

Arthur Liou
CS372
Lab 2

Notes: I've attached my screenshots and boxed in red where I annotated my output.

Section 1

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

Running HTTP/v1.1

Running HTTP/v1.1

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

I'm assuming the language/file type that the server can accept, but also adding languages to

Accept:

- text/html,
- application/xhtml+xml,
- application/xml;

From "Accept languages:"

- en-US
- en

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

My Computer: 192.168.146.130

Server: 128.119.245.12

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

200

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

Monday, October 15, 2018 05:59:01 GMT

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

552 bytes are returned in the 200 status code request.

For content, it shows that file data is **128 bytes.**

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

Yes, Server info (Apache, etc.), Date, last modified, etc. These, and more, are not shown in the packet-listing window (I'm assuming just the summary), but are shown in the details of the selected packet from the packet-listing window.

Headers wise, I see an interesting "Q...E...@...(and more)". Please see the screenshots for what I'm taking about

Screenshots for Section 1 (3x)

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
220	1.764048	192.168.146.130	128.119.245.12	HTTP	506	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
232	1.846505	128.119.245.12	192.168.146.130	HTTP	552	HTTP/1.1 200 OK (text/html)

Internet Protocol Version 4, Src: 192.168.146.130, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 55307, Dst Port: 80, Seq: 1, Ack: 1, Len: 440

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

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/53...

DNT: 1\r\n

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

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

\r\n

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

[HTTP request 1/1]

[Response in frame: 232]

0000 cc 03 d9 e9 86 e8 8c 85 90 c9 51 aa 08 00 45 00Q...E-

0010 01 ec 00 00 40 00 40 06 70 5d c0 a8 92 82 80 77@.p]...w

wireshark_en0_20181015115214.qkWYYE.pcapng Packets: 384 · Displayed: 2 (0.5%) Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
220	1.764048	192.168.146.130	128.119.245.12	HTTP	506	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
232	1.846505	128.119.245.12	192.168.146.130	HTTP	552	HTTP/1.1 200 OK (text/html)

Ethernet II, Src: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8), Dst: Apple_c9:51:aa (8c:85:90:c9:51:aa)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.146.130

Transmission Control Protocol, Src Port: 80, Dst Port: 55307, Seq: 1, Ack: 441, Len: 486

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Mon, 15 Oct 2018 18:52:15 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Last-Modified: Mon, 15 Oct 2018 05:59:01 GMT\r\n

Etag: "80-5783e223ec887"\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 1/1]

[Time since request: 0.082457000 seconds]

[Request in frame: 220]

