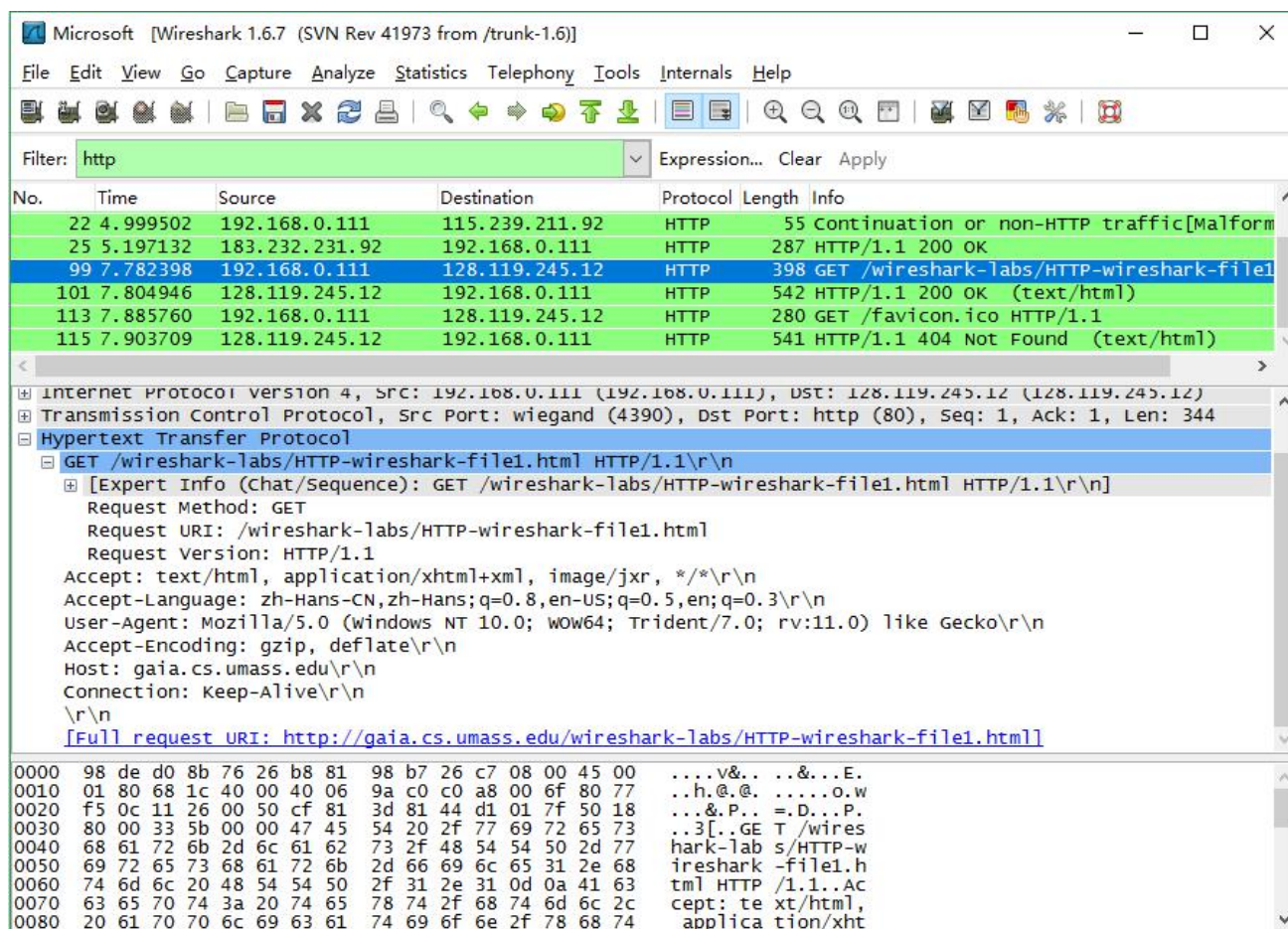


## Data Communications I Lab2 Report

Yang Meng

01679623

10/14/2016



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

Answer: My browser is running HTTP version 1.1. Also, the server is running HTTP version 1.1

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

Answer: Accept language: Simplified Chinese(zh-Hans-CN), English(en-US)

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

Answer: My computer IP: 192.168.0.111; Server IP address: 128.119.245.12;

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

Answer: Status code: 200;

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

Answer: Last-Modified: Friday, 10/14/2016 05:59:01 GMT

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

Answer: Content length: 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.

