

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

Both 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

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

My IP address is 192.168.1.46 and the server's is 128.119.245.12

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

HTTP/1.1 200 OK (text/html)

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

Last-Modified: Wed, 12 Aug 2015 18:42:56 GMT

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

Content-Length: 126

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 all of the headers can be found in the raw data.

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 we can see the contents in 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. The information following is: Thu, 07 Jun 2007 16:29:01 GMT which is the date of the last modification of the file from the previous get request.

11. What is the HTTP status code and phrase returned from the server in response to

Austin Vern Songer

this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

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

12. How many HTTP GET request messages were sent by your browser?

There was 1 HTTP GET request message sent by my browser

13. How many data-containing TCP segments were needed to carry the single HTTP response?

There were 5 data containing TCP segments containing 309 ,1452 ,1452, 1452 and 144 bytes respectively for a total of 4500 bytes.

14. What is the status code and phrase associated with the response to the HTTP GET request?

200 OK

15. Are there any HTTP status lines in the transmitted data associated with a TCP induced "Continuation"?

No

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

As you can see from the above screenshot there were 3 HTTP GET requests sent to the following Internet addresses:

a. 128.119.245.12

b. 128.119.240.90

c. 165.193.123.218

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.

By checking the TCP ports we can see if our files were downloaded serially or in parallel. In this case the 2 images were transmitted over 2 TCP connections therefore they were downloaded serially.

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 , Phrase: Authorization Required

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

As seen in the screenshot the new field (highlighted) is Authorization.

Authorization: Basic d2lyZXNoYXJrLXNOdWRlbnRzOm5ldHdvems=\r\n

1.

No.	Time	Source	Destination	Protocol	Info
4	0.048291	192.168.1.46	128.119.245.12	HTTP	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n Host:

gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20150515

Firefox/2.0.0.4\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8

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

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

Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n Keep-Alive:

300\r\n

Connection: keep-alive\r\n Cookie:

MintUnique=1;

\_utmz=198765611.1176212581.8.2.utmccn=(referral)|utmcsr=cs.umass.edu|utmcct=/c  
sinfo/news.html|utmcmd=referral;

\_utma=198765611.821901841.1145892528.1176212581.1179945703.9;

\_utma=267820956.1666738513.1163587262.118

If-Modified-Since: Wed, 12 Aug 2015 18:42:56 GMT

\r\n If-None-Match: "d6c95-7e-224fab40"\r\n

\r\n

2.

No.	Time	Source	Destination	Protocol	Info
6	0.155044	128.119.245.12	192.168.1.46	HTTP	HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol HTTP/1.1 200

OK\r\n

Date: Wed, 12 Aug 2015 18:42:56 GMT\r\n Server:

Apache/2.0.52 (CentOS)\r\n

Last-Modified: Wed, 12 Aug 2015 18:42:56 GMT\r\n ETag: "d6c95-7e-  
2976b940"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 126

Keep-Alive: timeout=10, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=ISO-8859-1\r\n

\r\n

Line-based text data: text/html

<html>\n

Congratulations. You've downloaded the file \n http://gaia.cs.umass.edu/ethereal-labs/HTTP-  
ethereal-file1.html!\n

</html>\n

## Austin Vern Songer

No.	Time	Source	Destination	Protocol Info
	7 0.151515	128.119.245.12	192.168.1.46	HTTP

HTTP/1.1 200 OK (text/html)

Hypertext Transfer Protocol HTTP/1.1 200

OK\r\n

Request Version: HTTP/1.1 Response

Code: 200

Date: Wed, 12 Aug 2015 18:42:56 GMT \r\n Server:

Apache/2.0.52 (CentOS)\r\n

Last-Modified: Wed, 12 Aug 2015 18:42:56 GMT \r\n ETag: " d6c96-

173-69876d40 " \r\n

Accept-Ranges: bytes\r\n

Content-Length: 371

Keep-Alive: timeout=10, max=100\r\n Connection: Keep-

Alive\r\n

Content-Type: text/html; charset=ISO-8859-1\r\n

\r\n

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 IN-

MODIFIED-SINCE<br>\n

field in your browser's HTTP GET request to the server.\n

\n

</html>\n

No.	Time	Source	Destination	Protocol Info
	12 2.932093	192.168.1.46	128.119.245.12	HTTP GET

/wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n 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; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515

Firefox/2.0.0.4\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8

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

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

Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n Keep-Alive:

300\r\n

Connection: keep-alive\r\n Cookie:

\_utmz=198765611.1176212581.8.2.utmccn=(referral)|utmcsr=cs.umass.edu|utmctt=/c  
sinfo/news.html|utmcmd=referral;

\_utma=198765611.821901841.1145892528.1176212581.1179945703.9;

\_utmz=267820956.1180131637.4.1.utmccn=(organic)|utmcsr= **If-Modified-**

**Since: Wed, 12 Aug 2015 18:42:56 GMT \r\n** If-None-Match: " d6c96-173-  
69876d40 " \r\n

Cache-Control: max-age=0\r\n

\r\n

Austin Vern Songer

No.	Time	Source	Destination	Protocol Info
	13 3.030398	128.119.245.12	192.168.1.46	HTTP
HTTP/1.1 304 Not Modified				
Hypertext Transfer Protocol HTTP/1.1 304 Not Modified\r\n				
Request Version: HTTP/1.1 Response				
Code: 304				
Date: Wed, 12 Aug 2015 18:42:56 GMT \r\n Server:				
Apache/2.0.52 (CentOS)\r\n Connection: Keep-Alive\r\n				
Keep-Alive: timeout=10, max=98\r\n ETag: "d6c96-				
173-69876d40"\r\n				
\r\n				