

Lab 6

Wireshark HTTP

Nicole Merritt



Section 1

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

HTTP 1.1

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

En-ca

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

My IP: 192.168.2.25 uMass IP: 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, 22 Mar 2018 05:59:02 GMT

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 headers within the data that are not displayed in the packet-listing window

http						
No.	Time	Source	Destination	Protocol	Length	Info
31	5.089568	192.168.2.25	128.119.245.12	HTTP	471	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
33	5.116692	128.119.245.12	192.168.2.25	HTTP	552	HTTP/1.1 200 OK (text/html)

▶ Frame 31: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits) on interface 0
▶ Ethernet II, Src: Apple_a4:89:fe (5c:f9:38:a4:89:fe), Dst: Tp-LinkT_01:a6:eb (d4:6e:0e:01:a6:eb)
▶ Internet Protocol Version 4, Src: 192.168.2.25, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 56640, Dst Port: 80, Seq: 1, Ack: 1, Len: 405
▼ 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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/604.5.6 (KHTML, like Gecko) Version/11.0.3 Safari/604.5.6\r\n
Accept-Language: en-ca\r\n
DNT: 1\r\n
Accept-Encoding: gzip, deflate\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: 33]

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

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

It did return the contents of the file. I can tell by looking at the Line-based text data.

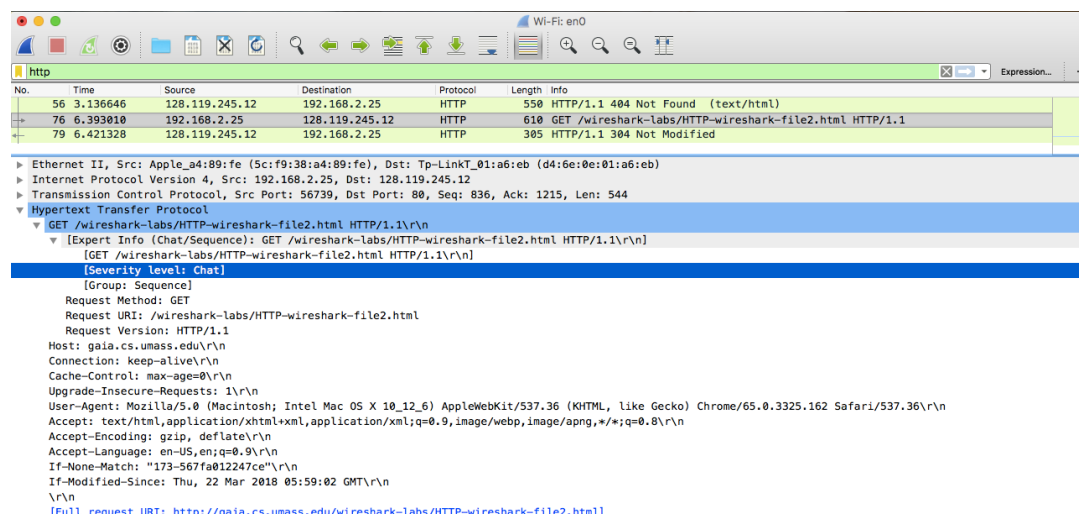
```
Line-based text data: text/html
\n
<html>\n
\n
Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
This file's last modification date will not change. <p>\n
Thus if you download this multiple times on your browser, a complete copy <br>\n
will only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\n
\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?

THU, 22 Mar 2018 05:59:02 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.

No. Because 304 Not Modified



Section 3

1. 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?

1 HTTP GET request message was sent. Packet number 4

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

9 is the response to the HTTP GET

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

200 OK

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

▶ [4 Reassembled TCP Segments (4861 bytes): #6(1368), #7(1368), #8(1368), #9(757)]

The image shows a Wireshark packet capture window. The top toolbar includes icons for file operations, network analysis, and search. The packet list pane shows two packets: packet 4 (GET request) and packet 9 (200 OK response). The packet details pane for packet 9 is expanded, showing the Hypertext Transfer Protocol section with fields like Request Method, Request URI, Request Version, Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, and Accept-Language. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.027084	10.105.107.164	128.119.245.12	HTTP	498	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
9	0.054389	128.119.245.12	10.105.107.164	HTTP	823	HTTP/1.1 200 OK (text/html)

Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
TCP payload (432 bytes)
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
[GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
[Severity level: Chat]
[Group: Sequence]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file3.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.162 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
[HTTP request 1/1]
[Response in frame: 9]

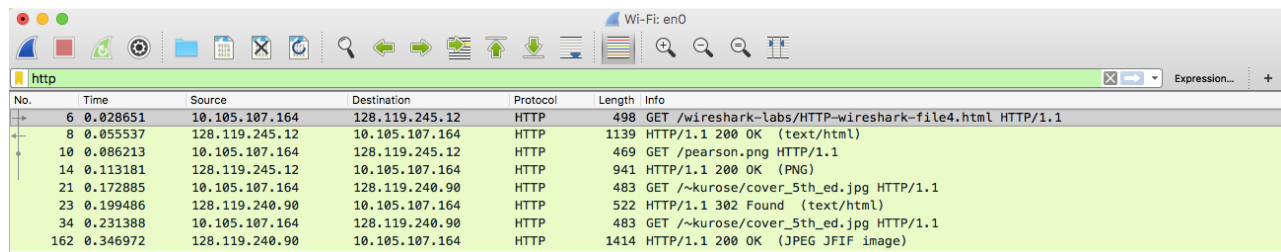
Section 4

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

4 HTTP GET requests were sent. They were sent to addresses 128.119.245.12 & 128.119.240.90

2. 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, because we get multiple GET and RESPONSES sent and received. If it was parallel they would come at the same time.



The image shows a Wireshark packet capture window with the filter 'http'. The packet list shows several HTTP GET requests and responses. The first request is to 128.119.245.12 for /wireshark-labs/HTTP-wireshark-file4.html. Subsequent requests are for /pearson.png and /~kurose/cover_5th_ed.jpg, alternating between the two IP addresses. The responses show status codes 200 OK and 302 Found.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.028651	10.105.107.164	128.119.245.12	HTTP	498	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
8	0.055537	128.119.245.12	10.105.107.164	HTTP	1139	HTTP/1.1 200 OK (text/html)
10	0.086213	10.105.107.164	128.119.245.12	HTTP	469	GET /pearson.png HTTP/1.1
14	0.113181	128.119.245.12	10.105.107.164	HTTP	941	HTTP/1.1 200 OK (PNG)
21	0.172885	10.105.107.164	128.119.240.90	HTTP	483	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
23	0.199486	128.119.240.90	10.105.107.164	HTTP	522	HTTP/1.1 302 Found (text/html)
34	0.231388	10.105.107.164	128.119.240.90	HTTP	483	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
162	0.346972	128.119.240.90	10.105.107.164	HTTP	1414	HTTP/1.1 200 OK (JPEG JFIF image)

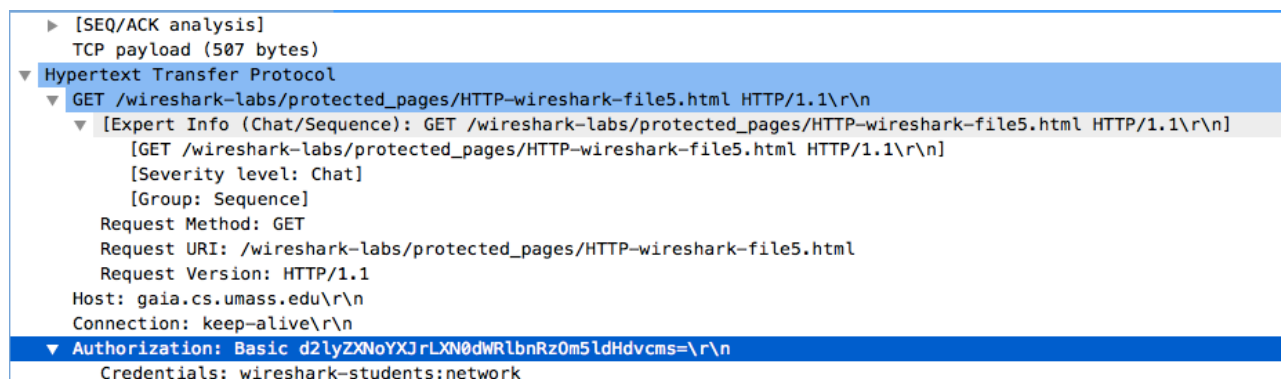
Section 5

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

401 Unauthorized

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

Authorization: Basic



The image shows a Wireshark packet capture window with the filter 'http'. The packet list shows an HTTP GET request to /wireshark-labs/protected_pages/HTTP-wireshark-file5.html. The packet details pane shows the request method, URI, version, host, connection, and the Authorization: Basic header with the value d2lyZXNoYXJrLXN0dWRlbnRz0m5ldHdvcm5=\r\n. The credentials are wireshark-students:network.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.105.107.164	128.119.245.12	HTTP	498	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1

Details pane:

- [Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
- [GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
- [Severity level: Chat]
- [Group: Sequence]
- Request Method: GET
- Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
- Request Version: HTTP/1.1
- Host: gaia.cs.umass.edu\r\n
- Connection: keep-alive\r\n
- Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRz0m5ldHdvcm5=\r\n
- Credentials: wireshark-students:network