Answer: No

Microsoft [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
13	0.824117	128.119.245.12	192.168.0.111	HTTP	786	HTTP/1.1 200 OK (text/html)
26	0.870579	192.168.0.111	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
28	0.888518	128.119.245.12	192.168.0.111	HTTP	541	HTTP/1.1 404 Not Found (text/html)
72	2.482402	192.168.0.111	128.119.245.12	HTTP	484	GET /wireshark-labs/HTTP-wireshark-file2
73	2.501127	128.119.245.12	192.168.0.111	HTTP	295	HTTP/1.1 304 Not Modified
75	2.520602	192.168.0.111	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1

Frame 13: 786 bytes on wire (6288 bits), 786 bytes captured (6288 bits)

Ethernet II, Src: 98:de:d0:8b:76:26 (98:de:d0:8b:76:26), Dst: b8:81:98:b7:26:c7 (b8:81:98:b7:26:c7)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.0.111 (192.168.0.111)

Transmission Control Protocol, Src Port: http (80), Dst Port: 6037 (6037), Seq: 1, Ack: 345, Len: 732

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[Message: HTTP/1.1 200 OK\r\n]

[Severity level: chat]

[Group: Sequence]

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK

Date: Sat, 15 Oct 2016 00:10:55 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

```

0000  b8 81 98 b7 26 c7 98 de  d0 8b 76 26 08 00 45 20  ....&... ..v&..E
0010  03 04 07 6b 40 00 33 06  06 ce 80 77 f5 0c c0 a8  ...k@.3. ...w....
0020  00 6f 00 50 17 95 49 79  f9 93 dc ab 0e f2 50 18  ..o.P..Iy .....P.
0030  00 ed fd 07 00 00 48 54  54 50 2f 31 2e 31 20 32  ....HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74  00 OK..D ate: Sat
0050  2c 20 31 35 20 4f 63 74  20 32 30 31 36 20 30 30  , 15 Oct 2016 00
0060  3a 31 30 3a 35 35 20 47  4d 54 0d 0a 53 65 72 76  :10:55 G MT..Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36  er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53  (CentOS ) opensS

```

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, because the server returns the information blow:

```

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 IN-MODIFIED-SINCE<br>\n
field in your browser's HTTP GET request to the server.\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, "If-Modified-Since:" followed by:

```

Host: gaia.cs.umass.edu\r\n
If-Modified-Since: Fri, 14 Oct 2016 05:59:01 GMT\r\n
If-None-Match: "173-53eccec489fc5"\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: 304, Response Phrase: Not Modified; The server didn't return the contents of the file since the copy has already existed in the client.



Microsoft [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:  Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
13	1.220470	192.168.0.111	128.119.245.12	HTTP	398	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
20	1.243527	128.119.245.12	192.168.0.111	HTTP	537	HTTP/1.1 200 OK (text/html)
32	1.292818	192.168.0.111	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
34	1.314364	128.119.245.12	192.168.0.111	HTTP	541	HTTP/1.1 404 Not Found (text/html)
74	2.345468	192.168.0.100	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
75	2.457592	fe80::7833:6b9d:f6aff02::c		SSDP	208	M-SEARCH * HTTP/1.1

Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1 [0]  
 [Message: GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]  
 [Severity level: Chat]  
 [Group: Sequence]  
 Request Method: GET  
 Request URI: /wireshark-labs/HTTP-wireshark-file3.html  
 Request Version: HTTP/1.1  
 Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n  
 Accept-Language: zh-Hans-CN,zh-Hans;q=0.8,en-US;q=0.5,en;q=0.3\r\n  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Host: gaia.cs.umass.edu\r\n  
 Connection: Keep-Alive\r\n  
 \r\n  
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

