

REPORT



과 목 명 : 네트워크 응용 설계

담당교수 : 백 정 엽 교수님

제 출 일 : 2019. 04. 05

전 공 명 : 소프트웨어전공

학 번 : 20165974

이 름 : 최 정 민

[A]. The Basic HTTP GET/response interaction

Recall that since the HTTP message was carried inside a TCP segment, which was carried inside an IP datagram, which was carried within an Ethernet frame, Wireshark displays the Frame, Ethernet, IP, and TCP packet information as well.

Please focus on the HTTP message only for now, but you may also need to look at other packet information, and you're more than welcome to look at other protocol fields for your own interest (and study).

By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages and indicate where in the message you've found the information that answers the following questions.

When you hand in your assignment, annotate the output so that it's clear where in the output you're getting the information for your answer (e.g., for our classes, we ask that students markup paper copies with a pen, or annotate electronic copies with text in a colored font).

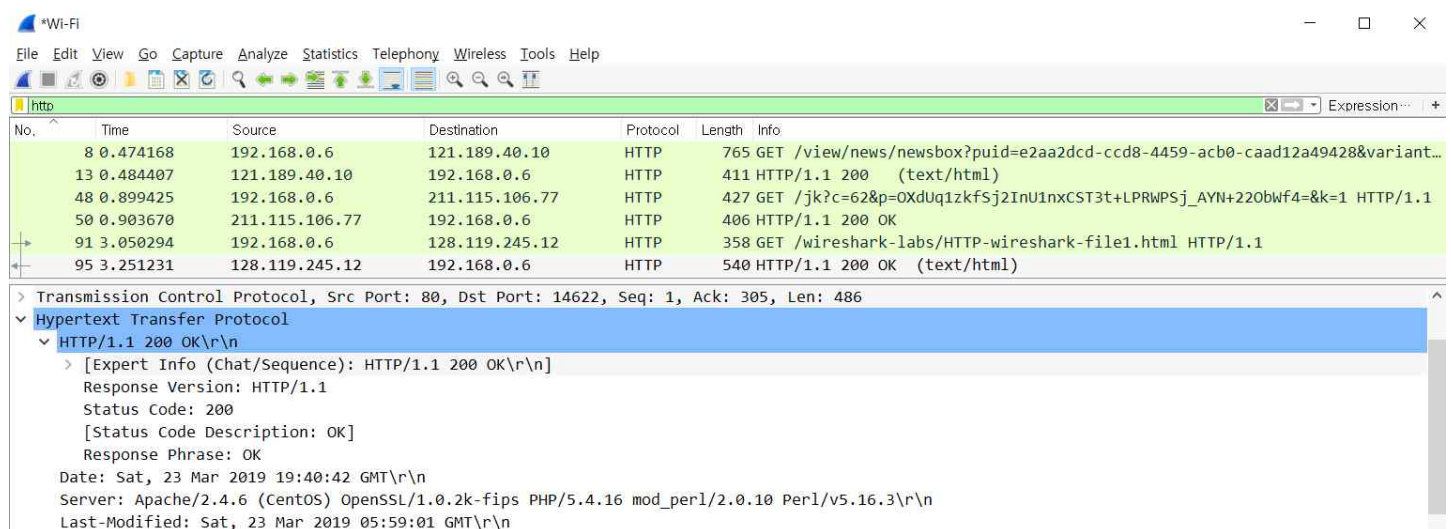
Answer the following questions:

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

The server is running http version 1.1



The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 95), which is an HTTP 200 OK response. The details pane is expanded to show the Hypertext Transfer Protocol section, which includes the response version (HTTP/1.1), status code (200), status code description (OK), response phrase (OK), date, server information, and last-modified timestamp.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.474168	192.168.0.6	121.189.40.10	HTTP	765	GET /view/news/newsbox?puid=e2aa2dcd-ccd8-4459-acb0-caad12a49428&variant...
13	0.484407	121.189.40.10	192.168.0.6	HTTP	411	HTTP/1.1 200 (text/html)
48	0.899425	192.168.0.6	211.115.106.77	HTTP	427	GET /jk?c=62&p=OXduqizkfsj2InU1nxCST3t+LPRWPSj_AYN+220bwf4=&k=1 HTTP/1.1
50	0.903670	211.115.106.77	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
91	3.050294	192.168.0.6	128.119.245.12	HTTP	358	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
95	3.251231	128.119.245.12	192.168.0.6	HTTP	540	HTTP/1.1 200 OK (text/html)

Transmission Control Protocol, Src Port: 80, Dst Port: 14622, Seq: 1, Ack: 305, Len: 486

