Wireshark Lab: Getting Started v6.0 LAB SOLUTION #2

90009559 MANASI SHARMA

1. Screenshot of captured packets.

No.	Time	Source	Destination	Protocol Len	- I
	412 41.153129000	CISCO_38:e1:80	Broadcast	ARP	42 Gratuitous ARP TOT
	413 41.326409000	127.0.0.1	127.0.0.1	TCP	56 64211→8585 [FIN, #
	414 41.326465000	127.0.0.1	127.0.0.1	TCP	56 8585→64211 [ACK] 5
	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 (
	418 41.805751000	10.136.123.6	128.119.245.12	TCP	78 64212→80 [SYN] Sec
	419 41.847238000	128.119.245.12	10.136.123.6	TCP	74 80→64212 [SYN, ACF
	420 41.847334000	10.136.123.6	128.119.245.12	TCP	66 64212→80 [ACK] Sec
	421 41.848907000	10.136.123.6	128.119.245.12	HTTP	608 GET /wireshark-lak
	422 41.971889000	128.119.245.12	10.136.123.6	TCP	66 80→64212 [ACK] Sec
	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] Sec
	425 41 000132MMM	Circo 30.of.on	Proodcast	ADD	42 Gratuitous ADD for
4				•)+

Filtering "http"

No.	Time	Source	Destination	Protocol	Length Info
42	21 41.848907000	10.136.123.6	128.119.245.12	HTTP	608 GET /wireshark-labs/
42	23 41.971893000	128.119.245.12	10.136.123.6	HTTP	494 HTTP/1.1 200 OK (te
1086	02 506.330019000	10.136.123.6	173.194.37.19	HTTP	1473 GET /url?sa=t&rct=j&
1086	04 506.371744000	173.194.37.19	10.136.123.6	HTTP	715 HTTP/1.1 200 OK (te
1081	12 506.496990000	10.136.123.6	128.32.42.199	HTTP	745 GET /~ee122/sp06/Hom
1155	59 507.441829000	128.32.42.199	10.136.123.6	HTTP	227 HTTP/1.1 200 OK (ap
1156	58 507.731972000	10.136.123.6	128.32.42.199	HTTP	438 GET /favicon.ico HTT
1157	70 507.805943000	128.32.42.199	10.136.123.6	HTTP	340 HTTP/1.1 200 OK
1272	27 599.025453000	10.136.123.6	23.13.171.27	HTTP	370 GET /MFYwVKADAgEAME0
1273	34 599.055188000	23.13.171.27	10.136.123.6	0CSP	682 Response
1275	57 599.094480000	10.136.123.6	23.13.171.27	HTTP	425 GET /MFYwVKADAgEAME@
1276	50 599.127510000	23.13.171.27	10.136.123.6	HTTP	353 HTTP/1.1 304 Not Mod
4)+

HTTP information for the GET

```
421 41.848907000 10.136.123.6
                                                                                                                                  128.119.245.12
                                                                                                                                                                                                                                           66 80→64212 [ACK] Sec
                422 41.971889000
                                                             128.119.245.12
                                                                                                                                  10.136.123.6
                423 41.971893000 128.119.245.12
                                                                                                                                  10.136.123.6
                                                                                                                                                                                                      HTTP
                                                                                                                                                                                                                                         494 HTTP/1.1 200 0K
                424 41.971966000 10.136.123.6
                                                                                                                                  128.119.245.12
                                                                                                                                                                                                                                           66 64212-80 [ACK] Sec
                                                                                                                                                                                                      TCP
                425 41.989132000 Cisco_38:ef:80
                                                                                                                                                                                                      ΔRP
                                                                                                                                                                                                                                            42 Gratuitous ARP for
                                                                                                                                  Broadcast
                426 42.327663000 127.0.0.1
                                                                                                                                  127.0.0.1
                                                                                                                                                                                                       TCP
                                                                                                                                                                                                                                           68 64213-8585 [SYN] S
                427 42.327751000 127.0.0.1
                                                                                                                                  127.0.0.1
                                                                                                                                                                                                                                           68 8585→64213 [SYN. A
                                                                                                                                                                                                       TCP
▶ Frame 421: 608 bytes on wire (4864 bits), 608 bytes captured (4864 bits) on interface 0

    Ethernet II, Src: Apple_0f:31:e8 (2c:f0:ee:0f:31:e8), Dst: All-HSRP-routers_01 (00:00:0c:07:ac:01)

▶ Internet Protocol Version 4, Src: 10.136.123.6 (10.136.123.6), Dst: 128.119.245.12 (128.119.245.12)
▶ Transmission Control Protoco

▼ Hypertext Transfer Protocol

      ▶ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
           Host: gaia.cs.umass.edu\r\n
            Accept: \ text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8 \\ \ r\ n=0.8 \\ 
      ▷ Cookie: __utma=198765611.1280010052.1410544820.1410544820.1; __utmz=198765611.1410544820.1.1.utmc:
            User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.78.2 (KHTML, like Gecko) Version/
            Accept-Language: en-us\r\n
            Accept-Encoding: gzip, deflate\r\n
            Connection: keep-alive\r\n
            [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
            [HTTP request 1/1]
```

