

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

Ans:- Browser is running HTTP version 1.1

The image shows a Wireshark packet capture window titled 'http-ethereal-trace-1'. The packet list on the left shows four packets. Packet 10 is a GET request for '/ethereal-labs/lab2-1.html' from 192.168.1.102 to 128.119.245.12. Packet 12 is the corresponding 200 OK response. Packets 13 and 14 are subsequent requests for a favicon and a 'Not Found' response.

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

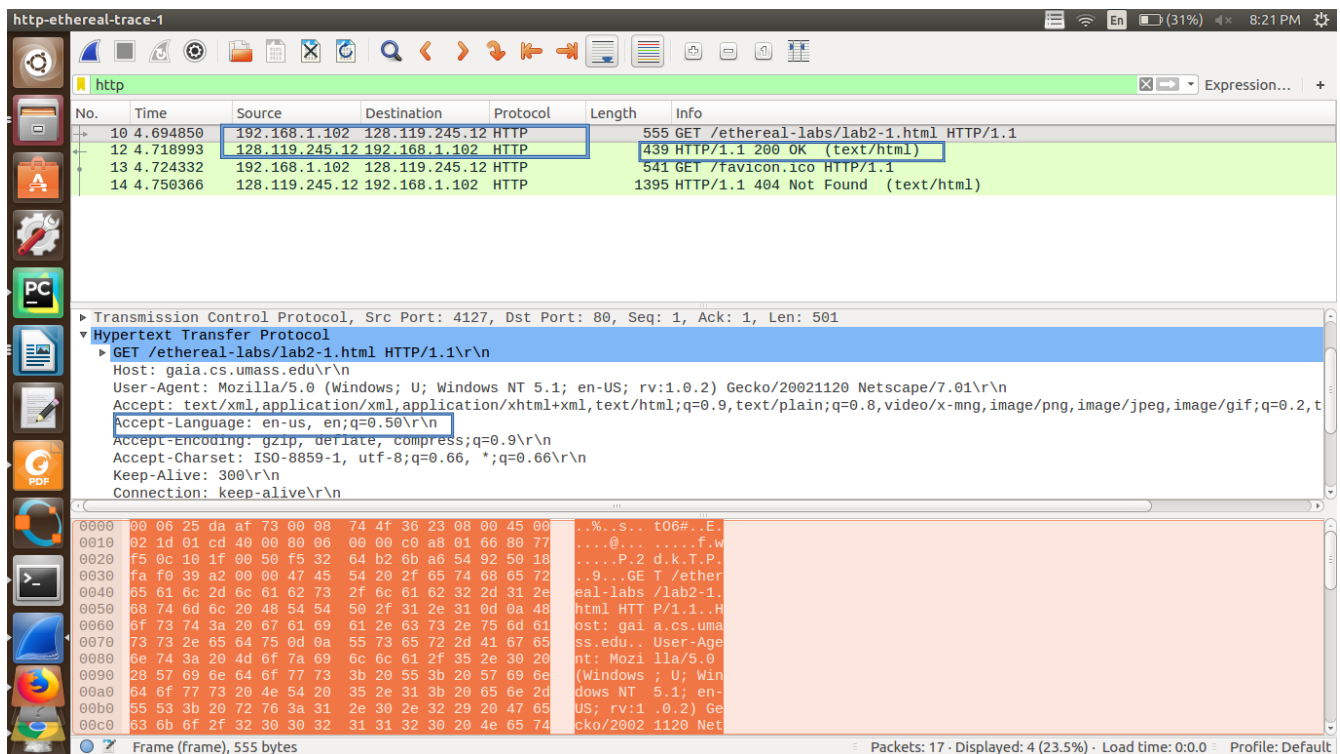
The packet details pane for packet 10 shows the following information:

- Frame 10: 555 bytes on wire (4440 bits), 555 bytes captured (4440 bits)
- Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
- Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 4127, Dst Port: 80, Seq: 1, Ack: 1, Len: 501
- Hypertext Transfer Protocol
 - GET /ethereal-labs/lab2-1.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:1.0.2) Gecko/20021120 Netscape/7.01\r\n
 - Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,t
 - Accept-Language: en-us,en;q=0.50\r\n
 - Accept-Encoding: gzip, deflate, compress;q=0.9\r\n

The packet bytes pane shows the raw data of the request, including the status bar at the bottom: 'Frame (frame), 555 bytes', 'Packets: 17 - Displayed: 4 (23.5%)', 'Load time: 0:0.0', 'Profile: Default'.