Hypertext Transfer Protocol

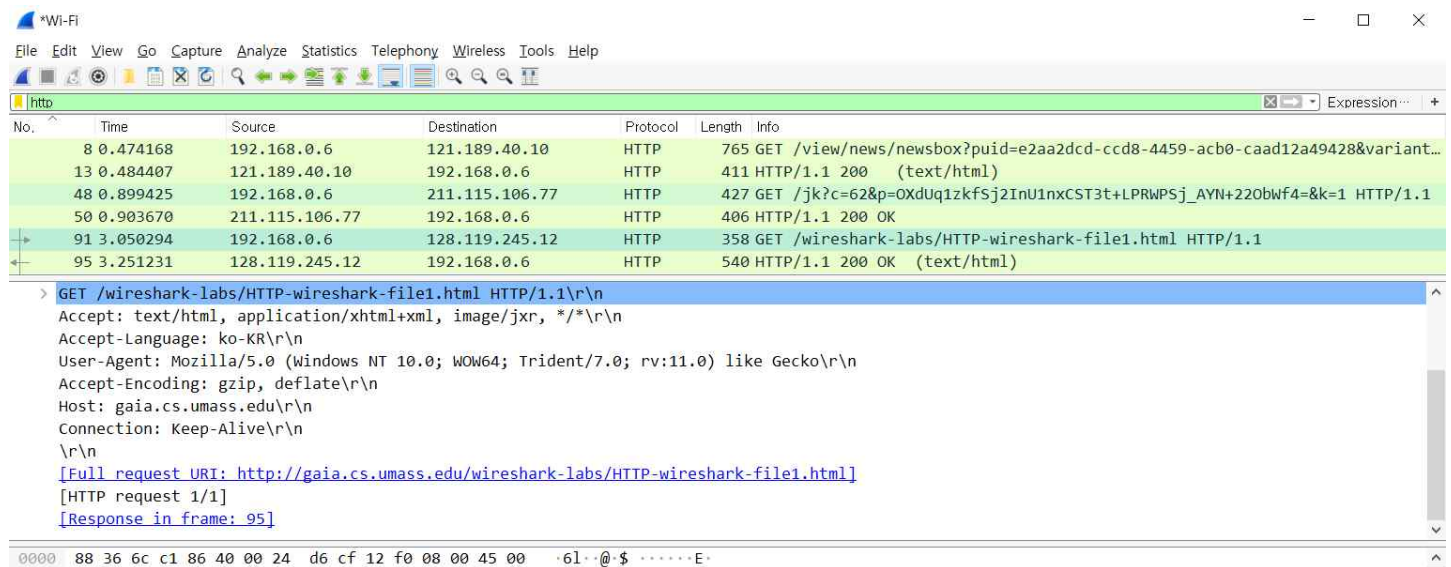
- HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Sat, 23 Mar 2019 19:40:42 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 - Last-Modified: Sat, 23 Mar 2019 05:59:01 GMT\r\n

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

Answer :

The IP address of my computer is 192.168.0.6

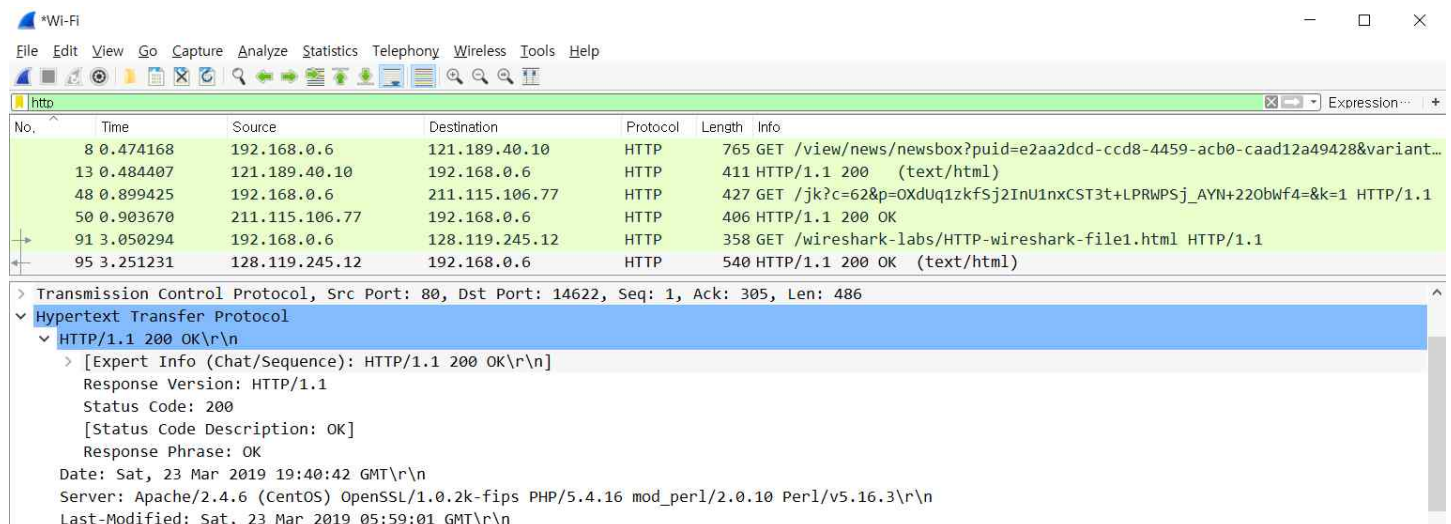
The IP address of the gaia.cs.umass.edu server is 128.119.245.12