0000	98 de d0 8b 76 26 b8 81	98 b7 26 c7 08 00 45 00	....v&.. ..&...E.
0010	01 80 68 c2 40 00 40 06	9a 1a c0 a8 00 6f 80 77	..h.@. ....o.w
0020	f5 0c 18 42 00 50 c8 43	37 14 57 46 3f 3c 50 18	...B.P.C 7.WF?<P.
0030	80 00 e9 b5 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 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 33 2e 68	reshark -file3.h
0060	74 6d 6c 20 48 54 54 50	2f 31 2e 31 0d 0a 41 63	tml HTTP /1.1..AC
0070	63 65 70 74 3a 20 74 65	78 74 2f 68 74 6d 6c 2c	cept: te xt/html,
0080	20 61 70 70 6c 69 63 61	74 69 6f 6e 2f 78 68 74	applica tion/xht

**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?**

Answer: My browser sent 1 HTTP GET request; Packet number 13 contains 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?**

Answer: Packet 20 does.

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

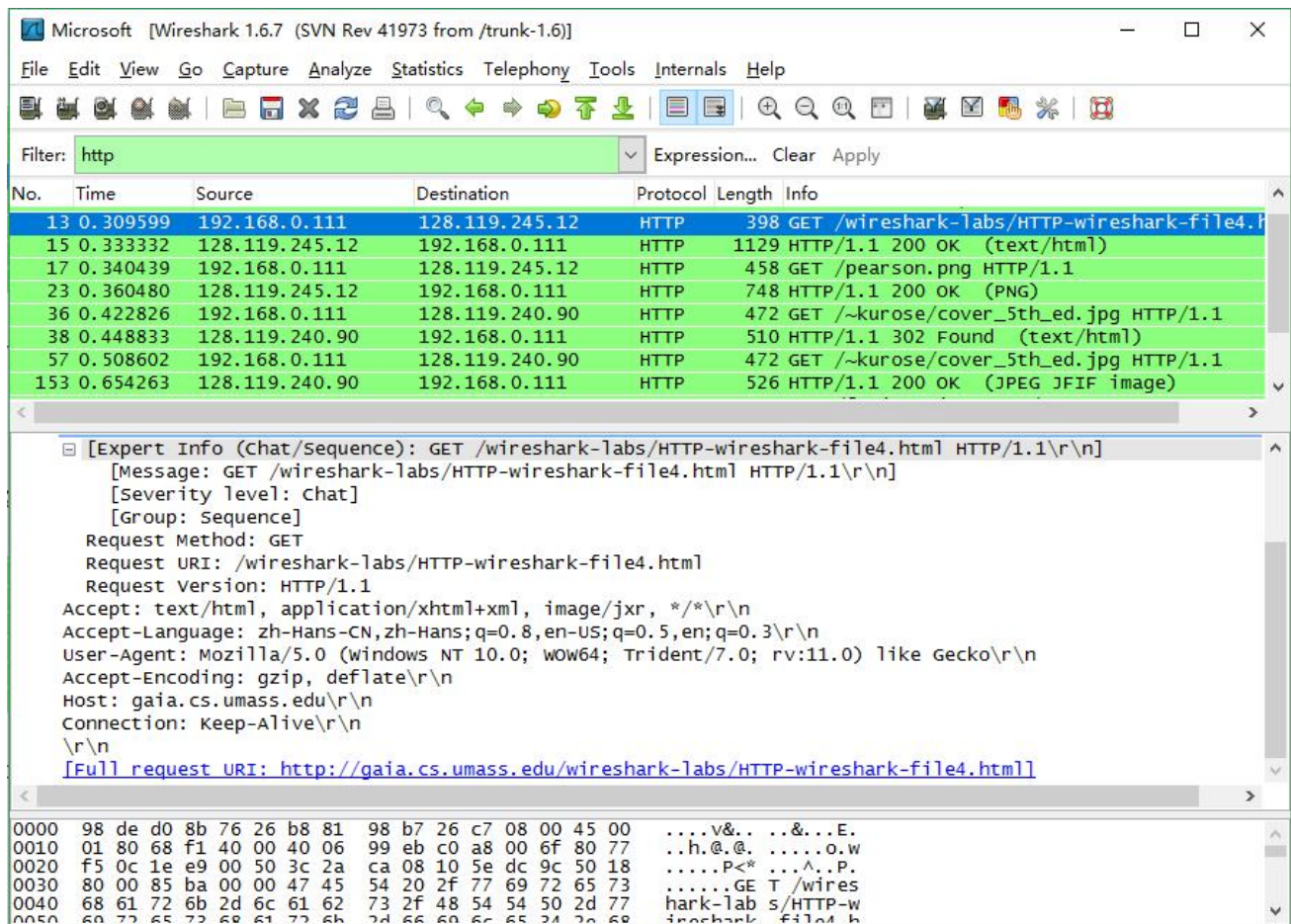
Answer: The Status code: 200, and the response phrase: OK