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

Ans:- Browser indicates to the server that accepts language : en-us. and it can also accept other english at the factor of 0.5



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

Ans:- Computer : 172.16.15.186

Server : 77.67.29.136

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

Ans:- 200

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

Ans:- Tue, 23rd Sep 2003 05:29:50 GMT.

http-ethereal-trace-1

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

Frame 12: 439 bytes on wire (3512 bits), 439 bytes captured (3512 bits)

Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102

Transmission Control Protocol, Src Port: 80, Dst Port: 4127, Seq: 1, Ack: 502, Len: 385

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 23 Sep 2003 05:29:50 GMT\r\n

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n

ETag: "1bfed-49-79d5bf00"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 73\r\n

0000 39 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 .t06#..%.s..E

0010 01 a9 b6 fa 40 00 37 06 53 c2 80 77 f5 0c c0 a8 ...@.7. S..w...

0020 01 66 00 50 10 1f 6b a6 54 92 f5 32 66 a7 50 18 .f.P..k. T..2f.P.

0030 19 20 7a 1c 00 00 48 54 54 50 2f 31 2e 31 20 32 .z...HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK..D ate: Tue

0050 2c 20 32 33 20 53 65 70 20 32 30 30 33 20 30 35 , 23 Sep 2003 05

0060 3a 32 39 3a 35 30 20 47 4d 54 0d 0a 53 65 72 76 :29:50 G MT..Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4

0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux

0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64)..Last- Modified

00a0 3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30 : Tue, 2 3 Sep 20

00b0 30 33 20 30 35 3a 32 39 3a 30 30 20 47 4d 54 0d 03 05:29 :00 GMT.

00c0 0a 45 54 61 67 3a 20 22 31 62 66 65 64 2d 34 39 .ETag: " 1bfed-49

Frame (frame), 439 bytes

Packets: 17 · Displayed: 4 (23.5%) · Load time: 0:0:0 · Profile: Default

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

Ans:- Content length : 73 Bytes and including header it is : 439 bytes.

http-ethereal-trace-1

No.	Time	Source	Destination	Protocol	Length	Info
10	4.694850	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-1.html HTTP/1.1
12	4.718993	128.119.245.12	192.168.1.102	HTTP	439	HTTP/1.1 200 OK (text/html)
13	4.724332	192.168.1.102	128.119.245.12	HTTP	541	GET /favicon.ico HTTP/1.1
14	4.750366	128.119.245.12	192.168.1.102	HTTP	1395	HTTP/1.1 404 Not Found (text/html)

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Last-Modified: Tue, 23 Sep 2003 05:29:00 GMT\r\n

ETag: "1bfed-49-79d5bf00"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 73\r\n

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

[HTTP response 1/2]

[Time since request: 0.024143000 seconds]

[Request in frame: 10]

0020 01 66 00 50 10 1f 6b a6 54 92 f5 32 66 a7 50 18 .f.P..k. T..2f.P.

0030 19 20 7a 1c 00 00 48 54 54 50 2f 31 2e 31 20 32 .z...HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 00 OK..D ate: Tue

0050 2c 20 32 33 20 53 65 70 20 32 30 30 33 20 30 35 , 23 Sep 2003 05

0060 3a 32 39 3a 35 30 20 47 4d 54 0d 0a 53 65 72 76 :29:50 G MT..Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4

0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux

0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64)..Last- Modified

00a0 3a 20 54 75 65 2c 20 32 33 20 53 65 70 20 32 30 : Tue, 2 3 Sep 20

00b0 30 33 20 30 35 3a 32 39 3a 30 30 20 47 4d 54 0d 03 05:29 :00 GMT.

00c0 0a 45 54 61 67 3a 20 22 31 62 66 65 64 2d 34 39 .ETag: " 1bfed-49

00d0 2d 37 39 64 35 62 66 30 30 22 0d 0a 41 63 63 65 -79d5bf0 0"..Acce

00e0 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 pt-Range s: bytes

Transmission Control Protocol (tcp), 20 bytes

Packets: 17 · Displayed: 4 (23.5%) · Load time: 0:0:0 · Profile: Default

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.