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

Answer :

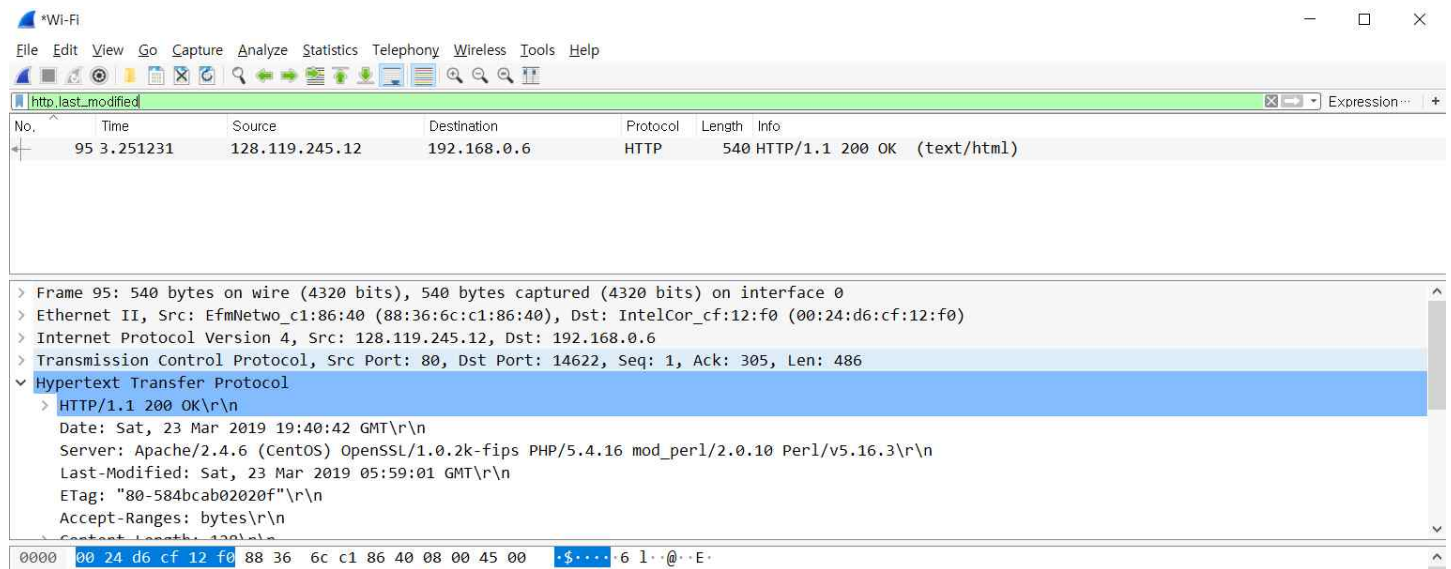
The status code returned was 200 OK



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

Answer :

