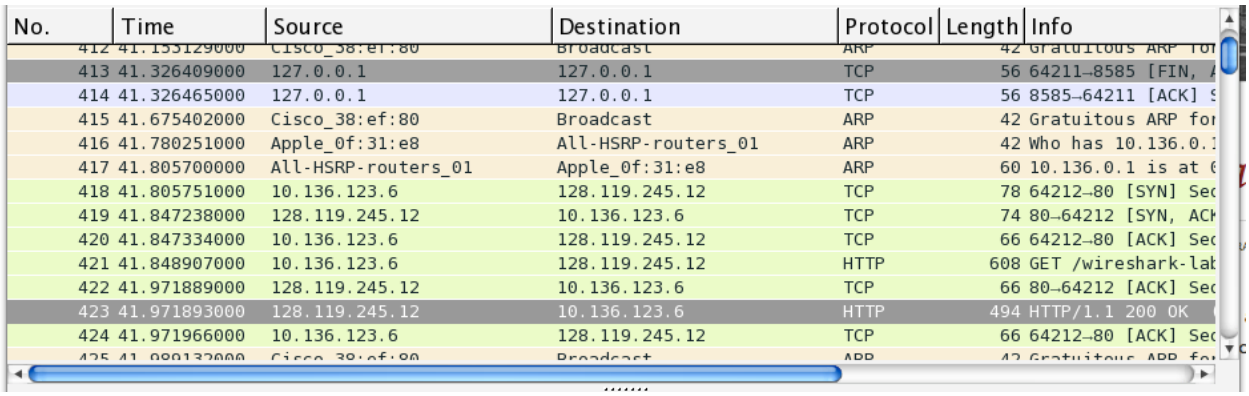
Wireshark Lab: Getting Started v6.0

LAB SOLUTION #2

90009559

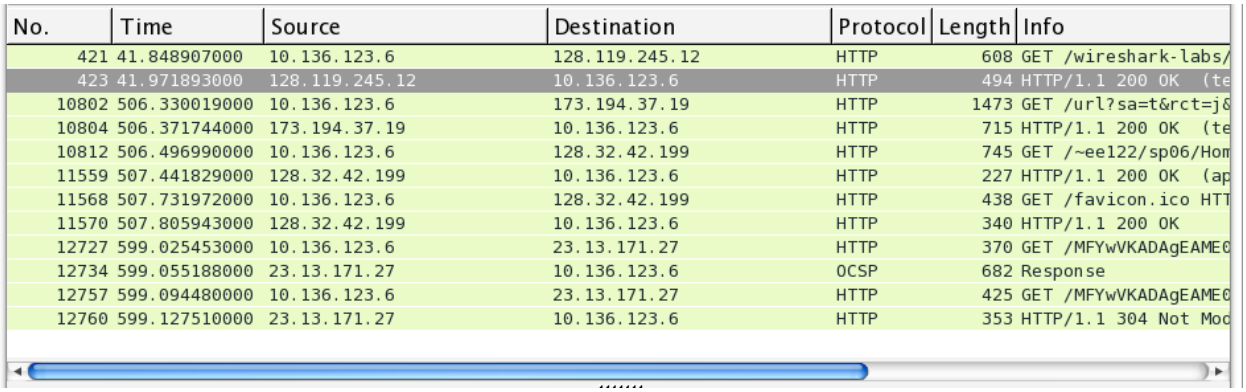
MANASI SHARMA

1. Screenshot of captured packets.



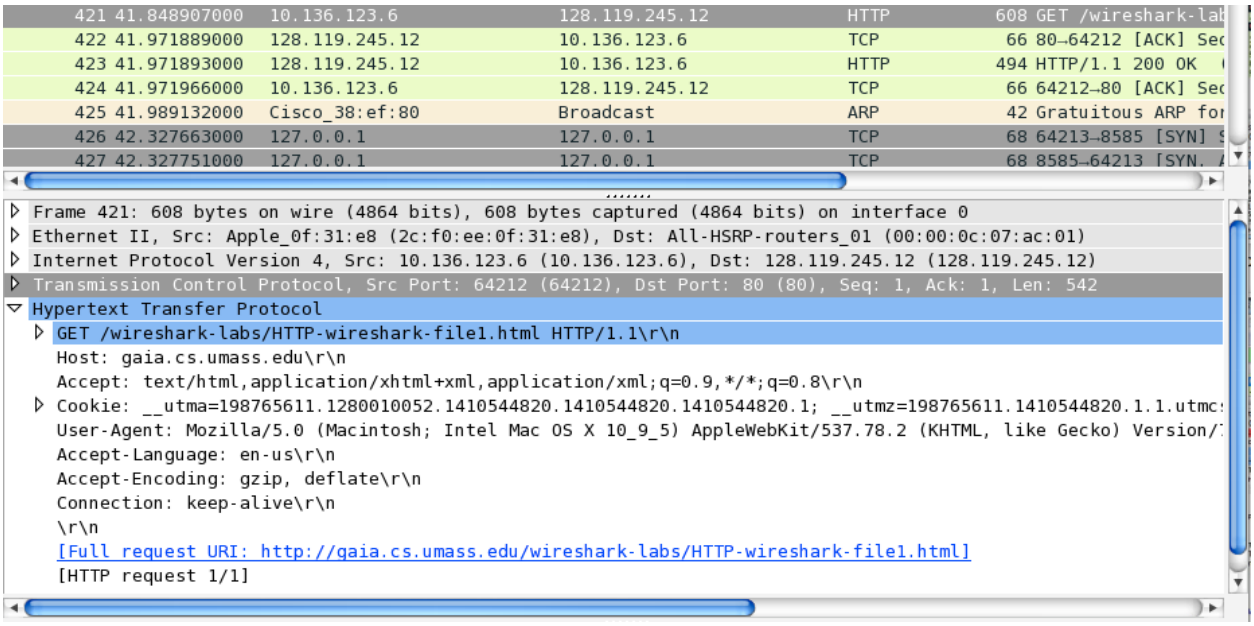
No.	Time	Source	Destination	Protocol	Length	Info
413	41.326409000	127.0.0.1	127.0.0.1	TCP	56	64211→8585 [FIN, A
414	41.326465000	127.0.0.1	127.0.0.1	TCP	56	8585→64211 [ACK] S
415	41.675402000	Cisco_38:ef:80	Broadcast	ARP	42	Gratuitous ARP for
416	41.780251000	Apple_0f:31:e8	All-HSRP-routers_01	ARP	42	Who has 10.136.0.1
417	41.805700000	All-HSRP-routers_01	Apple_0f:31:e8	ARP	60	10.136.0.1 is at 0
418	41.805751000	10.136.123.6	128.119.245.12	TCP	78	64212→80 [SYN] Seq
419	41.847238000	128.119.245.12	10.136.123.6	TCP	74	80→64212 [SYN, ACK
420	41.847334000	10.136.123.6	128.119.245.12	TCP	66	64212→80 [ACK] Seq
421	41.848907000	10.136.123.6	128.119.245.12	HTTP	608	GET /wireshark-lab
422	41.971889000	128.119.245.12	10.136.123.6	TCP	66	80→64212 [ACK] Seq
423	41.971893000	128.119.245.12	10.136.123.6	HTTP	494	HTTP/1.1 200 OK
424	41.971966000	10.136.123.6	128.119.245.12	TCP	66	64212→80 [ACK] Seq

Filtering “http”