Ans:- NO

2. The HTTP CONDITIONAL GET/response interaction:

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?

Ans :- Not for the first GET request but for the Second GET request.

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

Ans: - Yes, the server explicitly returned the contents of the file. It can be seen in the field line based text data.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

The packet details pane shows the content of the second response (packet 10), which is an HTML document. The text data is as follows:

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

The packet bytes pane shows the raw data of the second response, which is a 739-byte HTML document. The status bar at the bottom indicates that the frame (frame) is 739 bytes, and the packets displayed are 4 (20.0%) of the total 20 packets.

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?

Ans:- The time and date when it was last modified.

In this case: **Tue, 13 Feb 2018 05:35:00 GMT.**

http-ethereal-trace-2

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357992	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20021120 Netscape/7.01\r\n
 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,t
 Accept-Language: en-us,en;q=0.50\r\n
 Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
 Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
 Keep-Alive: 300\r\n
 Connection: keep-alive\r\n
 If-Modified-Since: Tue, 23 Sep 2003 05:35:00 GMT\r\n
 If-None-Match: "1DfEr-173-874ae900"\r\n
 Cache-Control: max-age=0\r\n
 \r\n

0020 f5 0c 10 97 00 50 fa 88 03 26 81 6a b6 2e 50 18 ...P...&.j..P
 0030 f8 43 3a 13 00 00 47 45 54 20 2f 65 74 68 65 72 .C...GE T /ether
 0040 65 61 6c 2d 6c 61 62 73 2f 6c 61 62 32 2d 32 2e eal-labs /lab2-2.
 0050 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTT P/1.1..H
 0060 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gai a.cs.uma
 0070 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 ss.edu.. User-Age
 0080 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 nt: Mozi lla/5.0
 0090 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 6e (Windows ; U; Win
 00a0 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e 2d dows NT 5.1; en-
 00b0 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47 65 US; rv:1 .0.2) Ge
 00c0 63 6b 6f 2f 32 30 30 32 31 31 32 30 20 4e 65 74 cko/2002 1120 Net
 00d0 73 63 61 70 65 2f 37 2e 30 31 0d 0a 41 63 63 65 scape/7. 01..Acce
 00e0 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70 70 pt: text /xml,app

Transmission Control Protocol (tcp), 20 bytes

Packets: 20 - Displayed: 4 (20.0%) - Load time: 0:0.1 - Profile: Default

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.

Ans:- The status code returned is 304 – Not Modified. No, The server didn't send the contents of explicitly. The server returned the status code as 304 Not Modified and hence the file was taken from the cache instead of the server.

http-ethereal-trace-2

No.	Time	Source	Destination	Protocol	Length	Info
8	2.331268	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-2.html HTTP/1.1
10	2.357902	128.119.245.12	192.168.1.102	HTTP	739	HTTP/1.1 200 OK (text/html)
14	5.517390	192.168.1.102	128.119.245.12	HTTP	668	GET /ethereal-labs/lab2-2.html HTTP/1.1
15	5.540216	128.119.245.12	192.168.1.102	HTTP	243	HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Tue, 23 Sep 2003 05:35:53 GMT\r\n

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Connection: Keep-Alive\r\n

Keep-Alive: timeout=10, max=99\r\n

ETag: "1bfef-173-8f4ae900"\r\n

\r\n

[HTTP response 2/2]

[Time since request: 0.022826000 seconds]

[Prev request in frame: 8]

[Prev response in frame: 10]

0030 1f 2e 89 37 00 00 48 54 54 50 2f 31 2e 31 20 33 ...7..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 0a 44 61 74 65 3a 20 54 75 65 2c 20 32 33 20 53 .Date: Tue, 23 S

0060 65 70 20 32 30 30 33 20 30 35 3a 33 35 3a 35 33 ep 2003 05:35:53

0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap

0080 61 63 68 65 2f 32 2e 30 2e 34 30 20 28 52 65 64 ache/2.0 .40 (Red

0090 20 48 61 74 20 4c 69 6e 75 78 29 0d 0a 43 6f 6e Hat Lin ux)..Con

00a0 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nection: Keep-Al

00b0 69 76 65 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a ive..Kee p-Alive:

00c0 20 74 69 6d 65 6f 75 74 3d 31 30 2c 20 6d 61 78 timeout =10, max

00d0 3d 39 39 0d 0a 45 54 61 67 3a 20 22 31 62 66 65 =99. Eta g: "1bfe

00e0 66 2d 31 37 33 2d 38 66 34 61 65 39 30 30 22 0d f-173-8f 4ae900".