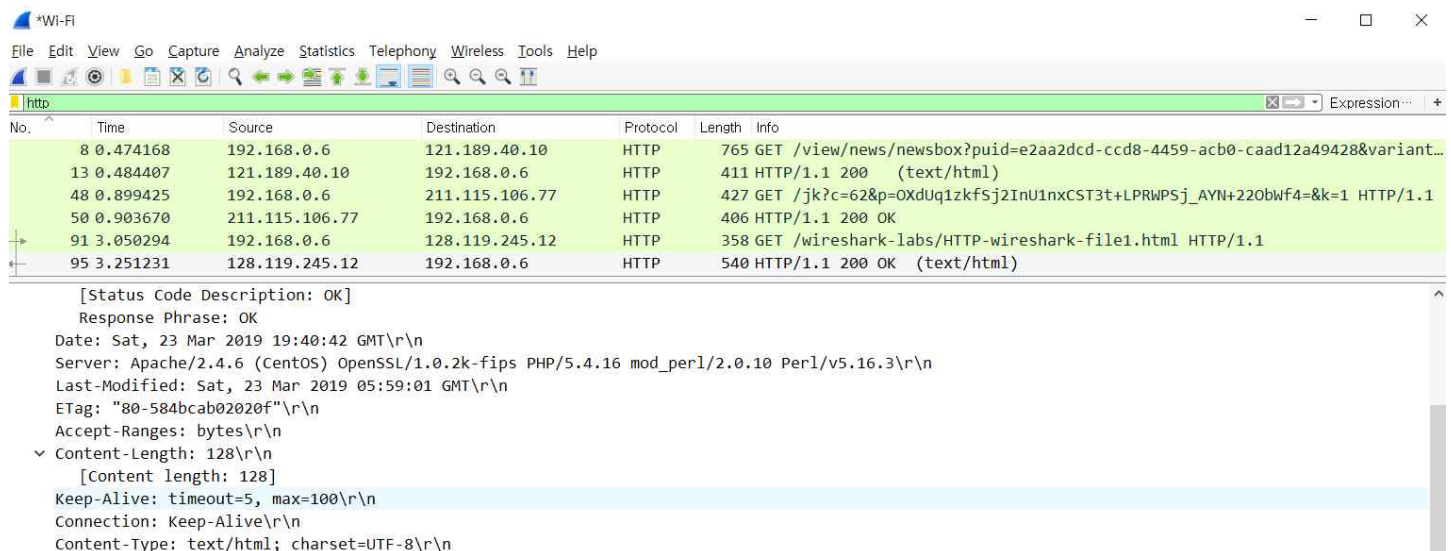
The file was last modified on Saturday, March 23, 2019 at 05:59:01 GMT



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

Answer :

128 bytes of content are being returned



[B]. The HTTP CONDITIONAL GET/response interaction → HTTP CONDITIONAL GET / 응답 상호 작용

Most web browsers perform object caching and thus perform a conditional GET when retrieving an HTTP object. Before performing the steps below, make sure your browser's cache is empty. (To do this under Internet Explorer, select Tools->Internet Options->Delete File; these actions will remove cached files from your browser's cache.) Now do the following:

- Start up your web browser, and make sure your browser's cache is cleared, as discussed above.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser
 - <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>
 - Your browser should display a very simple five-line HTML file.
- Quickly enter the same URL into your browser again
(or simply select the refresh button on your browser)
- Stop Wireshark packet capture, and enter “http” in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window.

Answer the following questions:

6. 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 there is no IF-MODIFIED-SINCE line in the GET message.

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane shows four packets, with the third packet (No. 86) selected. The packet details pane shows the selected packet's structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded, showing the GET request details. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
42	0.649469	172.30.1.28	211.115.106.204	HTTP	427	GET /jk?c=62&p=EdeIgbwsI6DNVVRVx61PuasLSgU282DzeZNI69jXtPg=&k=1 HTTP/1.1
44	0.668467	211.115.106.204	172.30.1.28	HTTP	406	HTTP/1.1 200 OK
86	1.340232	172.30.1.28	128.119.245.12	HTTP	358	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
89	1.744116	128.119.245.12	172.30.1.28	HTTP	784	HTTP/1.1 200 OK (text/html)

> Frame 86: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits) on interface 0
> Ethernet II, Src: IntelCor_cf:12:f0 (00:24:d6:cf:12:f0), Dst: Mercury_d2:4d:eb (88:3c:1c:d2:4d:eb)
> Internet Protocol Version 4, Src: 172.30.1.28, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 5818, Dst Port: 80, Seq: 1, Ack: 1, Len: 304
v Hypertext Transfer Protocol
v GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, image/jxr, */*\r\n
Accept-Language: ko-KR\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-file2.html>]
[HTTP request 1/1]
[Response in frame: 89]

0000 88 3c 1c d2 4d eb 00 24 d6 cf 12 f0 08 00 45 00 -<-M-\$E-

Wireshark - Wi-Fi 20190404224818 a18680 ncann

Partials: 156 · Downloaded: 4 (2.6%) · Downloaded: 0 (0.0%) Profile: Def

7. Inspect the contents of the server response. Did the server explicitly return the contents of the file?

Answer :

The server did explicitly return the contents of the file.

Wireshark packet capture showing an HTTP 200 OK response. The packet list shows a GET request from 172.30.1.28 to 128.119.245.12. The packet details pane shows the request URI as `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html` and the response body as HTML content.