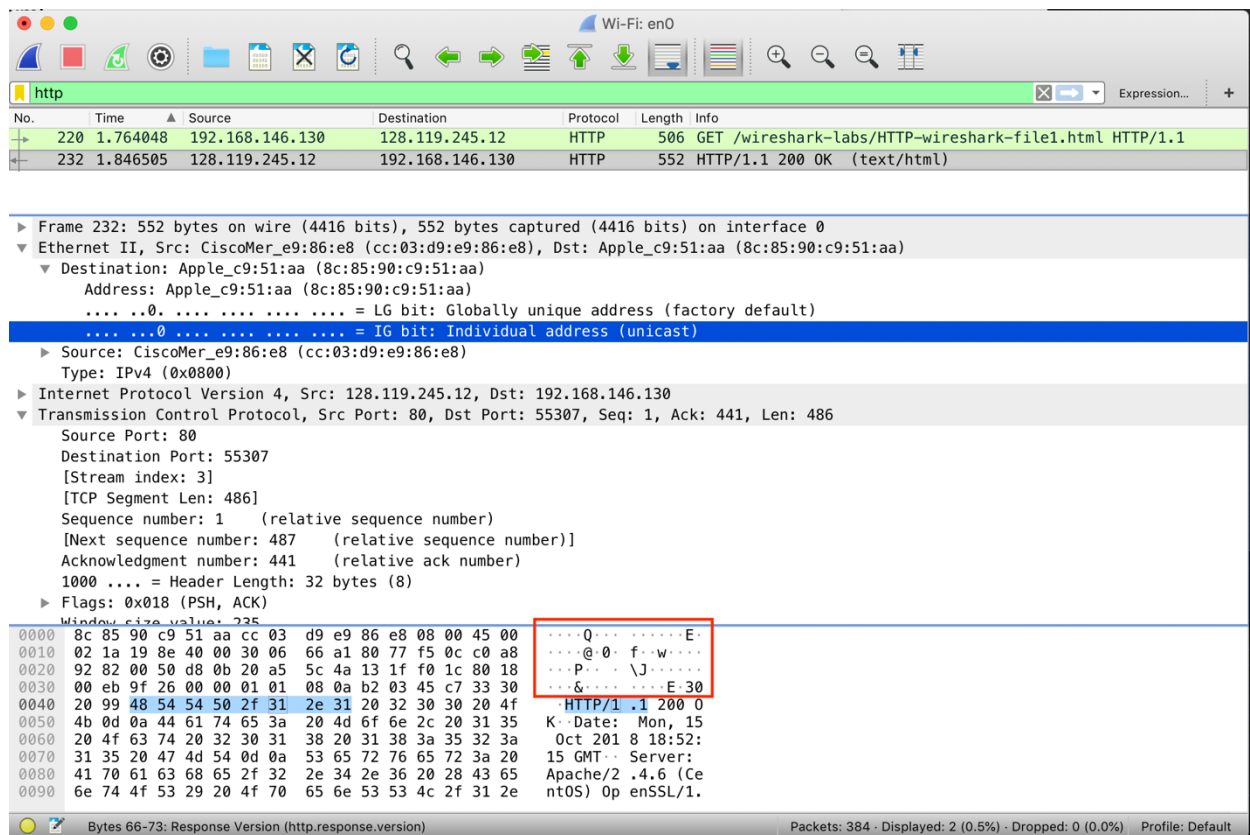
File Data: 128 bytes

Line-based text data: text/html (4 lines)

0000 8c 85 90 c9 51 aa cc 03 d9 e9 86 e8 08 00 45 00Q...E-

0010 02 1a 19 8e 40 00 30 06 66 a1 80 77 f5 0c c0 a8@.f..w...

wireshark_en0_20181015115214.qkWYYE.pcapng Packets: 384 · Displayed: 2 (0.5%) · Dropped: 0 (0.0%) Profile: Default



Section 2

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, not in the first HTTP GET request.

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

Yes, I can see it under the “Line-Based 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: Mon, 15 Oct 2018 05:59:01 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 Status Code: 304 (Not Modified)

No, the server did not. I looked for the “Line-Based Text Data” field and within the raw data and didn’t see the file contents being explicitly returned by the server

Screenshots for Part 2 (3x)

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
153	1.451619	192.168.146.130	128.119.245.12	HTTP	506	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
155	1.531675	128.119.245.12	192.168.146.130	HTTP	796	HTTP/1.1 200 OK (text/html)
269	2.650652	192.168.146.130	128.119.245.12	HTTP	618	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
281	2.729850	128.119.245.12	192.168.146.130	HTTP	305	HTTP/1.1 304 Not Modified

Ethernet II, Src: Apple_c9:51:aa (8c:85:90:c9:51:aa), Dst: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)

Internet Protocol Version 4, Src: 192.168.146.130, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 56788, Dst Port: 80, Seq: 441, Ack: 731, Len: 552

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_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\n

DNT: 1\r\n

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

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en;q=0.9\r\n

If-None-Match: "173-5783e223eb8e7"\r\n

If-Modified-Since: Mon, 15 Oct 2018 05:59:01 GMT\r\n

\r\n

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

[HTTP request 2/2]

0100 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 -Accept- Encoding

0100 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d : gzip, deflate

0100 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 -Accept- Language

0200 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 : en-US, en;q=0.9

0210 0d 0a 49 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a : If-None-Match:

0220 20 22 31 37 33 2d 35 37 38 33 65 32 33 65 62 "173-57 83e223eb

0230 38 65 37 22 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 8e7"-If -Modifie

0240 64 2d 53 69 6e 63 65 3a 20 4d 6f 6e 2c 20 31 35 d-Since: Mon, 15

0250 20 4f 63 74 2d 32 31 38 20 30 35 3a 35 39 3a Oct 201 8 05:59:

0260 30 31 20 47 4d 54 0d 0a 0d 0a 01 GMT--

Request line (http request line), 60 bytes

Packets: 428 - Displayed: 4 (0.9%) - Dropped: 0 (0.0%) - Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
153	1.451619	192.168.146.130	128.119.245.12	HTTP	506	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
155	1.531675	128.119.245.12	192.168.146.130	HTTP	796	HTTP/1.1 200 OK (text/html)
269	2.650652	192.168.146.130	128.119.245.12	HTTP	618	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
281	2.729850	128.119.245.12	192.168.146.130	HTTP	305	HTTP/1.1 304 Not Modified

Accept-Ranges: bytes\r\n

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

\r\n

[HTTP response 1/2]

[Time since request: 0.080056000 seconds]

[Request in frame: 153]

[Next request in frame: 269]

[Next response in frame: 281]

File Data: 371 bytes

Line-based text data: text/html (10 lines)

\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

0200 2d 53 49 4e 43 45 3c 62 72 3e 0a 66 69 65 6c 64 -SINCE<b r> field

0200 20 69 6e 28 79 6f 75 72 20 62 72 6f 77 73 65 72 in your browser

0210 27 73 20 48 54 54 50 20 47 45 54 20 72 65 71 75 's HTTP GET requ

0300 65 73 74 20 74 6f 20 74 68 65 20 73 65 72 76 65 est to t he serve

0310 72 2e 0a 0a 3c 2f 68 74 6d 6c 3e 0a r> </ht ml>

wireshark_en0_20181015142236.NhZro.pcapng

Packets: 428 - Displayed: 4 (0.9%) - Dropped: 0 (0.0%) - Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
153	1.451619	192.168.146.130	128.119.245.12	HTTP	506	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
155	1.531675	128.119.245.12	192.168.146.130	HTTP	796	HTTP/1.1 200 OK (text/html)
269	2.650652	192.168.146.130	128.119.245.12	HTTP	618	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
281	2.729850	128.119.245.12	192.168.146.130	HTTP	305	HTTP/1.1 304 Not Modified

Frame 281: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on interface 0

Ethernet II, Src: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8), Dst: Apple_c9:51:aa (8c:85:90:c9:51:aa)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.146.130

Transmission Control Protocol, Src Port: 80, Dst Port: 56788, Seq: 731, Ack: 993, Len: 239

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Mon, 15 Oct 2018 21:22:38 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=99\r\n

Etag: "173-5783e223eb8e7"\r\n

\r\n

[HTTP response 2/2]

[Time since request: 0.079198000 seconds]

[Prev request in frame: 153]

[Prev response in frame: 155]

[Request in frame: 269]

00f0 69 76 65 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a ive Kee p-Alive:

0100 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d timeout =5, max=

0110 39 39 0d 0a 45 54 61 67 3a 20 22 31 37 33 2d 35 99-ETag: "173-5

0120 37 38 33 65 32 32 33 65 62 38 65 37 22 0d 0a 0d 783e223e b8e7"--

0130 0a

wireshark_en0_20181015142236.NhZro.pcapng

Packets: 428 - Displayed: 4 (0.9%) - Dropped: 0 (0.0%) - Profile: Default

Section 3

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

1x HTTP GET request messages

Packet Number 117

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

Packet Number 124

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

Status Code: 200

Response Phrase: 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 data-containing TCP segments were needed.

Screenshots for Part 3 (2x)

The top screenshot shows a Wireshark capture of network traffic. The packet list pane at the top shows several packets. Packet 117 is selected, which is an HTTP GET request from 192.168.146.130 to 128.119.245.12. The packet details pane for packet 117 shows the Hypertext Transfer Protocol section with the request method GET and the request URI /wireshark-labs/HTTP-wireshark-file3.html.

The bottom screenshot shows the same capture with packet 124 selected, which is the HTTP response from 128.119.245.12 to 192.168.146.130. The packet details pane for packet 124 shows the Hypertext Transfer Protocol section with the status code 200 and the response phrase OK.