00f0 0a 0d 0a ...

HTTP Date (http.date), 37 bytes

Packets: 20 · Displayed: 4 (20.0%) · Load time: 0:0.0 · Profile: Default

3. Retrieving Long Documents

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?

Ans:- Only one Get request is sent by the browser (ignoring the favicon.ico request). Packet Number 8 contains the get message for the Bill or Rights.

http-ethereal-trace-3

No.	Time	Source	Destination	Protocol	Length	Info
8	1.623732	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-3.html HTTP/1.1
14	1.680920	128.119.245.12	192.168.1.102	HTTP	490	HTTP/1.1 200 OK (text/html)

Frame 14: 490 bytes on wire (3920 bits), 490 bytes captured (3920 bits)

Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell 4f:36:23 (00:08:74:4f:36:23)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102

Transmission Control Protocol, Src Port: 80, Dst Port: 4272, Seq: 4381, Ack: 502, Len: 436

[4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 23 Sep 2003 05:37:02 GMT\r\n

Server: Apache/2.0.40 (Red Hat Linux)\r\n

Last-Modified: Tue, 23 Sep 2003 05:37:01 GMT\r\n

ETag: "1bff2-1194-96813940"\r\n

Accept-Ranges: bytes\r\n

0000 00 08 74 4f 36 23 00 06 25 da af 73 08 00 45 00 ..t06#..%.s..E

0010 01 dc 21 71 40 00 37 06 e9 18 80 77 f5 0c c0 a8 ..!q@.7. ...w...

0020 01 66 00 50 10 b0 85 b2 bb 80 fb 98 e0 df 50 18 .f.P.....P.

0030 19 20 25 ab 00 00 3e 3c 68 33 3e 41 6d 65 6e 64 .%.%>< h3>Amend

0040 6d 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 ment IX< /h3></st

0050 72 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f rong>...<p></

0060 70 3e 3c 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 p><p>The enumera

0070 74 69 6f 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 tion in the Cons

0080 74 69 74 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 titution , of cer

0090 74 61 69 6e 20 72 69 67 68 74 73 2c 20 73 68 61 tain rig hts, sha

00a0 6c 6c 0a 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 ll.not b e constr

Frame (490 bytes) Reassembled TCP (4816 bytes)

Frame (frame), 490 bytes

Packets: 19 · Displayed: 2 (10.5%) · Load time: 0:0.0 · Profile: Default

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

Ans:- Packet Number 14 contains the status code and phrase associated with the response to the HTTP get Request.

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

Ans:- The status code is 200 and 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?

Ans:- 4 data containing TCP segments were required.

The image shows a Wireshark packet capture of an HTTP GET request and response. The top pane displays a list of packets. Packet 8 is the GET request, and packet 14 is the response. The bottom pane shows the details of packet 14, which is an HTTP 200 OK response. The response body contains the text of the Bill of Rights, which is displayed in a hex dump and ASCII view. The status code is 200 and the phrase is OK.

No.	Time	Source	Destination	Protocol	Length	Info
8	4.623732	192.168.1.102	128.119.245.12	HTTP	555	GET /ethereal-labs/lab2-3.html HTTP/1.1
14	4.680920	128.119.245.12	192.168.1.102	HTTP	490	HTTP/1.1 200 OK (text/html)