No.	Time	Source	Destination	Protocol	Length	Info
42	0.649469	172.30.1.28	211.115.106.204	HTTP	427	GET /jk?c=62&p=EdelgbwsI6DNVVRVx61PuasLSgU282DzeZNI69jXtPg=&k=
44	0.668467	211.115.106.204	172.30.1.28	HTTP	406	HTTP/1.1 200 OK
86	1.340232	172.30.1.28	128.119.245.12	HTTP	358	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
89	1.744116	128.119.245.12	172.30.1.28	HTTP	784	HTTP/1.1 200 OK (text/html)

Line-based text data: text/html (10 lines)

```
\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
```

8. 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 in the second HTTP message an IF-MODIFIED-SINCE line is included. The information that follows is the data and time (sun, 24 Mar 2019 05:25:01 GMT)

Wireshark packet capture showing an HTTP 304 Not Modified response. The packet list shows a GET request from 192.168.0.6 to 128.119.245.12. The packet details pane shows the request URI as `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html` and the response body as empty.

No.	Time	Source	Destination	Protocol	Length	Info
55	2.634863	192.168.0.6	128.119.245.12	HTTP	613	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
59	2.839535	128.119.245.12	192.168.0.6	HTTP	784	HTTP/1.1 200 OK (text/html)
97	4.074423	192.168.0.6	211.115.106.80	HTTP	427	GET /jk?c=62&p=OXduq1zkfsj2InU1nxCST3t+LPRWPSj_AYN+220bwf4=&k=1 HTTP/1.1
100	4.078805	211.115.106.80	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
127	5.779144	192.168.0.6	128.119.245.12	HTTP	613	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
128	5.981472	128.119.245.12	192.168.0.6	HTTP	293	HTTP/1.1 304 Not Modified

Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file2.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "173-584d04f474ed4"\r\n
If-Modified-Since: Sun, 24 Mar 2019 05:25:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
[HTTP request 2/2]

9. 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 :

The HTTP status code is 304 and Response Phrase is Not Modified

The server did not return the contents of the file because the browser simply retrieved the contents from its cache

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The packet list pane displays several HTTP packets. The selected packet is number 128, which is an HTTP 304 Not Modified response. The packet details pane shows the following information:

- Protocol: Hypertext Transfer Protocol
- HTTP/1.1 304 Not Modified\r\n
- [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
- Response Version: HTTP/1.1
- Status Code: 304
- [Status Code Description: Not Modified]
- Response Phrase: Not Modified
- Date: Sun, 24 Mar 2019 05:25:07 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
- Connection: Keep-Alive\r\n
- Keep-Alive: timeout=5, max=99\r\n
- ETag: "173-584d04f474ed4"\r\n
- \r\n
- [HTTP response 2/2]
- [Time since request: 0.202328000 seconds]
- [Prev request in frame: 55]

[C]. Retrieving Long Documents //긴 문서 검색

In our examples thus far, the documents retrieved have been simple and short HTML files. Let's next see what happens when we download a long HTML file. Do the following:

- Start up your web browser, and make sure your browser's cache is cleared
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser
 - <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>
- Stop Wireshark packet capture, and filter "http"

In the packet-listing window, you should see your HTTP GET message, followed by a multiple-packet TCP response to your HTTP GET request.

Answer the following questions:

10. How many HTTP GET request messages did your browser send?
Which packet number in the trace contains the GET message for the 'Bill of Rights'?

Answer :

My browser sent 1 HTTP GET request to the server except favicon.ico.
The Packet that contained the GET message was packet number 232

The image shows a Wireshark packet capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The packet list pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet is number 232, which is an HTTP GET request for the file <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>. The packet details pane shows the structure of the HTTP request, including the Host, Connection, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language, If-None-Match, and If-Modified-Since headers. The packet bytes pane shows the raw data of the packet in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
232	2.856160	10.210.45.172	128.119.245.12	HTTP	620	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
248	2.880755	10.210.45.172	211.115.106.201	HTTP	427	GET /jk?c=62&p=EdelgbwsI6DNVVRVx61PuasLSgU282DzeZNI69jXtPg=&k=1 HTTP/1.1
250	2.897932	211.115.106.201	10.210.45.172	HTTP	406	HTTP/1.1 200 OK
271	3.072675	128.119.245.12	10.210.45.172	HTTP	757	HTTP/1.1 200 OK (text/html)
305	3.202957	10.210.45.172	211.115.106.201	HTTP	451	GET /jk?c=62&p=EdelgbwsI6DNVVRVx61PuasLSgU282DzeZNI69jXtPg=&k=1 HTTP/1.1
309	3.206988	211.115.106.201	10.210.45.172	HTTP	406	HTTP/1.1 200 OK
310	3.214935	10.210.45.172	128.119.245.12	HTTP	471	GET /favicon.ico HTTP/1.1
357	3.420836	128.119.245.12	10.210.45.172	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "1194-58599f346a041"\r\n
If-Modified-Since: Wed, 03 Apr 2019 05:59:01 GMT\r\n
\r\n
[Full request URI: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>]
[HTTP request 1/2]
[Response in frame: 271]

0000 00 00 5e 00 01 18 00 24 d6 cf 12 f0 08 00 45 00 ..^...\$E..