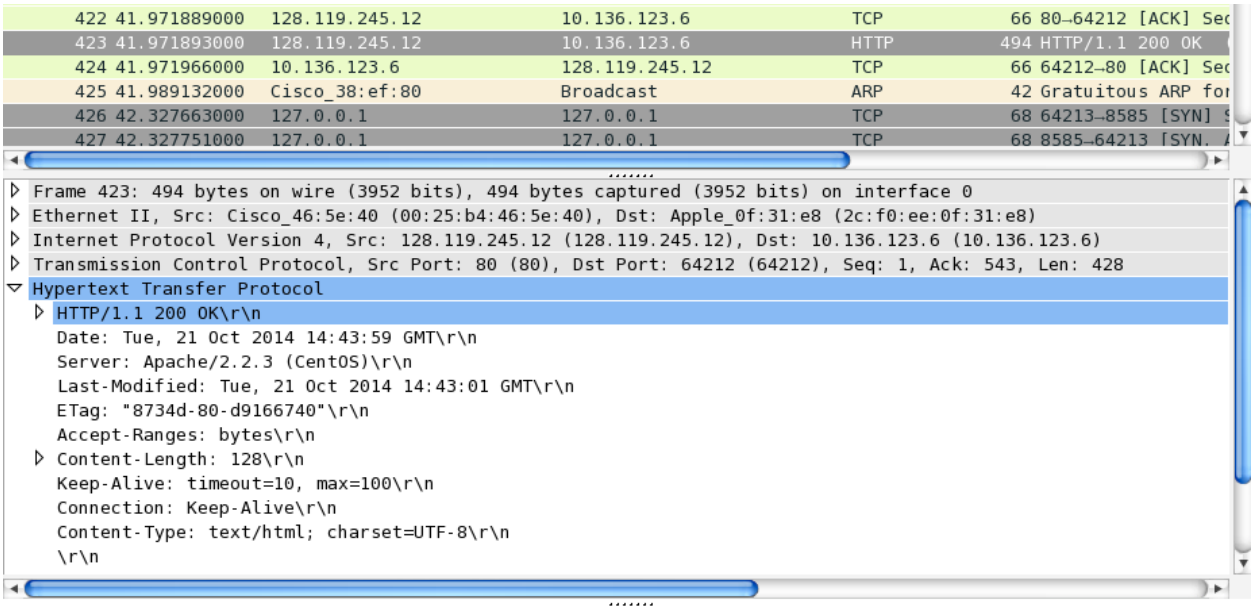


No.	Time	Source	Destination	Protocol	Length	Info
421	41.848907000	10.136.123.6	128.119.245.12	HTTP	608	GET /wireshark-labs/
423	41.971893000	128.119.245.12	10.136.123.6	HTTP	494	HTTP/1.1 200 OK (te
10802	506.330019000	10.136.123.6	173.194.37.19	HTTP	1473	GET /url?sa=t&rct=j&
10804	506.371744000	173.194.37.19	10.136.123.6	HTTP	715	HTTP/1.1 200 OK (te
10812	506.496990000	10.136.123.6	128.32.42.199	HTTP	745	GET /~ee122/sp06/Hom
11559	507.441829000	128.32.42.199	10.136.123.6	HTTP	227	HTTP/1.1 200 OK (ap
11568	507.731972000	10.136.123.6	128.32.42.199	HTTP	438	GET /favicon.ico HTT
11570	507.805943000	128.32.42.199	10.136.123.6	HTTP	340	HTTP/1.1 200 OK
12727	599.025453000	10.136.123.6	23.13.171.27	HTTP	370	GET /MFYwVKADAgEAME0
12734	599.055188000	23.13.171.27	10.136.123.6	OCSP	682	Response
12757	599.094480000	10.136.123.6	23.13.171.27	HTTP	425	GET /MFYwVKADAgEAME0
12760	599.127510000	23.13.171.27	10.136.123.6	HTTP	353	HTTP/1.1 304 Not Mod

HTTP information for the GET



HTTP information for the response:



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

Ans. Both the GET and response mention the request version : HTTP/1.1. Hence, my browser and the HTTP server is running version 1.1

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

Ans. The Accept-Language inside HTTP information for the GET indicates that it accepts en-s, en.

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

```
Source: 10.136.123.6 (10.136.123.6)
Destination: 128.119.245.12 (128.119.245.12)
```

Ans. My IP address is 10.136.123.6. The IP address of gaia.cs.umass.edu is 128.119.245.12.

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

Ans. The status code returned from the server is 200 ok.

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

Ans. Last-Modified: Tue, 21 October 2014 14:43:01 GMT

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

Ans. 128 bytes as Content-Length is 128\r\n.