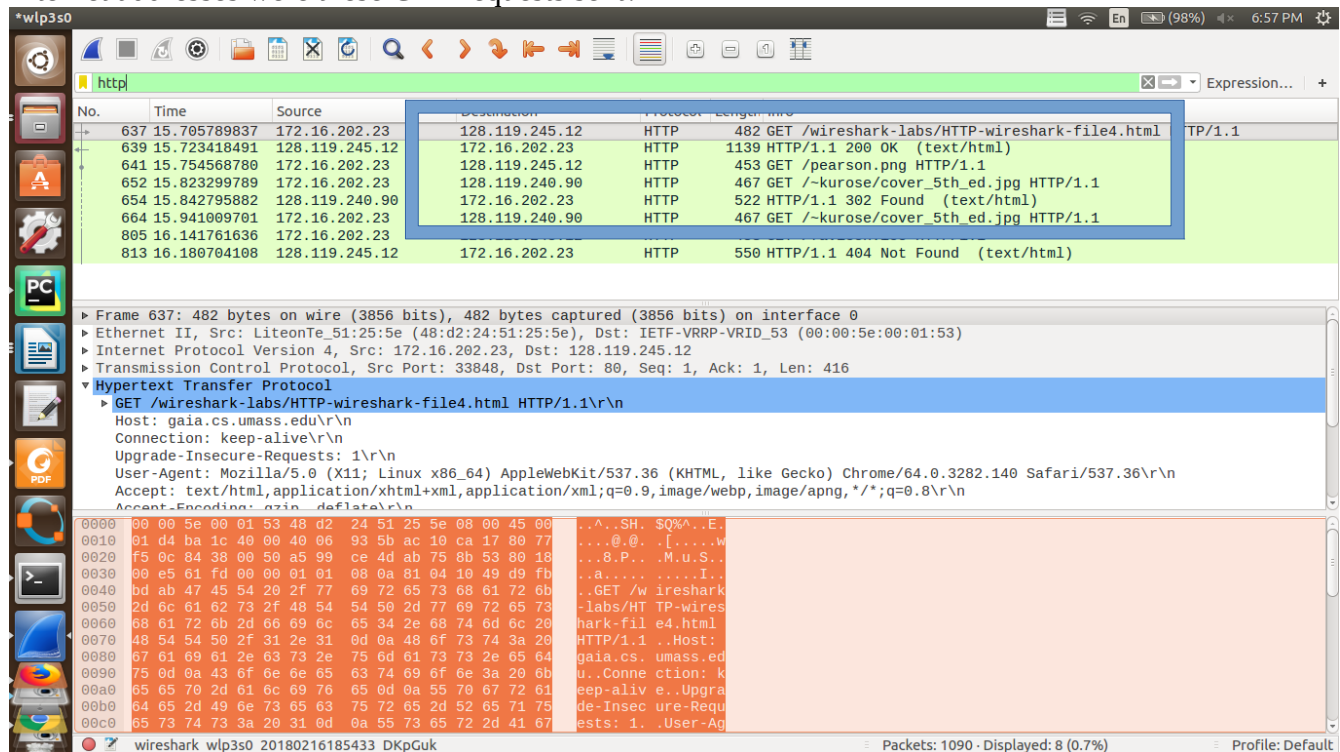
Details of Packet 14 (HTTP 200 OK):

- Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.102
- Transmission Control Protocol, Src Port: 80, Dst Port: 4272, Seq: 4381, Ack: 502, Len: 436
- [4 Reassembled TCP Segments (4816 bytes): #10(1460), #11(1460), #13(1460), #14(436)]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - Date: Tue, 23 Sep 2003 05:37:02 GMT\r\n
 - Server: Apache/2.0.40 (Red Hat Linux)\r\n
 - Last-Modified: Tue, 23 Sep 2003 05:37:01 GMT\r\n
 - ETag: "1bff2-1194-96813940"\r\n
 - Accept-Ranges: bytes\r\n
 - Content-Length: 4500\r\n

Frame (490 bytes) Reassembled TCP (4816 bytes)

4. HTML Documents with Embedded Objects

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



No.	Time	Source	Destination	Protocol	Length	Info
637	15.705789837	172.16.202.23	128.119.245.12	HTTP	482	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
639	15.723418491	128.119.245.12	172.16.202.23	HTTP	1139	HTTP/1.1 200 OK (text/html)
641	15.754568780	172.16.202.23	128.119.245.12	HTTP	453	GET /pearson.png HTTP/1.1
652	15.823299789	172.16.202.23	128.119.240.90	HTTP	467	GET /-kurose/cover_5th_ed.jpg HTTP/1.1
654	15.842795882	128.119.240.90	172.16.202.23	HTTP	522	HTTP/1.1 302 Found (text/html)
664	15.941009701	172.16.202.23	128.119.240.90	HTTP	467	GET /-kurose/cover_5th_ed.jpg HTTP/1.1
805	16.141761636	172.16.202.23	172.16.202.23	HTTP	550	HTTP/1.1 404 Not Found (text/html)
813	16.180704108	128.119.245.12	172.16.202.23	HTTP	550	HTTP/1.1 404 Not Found (text/html)