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

Answer :

The status code was 200 and phrase was OK in the response

The screenshot shows a Wireshark packet capture of an HTTP response. The packet list pane displays several packets, with packet 271 selected. The packet details pane shows the structure of the HTTP response, including the status code 200 and the phrase 'OK'.

No.	Time	Source	Destination	Protocol	Length	Info
232	2.856160	10.210.45.172	128.119.245.12	HTTP	620	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
248	2.880755	10.210.45.172	211.115.106.201	HTTP	427	GET /jk?c=62&p=EdelgbwsI6DNVVRVx61PuasLSgU282DzeZNI69jXtPg=&k=1 HTTP/1.1
250	2.897932	211.115.106.201	10.210.45.172	HTTP	406	HTTP/1.1 200 OK
271	3.072675	128.119.245.12	10.210.45.172	HTTP	757	HTTP/1.1 200 OK (text/html)
305	3.202957	10.210.45.172	211.115.106.201	HTTP	451	GET /jk?c=62&p=EdelgbwsI6DNVVRVx61PuasLSgU282DzeZNI69jXtPg=&k=1 HTTP/1.1
309	3.206988	211.115.106.201	10.210.45.172	HTTP	406	HTTP/1.1 200 OK
310	3.214935	10.210.45.172	128.119.245.12	HTTP	471	GET /favicon.ico HTTP/1.1
357	3.420836	128.119.245.12	10.210.45.172	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Packet 271 details:

- [4 Reassembled TCP Segments (4861 bytes): #268(1386), #269(1386), #270(1386), #271(703)]
- Hypertext Transfer Protocol
 - HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - Response Version: HTTP/1.1
 - Status Code: 200
 - [Status Code Description: OK]
 - Response Phrase: OK
 - Date: Thu, 04 Apr 2019 11:55:43 GMT\r\n
 - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
 - Last-Modified: Thu, 04 Apr 2019 05:59:01 GMT\r\n
 - ETag: "1194-585ae11189d71"\r\n
 - Accept-Ranges: bytes\r\n

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

Answer :

The data was sent in 4 TCP segments to browser, then reassembled.

The screenshot shows a Wireshark packet capture of an HTTP response. The packet list pane displays several packets, with packet 271 selected. The packet details pane shows the structure of the HTTP response, including the status code 200 and the phrase 'OK'.

No.	Time	Source	Destination	Protocol	Length	Info
250	2.897932	211.115.106.201	10.210.45.172	HTTP	406	HTTP/1.1 200 OK
271	3.072675	128.119.245.12	10.210.45.172	HTTP	757	HTTP/1.1 200 OK (text/html)
305	3.202957	10.210.45.172	211.115.106.201	HTTP	451	GET /jk?c=62&p=EdelgbwsI6DNVVRVx61PuasLSgU282DzeZNI69jXtPg=&k=1 HT...
309	3.206988	211.115.106.201	10.210.45.172	HTTP	406	HTTP/1.1 200 OK
310	3.214935	10.210.45.172	128.119.245.12	HTTP	471	GET /favicon.ico HTTP/1.1
357	3.420836	128.119.245.12	10.210.45.172	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Packet 271 details:

- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (703 bytes)
- TCP segment data (703 bytes)
- [4 Reassembled TCP Segments (4861 bytes): #268(1386), #269(1386), #270(1386), #271(703)]
 - [Frame: 268, payload: 0-1385 (1386 bytes)]
 - [Frame: 269, payload: 1386-2771 (1386 bytes)]
 - [Frame: 270, payload: 2772-4157 (1386 bytes)]
 - [Frame: 271, payload: 4158-4860 (703 bytes)]
 - [Segment count: 4]
 - [Reassembled TCP length: 4861]
 - [Reassembled TCP Data: 485454502f312e312032303204f4b0d0a446174653a2054...]
- Hypertext Transfer Protocol
- Line-based text data: text/html (98 lines)

[D]. HTML Documents with Embedded Objects // 내장된 개체가 있는 HTML 문서

Now that we've seen how Wireshark displays the captured packet traffic for large HTML files, we can look at what happens when your browser downloads a file with embedded objects, i.e., a file that includes other objects (in the example below, image files) that are stored on another server(s). Do the following:

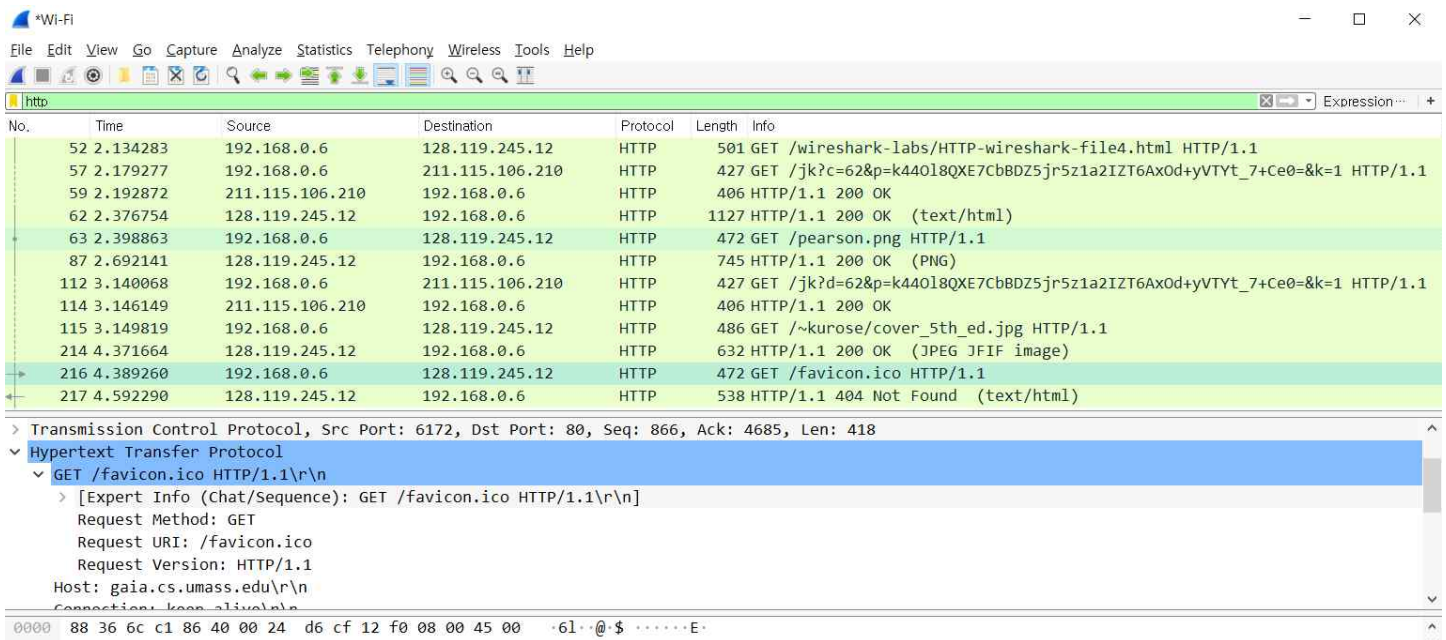
- Start up your web browser, and make sure your browser's cache is cleared.
- Start up the Wireshark packet sniffer
- Enter the following URL into your browser
 - <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>
 - Your browser should display a short HTML file with two images. These two images are referenced in the base HTML file. That is, the images themselves are not contained in the HTML; instead the URLs for the images are contained in the downloaded HTML file. Your browser will have to retrieve these logos from the indicated web sites, one from the gaia.cs.umass.edu web site, and another from caite.cs.umass.edu server.
- Stop Wireshark packet capture, and filter "http".

Answer the following questions:

13. How many HTTP GET request messages did your browser send?

Answer :

My browser sent 3 http GET message requests except favicon.ico.



To which Internet addresses were these GET requests sent?

Answer :

Initial Page address : 128.119.245.12

Pearson.png : 128.119.245.12

cover_5th_ed.jpg : 128.119.245.12

(favicon.ico (128.119.245.12))

The image shows a Wireshark packet capture window titled '*Wi-Fi'. The main pane displays a list of captured packets. The first several packets are HTTP GET requests from 192.168.0.6 to 128.119.245.12. The selected packet is packet 52, an HTTP GET request for /wireshark-labs/HTTP-wireshark-file4.html. The packet details pane on the right shows the structure of the HTTP request, including the method (GET), request URI, version (1.1), host (gaia.cs.umass.edu), and connection (keep-alive). The packet bytes pane at the bottom shows the raw data of the request, starting with the GET method and the request URI.