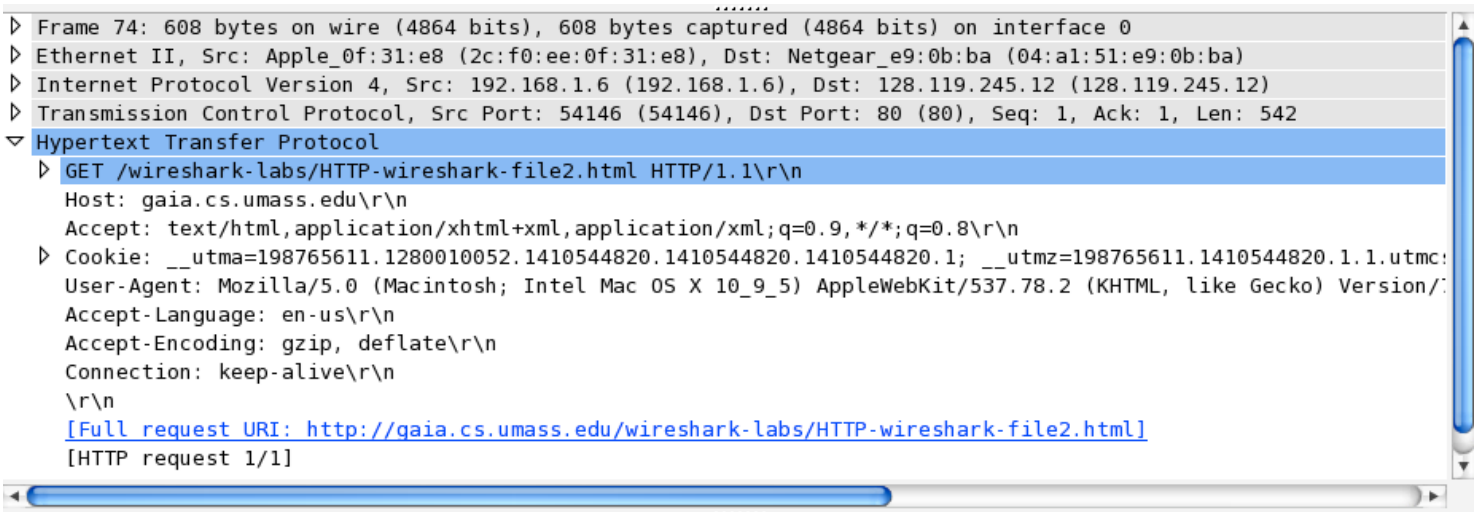
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Ans. No, there are no such headers.

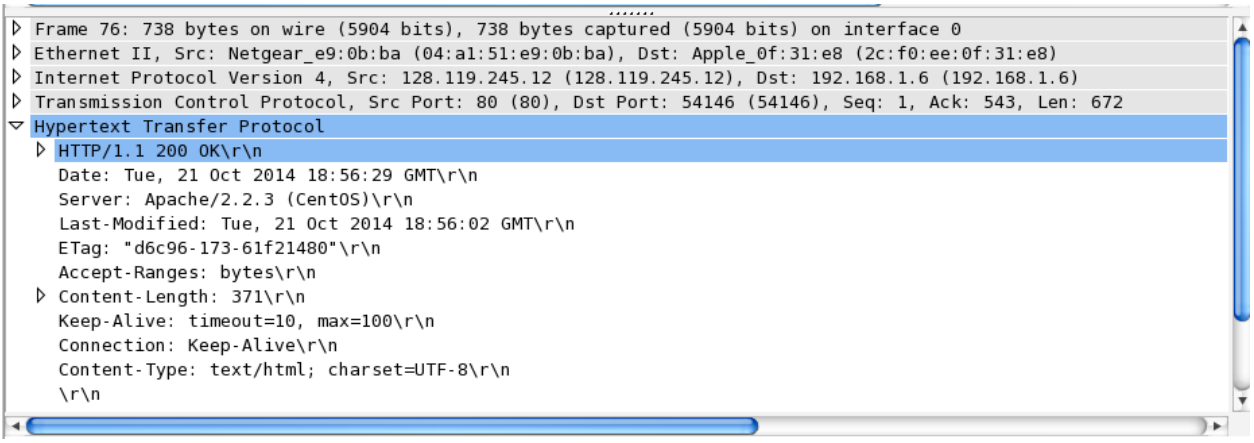
2. The HTTP CONDITIONAL GET/response interaction