Frame 637: 482 bytes on wire (3856 bits), 482 bytes captured (3856 bits) on interface 0
Ethernet II, Src: LiteonTe_51:25:5e (48:d2:24:51:25:5e), Dst: IETF-VRRP-VRID_53 (00:00:5e:00:01:53)
Internet Protocol Version 4, Src: 172.16.202.23, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 33848, Dst Port: 80, Seq: 1, Ack: 1, Len: 416
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
Host: gaia.cs.umass.edu
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 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

Ans:- Number of HTTP Get request : 4

Servers IP address to which get request was made : 128.119.245.12
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.

Ans:- The browser downloaded the file serially because as we see that browser first make a GET request for pearson.png and then after receiving the response for the given request

It later makes a HTTP GET Request for the second image .

Request Made for first image (Time): 128.119.245.12

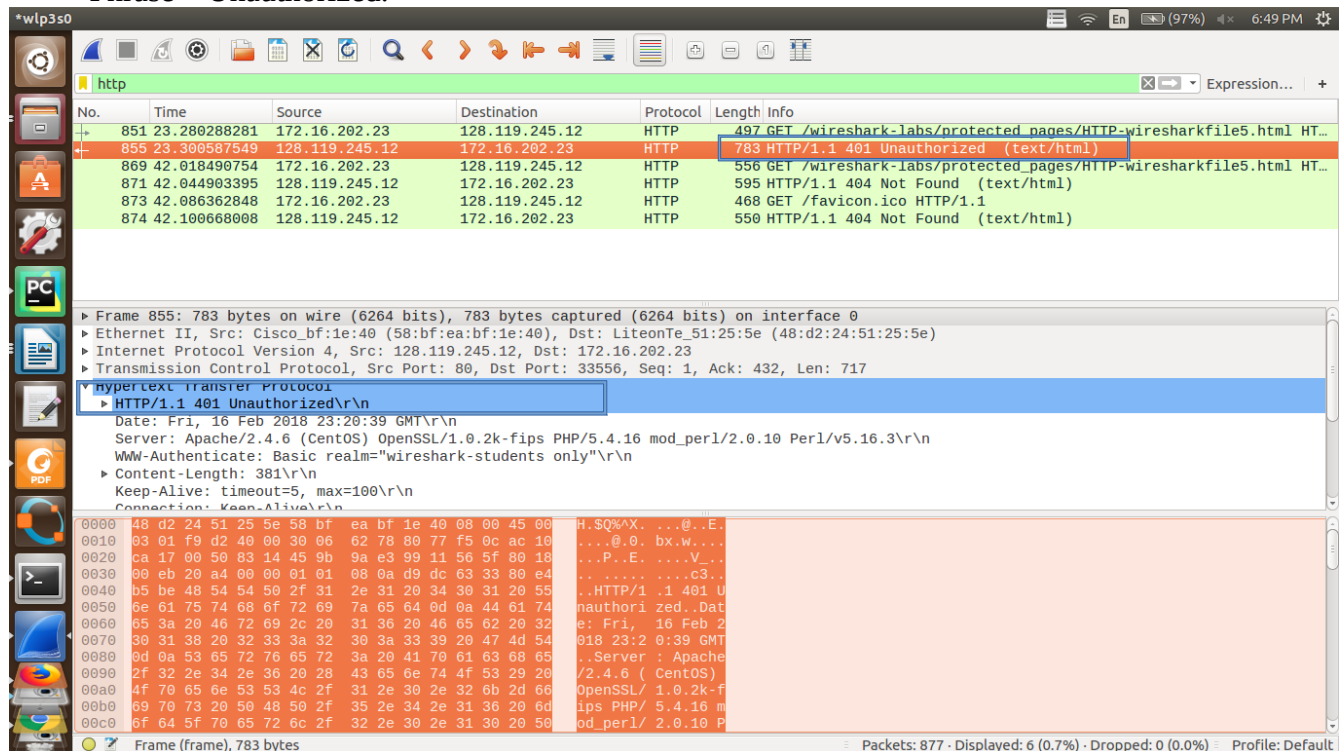
Request Made for second image(Time): 128.119.240.90

5. HTTP Authentication

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

Ans:- Status Code – 401

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?

Ans:- Additional field in second get message is : Authorization.