HTTP information for the response:

422 41.971889000	128.119.245.12	10.136.123.6	TCP	66 80→64212 [ACK] Sec
423 41.971893000	128.119.245.12	10.136.123.6	HTTP	494 HTTP/1.1 200	0K
424 41.971966000	10.136.123.6	128.119.245.12	TCP	66 64212→80 [ACK] Sec
425 41.989132000	Cisco_38:ef:80	Broadcast	ARP	42 Gratuitous AR	P for
426 42.327663000	127.0.0.1	127.0.0.1	TCP	68 64213→8585 [S	YN] S
427 42.327751000	127.0.0.1	127.0.0.1	TCP	68 8585→64213 「S	YN. ∤
4)-
▶ Frame 423: 494 bytes	on wire (3952 bits)	, 494 bytes captured (3952 bit	s) on interface	0	4
▶ Ethernet II, Src: Cis	co_46:5e:40 (00:25:	b4:46:5e:40), Dst: Apple_0f:31	:e8 (2c:f0:ee:0	f:31:e8)	ſ
▶ Internet Protocol Ver	sion 4, Src: 128.11	9.245.12 (128.119.245.12), Dst	: 10.136.123.6	(10.136.123.6)	
▶ Transmission Control I	Protocol, Src Port:	80 (80), Dst Port: 64212 (642	12), Seq: 1, Ac	k: 543, Len: 428	
→ Hypertext Transfer Property	otocol				
▶ HTTP/1.1 200 0K\r\n					
Date: Tue, 21 Oct 2	014 14:43:59 GMT\r\	,n			
Server: Apache/2.2.	3 (CentOS)\r\n				
Last-Modified: Tue,	21 Oct 2014 14:43:	01 GMT\r\n			
ETag: "8734d-80-d91	66740"\r\n				
Accept-Ranges: byte	s\r\n				
Content-Length: 128	\r\n				
Keep-Alive: timeout	=10, max=100\r\n				•
Connection: Keep-Al	ive\r\n				- 1
Content-Type: text/	html; charset=UTF-8	3\r\n			- 1
\r\n					7
4) b

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

```
Frame 74: 608 bytes on wire (4864 bits), 608 bytes captured (4864 bits) on interface 0

Ethernet II, Src: Apple_0f:31:e8 (2c:f0:ee:0f:31:e8), Dst: Netgear_e9:0b:ba (04:a1:51:e9:0b:ba)

Internet Protocol Version 4, Src: 192.168.1.6 (192.168.1.6), Dst: 128.119.245.12 (128.119.245.12)

Transmission Control Protocol, Src Port: 54146 (54146), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 542

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

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

Accept: text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8\r\n

Cookie: _utma=198765611.1280010052.1410544820.1410544820.1; _utmz=198765611.1410544820.1.1.utmc:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.78.2 (KHTML, like Gecko) Version/:
Accept-Language: en-us\r\n

Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n
\r\n

[Full request URI: http://qaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 1/1]

**

Internet II, Src: Apple_0f:31:e8, Dst: Netgear_e9:0b:ba (04:a1:51:e9:0b:ba)

Description: Netge: 00:ba (192.10:ba)

Description: Netge: 00:ba (192.
```

HTTP information for the first Response

```
▶ Frame 76: 738 bytes on wire (5904 bits), 738 bytes captured (5904 bits) on interface 0

▷ Ethernet II, Src: Netgear e9:0b:ba (04:a1:51:e9:0b:ba), 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: 192.168.1.6 (192.168.1.6)
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54146 (54146), Seq: 1, Ack: 543, Len: 672

→ Hypertext Transfer Protocol

    HTTP/1.1 200 0K\r\n

    Date: Tue, 21 Oct 2014 18:56:29 GMT\r\n
    Server: Apache/2.2.3 (CentOS)\r\n
    Last-Modified: Tue, 21 Oct 2014 18:56:02 GMT\r\n
    ETag: "d6c96-173-61f21480"\r\n
    Accept-Ranges: bytes\r\n
  Content-Length: 371\r\n
    Keep-Alive: timeout=10, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
```

