147000	192.168.1.249	128.119.245.12	HTTP	552	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1073	22:02:59.037579000	128.119.245.12	192.168.1.249	HTTP	546	HTTP/1.1 200 OK (text/html)

The packet details pane shows the selected packet (No. 186) expanded, displaying the following fields:

- Frame 182: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface 0
- Ethernet II, Src: Azurewaw_94:c2:8d (24:0a:64:94:c2:8d), Dst: AsustekC_e1:0e:e8 (54:a0:50:e1:0e:e8)
- Internet Protocol Version 4, Src: 192.168.1.249 (192.168.1.249), Dst: 128.119.245.12 (128.119.245.12)
- Transmission Control Protocol, Src Port: 51181 (51181), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 439
- 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
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
 - Upgrade-Insecure-Requests: 1\r\n
 - User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36\r\n
 - Accept-Encoding: gzip, deflate, sdch\r\n
 - Accept-Language: en-US,en;q=0.8\r\n
 - \r\n

The packet bytes pane shows the raw data of the selected packet, starting with:

```
0000 54 a0 50 e1 0e e8 24 0a 64 94 c2 8d 08 00 45 00 T.P...$. d....E.
0010 01 df 28 4e 40 00 80 06 98 a5 c0 a8 01 f9 80 77 ..(N@... ..w
0020 f5 0c c7 ed 00 50 b5 64 f4 92 bf d8 5a 46 50 18 ....P.d ...ZFP.
0030 01 00 89 c5 00 00 47 45 54 20 2f 77 69 72 65 73 .....GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 70 72 6f 74 65 63 hark-lab s/protec
0050 74 65 64 5f 70 61 67 65 73 2f 48 54 54 50 2d 77 ted_page s/HTTP-w
0060 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 35 2e 68 ireshark -file5.h
0070 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1..Ho
0080 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0090 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f s.edu... connectio
00a0 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 41 n: keep- alive..A
00b0 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 6d 6c ccept: t ext/html
00c0 2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 .applicatinn/xht
```