No.	Time	Source	Destination	Protocol	Length	Info
74	9.267341000	192.168.1.6	128.119.245.12	HTTP	608	GET /wireshark-labs/
76	9.342274000	128.119.245.12	192.168.1.6	HTTP	738	HTTP/1.1 200 OK (te
191	25.397526000	192.168.1.6	128.119.245.12	HTTP	695	GET /wireshark-labs/
194	25.468659000	128.119.245.12	192.168.1.6	HTTP	248	HTTP/1.1 304 Not Mod

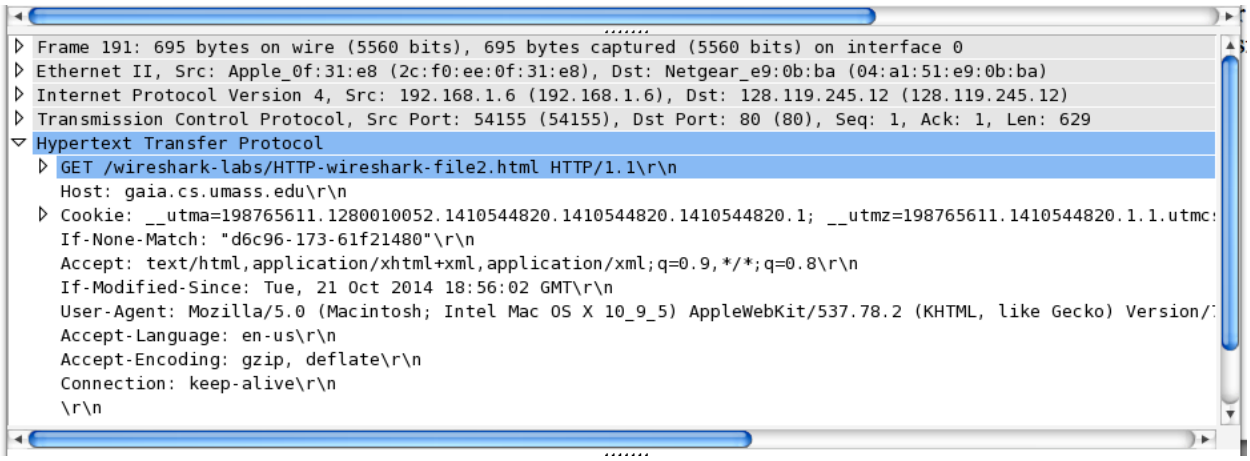
HTTP information for the first GET



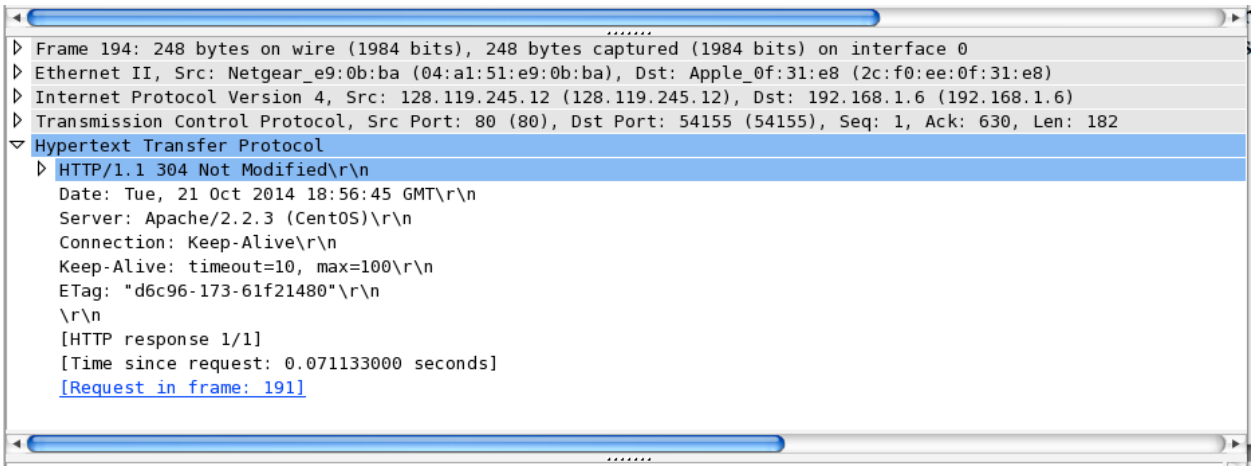
HTTP information for the first Response



HTTP information for the first GET



HTTP information for the first Response



Answer the following questions:

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. NO

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

Ans. Yes because the contents are visible 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?