HTTP information for the first GET

```
Frame 191: 695 bytes on wire (5560 bits), 695 bytes captured (5560 bits) on interface 0
Ethernet II, Src: Apple_0f:31:e8 (2c:f0:ee:0f:31:e8), Dst: Netgear_e9:0b:ba (04:a1:51:e9:0b:ba)
▶ Internet Protocol Version 4, Src: 192.168.1.6 (192.168.1.6), Dst: 128.119.245.12 (128.119.245.12)
Transmission Control Protocol, Src Port: 54155 (54155), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 629

→ Hypertext Transfer Protocol

  D GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
  ▶ Cookie: __utma=198765611.1280010052.1410544820.1410544820.1410544820.1; __utmz=198765611.1410544820.1.1.utmc:
    If-None-Match: "d6c96-173-61f21480"\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    If-Modified-Since: Tue, 21 Oct 2014 18:56:02 GMT\r\n
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.78.2 (KHTML, like Gecko) Version/
    Accept-Language: en-us\r\n
    Accept Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
```

HTTP information for the first Response

```
D Frame 194: 248 bytes on wire (1984 bits), 248 bytes captured (1984 bits) on interface 0

Ethernet II, Src: Netgear_e9:0b:ba (04:a1:51:e9:0b:ba), 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: 192.168.1.6 (192.168.1.6)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54155 (54155), Seq: 1, Ack: 630, Len: 182

Hypertext Transfer Protocol

HTTP/1.1 304 Not Modified\r\n

Date: Tue, 21 0ct 2014 18:56:45 GMT\r\n

Server: Apache/2.2.3 (CentOS)\r\n

Connection: Keep-Alive\r\n

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

ETag: "d6c96-173-61f21480"\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.071133000 seconds]

[Request in frame: 191]
```

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?

[▶] Transmission Control Protocol, Src Port: 80 (80), Dst Port: 54597 (54597), Seq: 4345, Ack: 543, Len: 459

^{▷ [4} Reassembled TCP Segments (4803 bytes): #48(1448), #49(1448), #51(1448), #53(459)]

Numertext Transfer Protocol

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 Len	ngth Info
906	29.123070000	10.136.90.16	128.119.245.12	HTTP	452 GET /wireshark-lak
907	29.165655000	128.119.245.12	10.136.90.16	HTTP	838 HTTP/1.1 401 Autho
918	29.808347000	10.136.90.16	128.119.245.12	HTTP	452 GET /wireshark-lak
920	29.850044000	128.119.245.12	10.136.90.16	HTTP	839 HTTP/1.1 401 Autho
937	30.033463000	10.136.90.16	128.119.245.12	HTTP	452 GET /wireshark-lak
939	30.078984000	128.119.245.12	10.136.90.16	HTTP	839 HTTP/1.1 401 Autho
947	30.272054000	10.136.90.16	128.119.245.12	HTTP	452 GET /wireshark-lak
949	30.314452000	128.119.245.12	10.136.90.16	HTTP	839 HTTP/1.1 401 Autho
957	30.546916000	10.136.90.16	128.119.245.12	HTTP	452 GET /wireshark-lak
959	30.588014000	128.119.245.12	10.136.90.16	HTTP	839 HTTP/1.1 401 Autho
974	31.005485000	10.136.90.16	128.119.245.12	HTTP	452 GET /wireshark-lak
976	31.050469000	128.119.245.12	10.136.90.16	HTTP	839 HTTP/1.1 401 Autho
1214	31.437811000	10.136.90.16	128.119.245.12	HTTP	452 GET /wireshark-lak
4) •
▶ Frame 9	20: 839 bytes d	on wire (6712 bits), 839 by	tes captured (6712 bits) on	interface 0	
	•		:00), Dst: Apple 0f:31:e8 (1:e8)
		_	(128.119.245.12), Dst: 10.		
▶ Transmi	ssion Control F	Protocol, Src Port: 80 (80)	, Dst Port: 56874 (56874),	Seq: 1, Ack: 3	387, Len: 773
▶ Hyperte:	xt Transfer Pro	otocol		•	
D Line-ha	sed 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.