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

Answer:

[4 Reassembled TCP Segments (4863 bytes): #16(1460), #18(1460), #19(1460), #20(483)]  
 [Frame: 16, payload: 0-1459 (1460 bytes)]  
 [Frame: 18, payload: 1460-2919 (1460 bytes)]  
 [Frame: 19, payload: 2920-4379 (1460 bytes)]  
 [Frame: 20, payload: 4380-4862 (483 bytes)]  
 [Segment count: 4]  
 [Reassembled TCP length: 4863]

Therefore, four data-containing TCP segments were needed



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

Answer:

13	0.309599	192.168.0.111	128.119.245.12	HTTP	398	GET /wireshark-labs/HTTP-wireshark-file4.html
15	0.333332	128.119.245.12	192.168.0.111	HTTP	1129	HTTP/1.1 200 OK (text/html)
17	0.340439	192.168.0.111	128.119.245.12	HTTP	458	GET /pearson.png HTTP/1.1
23	0.360480	128.119.245.12	192.168.0.111	HTTP	748	HTTP/1.1 200 OK (PNG)
36	0.422826	192.168.0.111	128.119.240.90	HTTP	472	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
38	0.448833	128.119.240.90	192.168.0.111	HTTP	510	HTTP/1.1 302 Found (text/html)
57	0.508602	192.168.0.111	128.119.240.90	HTTP	472	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
153	0.654263	128.119.240.90	192.168.0.111	HTTP	526	HTTP/1.1 200 OK (JPEG JFIF image)
164	0.689431	192.168.0.111	128.119.245.12	HTTP	280	GET /favicon.ico HTTP/1.1
169	0.728292	128.119.245.12	192.168.0.111	HTTP	541	HTTP/1.1 404 Not Found (text/html)

My browser sent 5 HTTP GET request messages;

These requests were sent to 2 IP addresses: 128.119.245.12 and 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.**

Answer: My browser downloaded these 2 images serially, because they are received over more than one TCP connection, ports are: 7914, 7916, 7918.



Microsoft [Wireshark 1.6.7 (SVN Rev 41973 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
30	1.816510	192.168.0.111	128.119.245.12	HTTP	413	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
34	1.840318	128.119.245.12	192.168.0.111	HTTP	773	HTTP/1.1 401 Unauthorized (text/html)
123	18.133405	192.168.0.111	128.119.245.12	HTTP	472	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
126	18.153253	128.119.245.12	192.168.0.111	HTTP	585	HTTP/1.1 404 Not Found (text/html)

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

Accept: text/html, application/xhtml+xml, image/jxr, \*/\*\r\n

Accept-Language: zh-Hans-CN,zh-Hans;q=0.8,en-US;q=0.5,en;q=0.3\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n

Accept-Encoding: gzip, deflate\r\n

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

Connection: Keep-Alive\r\n

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n

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

0130 3f 2e 30 3b 20 72 7b 3a 31 31 2e 30 29 20 6c 69 /.;;rv: 11.0) li

0140 6b 65 20 47 65 63 6b 6f 0d 0a 41 63 63 65 70 74 ke Gecko ..Accept

0150 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c -Encodin g: gzip,

0160 20 64 65 66 6c 61 74 65 0d 0a 48 6f 73 74 3a 20 deflate ..Host:

0170 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed

0180 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b u..Conne ction: K

0190 65 65 70 2d 41 6c 69 76 65 0d 0a 41 75 74 68 6f eep-Aliv e..Autho

01a0 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 rization : Basic

01b0 64 32 6c 79 5a 58 4e 6f 59 58 4a 72 4c 58 4e 30 d2lyZXNo YXJrLXN0

01c0 64 57 52 6c 62 6e 52 7a 4f 6d 35 6c 64 48 64 76 dWRlbnRz Om5ldHdv

01d0 63 6d 73 3d 0d 0a 0d 0a cms=...

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

Answer: 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?

Answer: Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n