Ans. Yes.

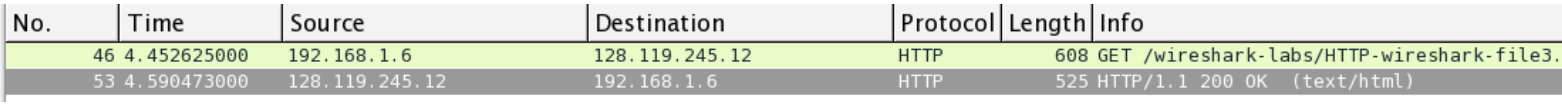
The information followed is: Tue, 21 Oct 2014 18:56:02 GMT\r\n.

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

Ans. The status code and phrase returned from the server is HTTP/1.1 304 Not Modified. The file contents are not returned from the server and instead loaded from its cache by the browser.

3. Retrieving Long Documents



No.	Time	Source	Destination	Protocol	Length	Info
46	4.452625000	192.168.1.6	128.119.245.12	HTTP	608	GET /wireshark-labs/HTTP-wireshark-file3.
53	4.590473000	128.119.245.12	192.168.1.6	HTTP	525	HTTP/1.1 200 OK (text/html)

Answer the following questions:

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. My browser sent 1 HTTP GET request to the server. Packet that contained the GET message was packet number 46.

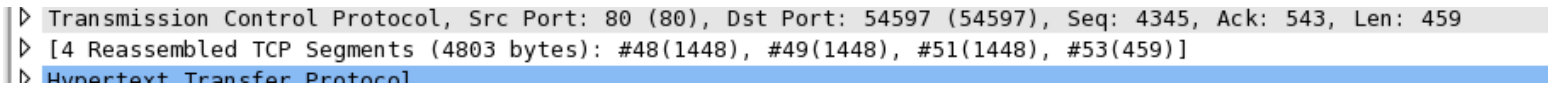
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Ans. The packet that contains the status code and phrase which the server sent in response to the GET message was packet number 53.

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

Ans. The code and phrase in the response was 200 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. The data was sent in 4 TCP segments to the browser, then reassembled.

4. HTML Documents with Embedded Objects

Answer the following questions:
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
33	3.677917000	192.168.1.6	128.119.245.12	HTTP	608	GET /wireshark-labs/
35	3.747160000	128.119.245.12	192.168.1.6	HTTP	1108	HTTP/1.1 200 OK (te
47	3.860333000	192.168.1.6	128.119.240.90	HTTP	609	GET /~kurose/cover_5
48	3.861259000	192.168.1.6	165.193.140.14	HTTP	661	GET /assets/hip/us/h
50	3.925553000	128.119.240.90	192.168.1.6	HTTP	522	HTTP/1.1 302 Found
60	3.936620000	165.193.140.14	192.168.1.6	HTTP	1022	HTTP/1.1 200 OK (GI

Ans. 3 http GET message requests, one each to each for each of the following are sent by my browser:

128.119.245.12 = Initial Page address;