Section 4

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

a) 3 HTTP GET request messages

@Instructors, please specify whether you want the IP address or the URL/web address (question could be considered ambiguous)

b) All 3 were going to the IP Address: 128.119.245.12

Web Address/URL

- 1) /wireshark-labs/HTTP-wireshark-file4.html
- 2) /pearson.png
- 3) /~kurose/cover_5th_ed.jpgs

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.

Serially. In the screenshot, we can see major differences in time along side the fact that the second image GET occurred significantly after image 1's GET completed. Packet 189 vs Packet 166. If they were downloaded in parallel, we would have seen both GET requests very close together (time and packet-wise). While it is possible that in parallel, the 1st GET request could come back before the 2nd GET goes out, it is not very likely (time to download from a server vs time to execute a request)

The screenshot shows a Wireshark packet capture on the 'http' filter. The packet list pane displays several packets, with packets 189 and 326 highlighted. Packet 189 is a GET request for '/~kurose/cover_5th_ed.jpg' and packet 326 is the corresponding 200 OK response. The packet details pane for packet 189 shows the full HTTP request, including the URI 'http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg'. The packet bytes pane at the bottom shows the raw data of the request, including the 'Host' and 'User-Agent' headers.

No.	Time	Source	Destination	Protocol	Length	Info
149	1.394200	192.168.146.130	128.119.245.12	HTTP	506	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
158	1.475789	128.119.245.12	192.168.146.130	HTTP	1139	HTTP/1.1 200 OK (text/html)
160	1.520739	192.168.146.130	128.119.245.12	HTTP	477	GET /pearson.png HTTP/1.1
166	1.603603	128.119.245.12	192.168.146.130	HTTP	781	HTTP/1.1 200 OK (PNG)
189	1.769702	192.168.146.130	128.119.245.12	HTTP	491	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
326	2.075232	128.119.245.12	192.168.146.130	HTTP	1472	HTTP/1.1 200 OK (JPEG JFIF image)

Frame 189: 491 bytes on wire (3928 bits), 491 bytes captured (3928 bits) on interface 0
Ethernet II, Src: Apple_c9:51:aa (8c:85:90:c9:51:aa), Dst: CiscoMer_e9:86:e8 (cc:03:d9:e9:86:e8)
Internet Protocol Version 4, Src: 192.168.146.130, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 57340, Dst Port: 80, Seq: 1, Ack: 1, Len: 425
Hypertext Transfer Protocol
GET /~kurose/cover_5th_ed.jpg HTTP/1.1\r\nHost: manic.cs.umass.edu\r\nConnection: keep-alive\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36\r\nDNT: 1\r\nAccept: image/webp,image/apng,image/*,*/*;q=0.8\r\nReferer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Full request URI: http://manic.cs.umass.edu/~kurose/cover_5th_ed.jpg]
[HTTP request 1/1]
[Response in frame: 326]

0040 a7 58 47 45 54 20 2f 7e 6b 75 72 6f 73 65 2f 63 -XGET /~ kurose/c
0050 6f 76 65 72 5f 35 74 68 5f 65 64 2e 6a 70 67 20 over_5th _ed.jpg
0060 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 HTTP/1.1 ..Host:
0070 6d 61 6e 69 63 2e 63 73 2e 75 6d 61 73 73 2e 65 manic.cs .umass.e
0080 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 du..Conn ection:

The full requested URI (including host name) (http.request.full_uri)

Packets: 506 - Displayed: 6 (1.2%) - Dropped: 0 (0.0%) Profile: Default

Section 5

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

Status Code: 401

Response Phrase: 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?

Authorization (also includes credentials as a sub-field)

Screenshots for Section 5 (2x)

The first screenshot shows a packet capture of an HTTP response. The packet list shows a GET request (No. 227) and an unauthorized response (No. 238). The packet details pane for the response (No. 238) shows the status code 401 and the phrase 'Unauthorized'. The packet bytes pane shows the raw data of the response.

The second screenshot shows a packet capture of an HTTP request. The packet list shows a GET request (No. 782) and an OK response (No. 794). The packet details pane for the request (No. 782) shows the 'Authorization' field with the value 'Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\\r\\n'. The packet bytes pane shows the raw data of the request.