No.	Time	Source	Destination	Protocol	Length	Info
52	2.134283	192.168.0.6	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
63	2.398863	192.168.0.6	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
115	3.149819	192.168.0.6	128.119.245.12	HTTP	486	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
216	4.389260	192.168.0.6	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
59	2.192872	211.115.106.210	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
62	2.376754	128.119.245.12	192.168.0.6	HTTP	1127	HTTP/1.1 200 OK (text/html)
87	2.692141	128.119.245.12	192.168.0.6	HTTP	745	HTTP/1.1 200 OK (PNG)
114	3.146149	211.115.106.210	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
214	4.371664	128.119.245.12	192.168.0.6	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)
217	4.592290	128.119.245.12	192.168.0.6	HTTP	538	HTTP/1.1 404 Not Found (text/html)
57	2.179277	192.168.0.6	211.115.106.210	HTTP	427	GET /jk?c=62&p=k44018QXE7CbBDZ5jr5z1a2IZT6Ax0d+yVTYt_7+Ce0=&k=1 HTTP/1.1
112	3.140068	192.168.0.6	211.115.106.210	HTTP	427	GET /jk?d=62&p=k44018QXE7CbBDZ5jr5z1a2IZT6Ax0d+yVTYt_7+Ce0=&k=1 HTTP/1.1

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n

> [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file4.html

Request Version: HTTP/1.1

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

Connection: keep-alive\r\n

Unassigned Requester: 1/1/1/1

0030 00 44 24 8f 00 00 47 45 54 20 2f 77 69 72 65 73 ·D\$···GE T /wires

14. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel?

Answer :

In the captures below, the time in the PNG and JPEG JFIF images will differ by 1 second. Therefore, you can see that they were downloaded sequentially from both websites.

This screenshot shows a Wireshark packet capture of an HTTP session. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
52	2.134283	192.168.0.6	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
57	2.179277	192.168.0.6	211.115.106.210	HTTP	427	GET /jk?c=62&p=k440l8QXE7CbBDZ5jr5z1a2IZT6AxOd+yVTYt_7+Ce0=&k=1 HTTP/1.1
59	2.192872	211.115.106.210	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
62	2.376754	128.119.245.12	192.168.0.6	HTTP	1127	HTTP/1.1 200 OK (text/html)
63	2.398863	192.168.0.6	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
87	2.692141	128.119.245.12	192.168.0.6	HTTP	745	HTTP/1.1 200 OK (PNG)
112	3.140068	192.168.0.6	211.115.106.210	HTTP	427	GET /jk?d=62&p=k440l8QXE7CbBDZ5jr5z1a2IZT6AxOd+yVTYt_7+Ce0=&k=1 HTTP/1.1
114	3.146149	211.115.106.210	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
115	3.149819	192.168.0.6	128.119.245.12	HTTP	486	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
214	4.371664	128.119.245.12	192.168.0.6	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)
216	4.389260	192.168.0.6	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
217	4.592290	128.119.245.12	192.168.0.6	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet details pane for the selected packet (No. 87) shows the following information:

- [Status Code Description: OK]
- Response Phrase: OK
- Date: Sun, 24 Mar 2019 13:42:34 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
- Last-Modified: Sat, 06 Aug 2016 10:08:14 GMT\r\n
- ETag: "cc3-539645c7f1ee7"\r\n
- Accept-Ranges: bytes\r\n
- > Content-Length: 3267\r\n
- Keep-Alive: timeout=5, max=90\r\n

Frame (745 bytes) | Reassembled TCP (3611 bytes)

This screenshot shows a Wireshark packet capture of an HTTP session, similar to the one above. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
52	2.134283	192.168.0.6	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
57	2.179277	192.168.0.6	211.115.106.210	HTTP	427	GET /jk?c=62&p=k440l8QXE7CbBDZ5jr5z1a2IZT6AxOd+yVTYt_7+Ce0=&k=1 HTTP/1.1
59	2.192872	211.115.106.210	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
62	2.376754	128.119.245.12	192.168.0.6	HTTP	1127	HTTP/1.1 200 OK (text/html)
63	2.398863	192.168.0.6	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
87	2.692141	128.119.245.12	192.168.0.6	HTTP	745	HTTP/1.1 200 OK (PNG)
112	3.140068	192.168.0.6	211.115.106.210	HTTP	427	GET /jk?d=62&p=k440l8QXE7CbBDZ5jr5z1a2IZT6AxOd+yVTYt_7+Ce0=&k=1 HTTP/1.1
114	3.146149	211.115.106.210	192.168.0.6	HTTP	406	HTTP/1.1 200 OK
115	3.149819	192.168.0.6	128.119.245.12	HTTP	486	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
214	4.371664	128.119.245.12	192.168.0.6	HTTP	632	HTTP/1.1 200 OK (JPEG JFIF image)
216	4.389260	192.168.0.6	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
217	4.592290	128.119.245.12	192.168.0.6	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet details pane for the selected packet (No. 87) shows the following information:

- [Status Code Description: OK]
- Response Phrase: OK
- Date: Sun, 24 Mar 2019 13:42:35 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n
- Last-Modified: Tue, 15 Sep 2009 18:23:27 GMT\r\n
- ETag: "18a68-473a1e0e6e5c0"\r\n
- Accept-Ranges: bytes\r\n
- > Content-Length: 100968\r\n

Frame (745 bytes) | Reassembled TCP (3611 bytes)