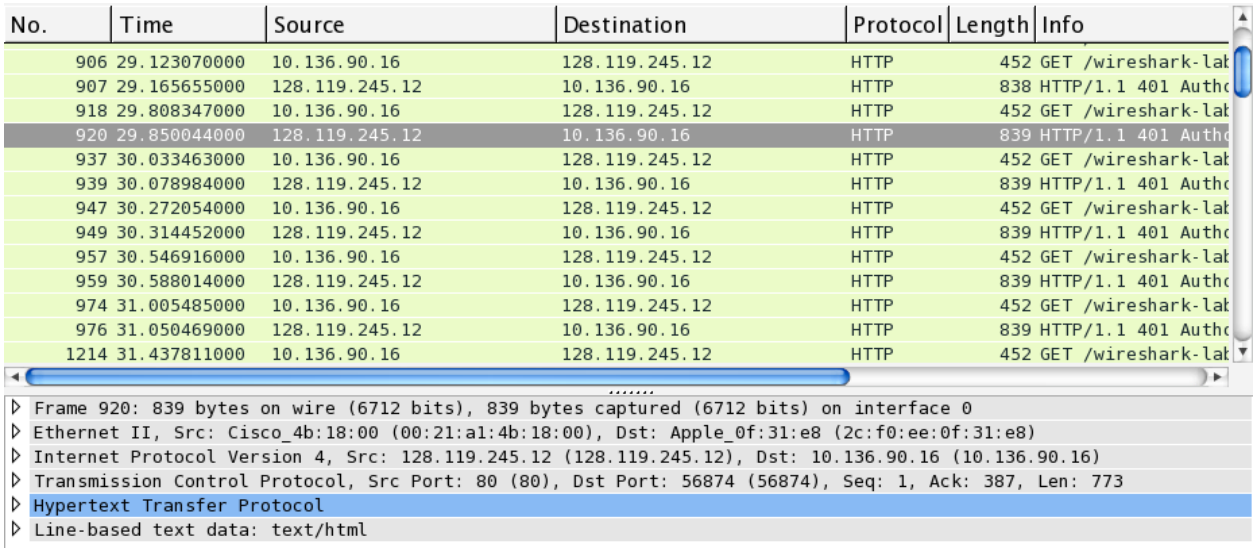
165.193.140.14 = Pearson Logo;

128.119.240.90 = Pearson book, 5th Edition;

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. By checking the TCP ports it can be seen if our files were downloaded serially or in parallel. Here, the 2 images were transmitted over 2 TCP connections. Hence, they were downloaded serially.

5. HTTP Authentication



No.	Time	Source	Destination	Protocol	Length	Info
906	29.123070000	10.136.90.16	128.119.245.12	HTTP	452	GET /wireshark-lab
907	29.165655000	128.119.245.12	10.136.90.16	HTTP	838	HTTP/1.1 401 Authc
918	29.808347000	10.136.90.16	128.119.245.12	HTTP	452	GET /wireshark-lab
920	29.850044000	128.119.245.12	10.136.90.16	HTTP	839	HTTP/1.1 401 Authc
937	30.033463000	10.136.90.16	128.119.245.12	HTTP	452	GET /wireshark-lab
939	30.078984000	128.119.245.12	10.136.90.16	HTTP	839	HTTP/1.1 401 Authc
947	30.272054000	10.136.90.16	128.119.245.12	HTTP	452	GET /wireshark-lab
949	30.314452000	128.119.245.12	10.136.90.16	HTTP	839	HTTP/1.1 401 Authc
957	30.546916000	10.136.90.16	128.119.245.12	HTTP	452	GET /wireshark-lab
959	30.588014000	128.119.245.12	10.136.90.16	HTTP	839	HTTP/1.1 401 Authc
974	31.005485000	10.136.90.16	128.119.245.12	HTTP	452	GET /wireshark-lab
976	31.050469000	128.119.245.12	10.136.90.16	HTTP	839	HTTP/1.1 401 Authc
1214	31.437811000	10.136.90.16	128.119.245.12	HTTP	452	GET /wireshark-lab

```
▷ Frame 920: 839 bytes on wire (6712 bits), 839 bytes captured (6712 bits) on interface 0
▷ Ethernet II, Src: Cisco_4b:18:00 (00:21:a1:4b:18:00), Dst: Apple_0f:31:e8 (2c:f0:ee:0f:31:e8)
▷ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 10.136.90.16 (10.136.90.16)
▷ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 56874 (56874), Seq: 1, Ack: 387, Len: 773
▷ Hypertext Transfer Protocol
▷ Line-based text data: text/html
```

Answer the following questions:

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 is 401 and Phrase is 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?

Answer: The new field is the Authorization field.