

HOMEWORK 1

Hale Şahin – 150116841

I.

1. HTTP server 1.1 is running on my server.

No.	Time	Source	Destination	Protocol	Length	Info
35	7.021953	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	7.160380	128.119.245.12	192.168.1.39	HTTP	540	HTTP/1.1 200 OK (text/html)

```
> Frame 40: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0
> Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.39
> Transmission Control Protocol, Src Port: 80, Dst Port: 54975, Seq: 1, Ack: 448, Len: 486
< Hypertext Transfer Protocol
  < HTTP/1.1 200 OK\r\n
    Date: Mon, 16 Oct 2017 13:28:57 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: Mon, 16 Oct 2017 05:59:01 GMT\r\n
    ETag: "80-55ba3b4031322"\r\n
    Accept-Ranges: bytes\r\n
  < Content-Length: 128\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.138427000 seconds]
    [Request in frame: 35]
    File Data: 128 bytes
  < Line-based text data: text/html
```

2. It accepts both Turkish and Englis-US.

```
Hypertext Transfer Protocol
  < GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.62 Safari/537.36\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.6,en;q=0.4\r\n
    \r\n
```

3. Ip address of my computer is first line's source 192.168.1.39. And the server's ip address is 128.119.245.12.

No.	Time	Source	Destination	Protocol	Length	Info
35	7.021953	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	7.160380	128.119.245.12	192.168.1.39	HTTP	540	HTTP/1.1 200 OK (text/html)

4. The code is “200 OK”.

No.	Time	Source	Destination	Protocol	Length	Info
35	7.021953	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
40	7.160380	128.119.245.12	192.168.1.39	HTTP	540	HTTP/1.1 200 OK (text/html)
236	61.005491	192.168.1.39	23.209.100.127	HTTP	212	GET /cgtile/v1/tr-TR/HealthAndFitness/Home.xml?cgversion=v6 HTTP/1.1
239	61.007164	192.168.1.39	195.175.112.112	HTTP	242	GET /api/feed/?view-name=data&name=livetile&market=tr-TR&version=2_0&format=xml HTTP/1.1
242	61.018710	23.209.100.127	192.168.1.39	HTTP/XML	148	HTTP/1.1 200 OK
245	61.022330	195.175.112.112	192.168.1.39	HTTP	1340	HTTP/1.1 200 OK (application/json)
880	271.584185	192.168.1.39	23.209.102.106	HTTP	271	GET /singletile/summary/alias/experiencebyname/today?market=tr-TR&source=appxmanifest&tenant=amp&vertical=s...
883	271.598750	23.209.102.106	192.168.1.39	HTTP/XML	232	HTTP/1.1 200 OK

> Frame 40: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface 0

> Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.39

> Transmission Control Protocol, Src Port: 80, Dst Port: 54975, Seq: 1, Ack: 448, Len: 486

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Mon, 16 Oct 2017 13:28:57 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: Mon, 16 Oct 2017 05:59:01 GMT\r\n

ETag: "80-55ba3b4031322"\r\n

Accept-Ranges: bytes\r\n

> Content-Length: 128\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

5. The file last modified at the server on Monday, October 16, 2017 at 05:59:01 GMT.

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Date: Mon, 16 Oct 2017 13:28:57 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: Mon, 16 Oct 2017 05:59:01 GMT\r\n

ETag: "80-55ba3b4031322"\r\n

Accept-Ranges: bytes\r\n

> Content-Length: 128\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/1]

6. The returned content's length is 128 bytes.

Last-Modified: Mon, 16 Oct 2017 05:59:01 GMT\r\n

ETag: "80-55ba3b4031322"\r\n

Accept-Ranges: bytes\r\n

Content-Length: 128\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

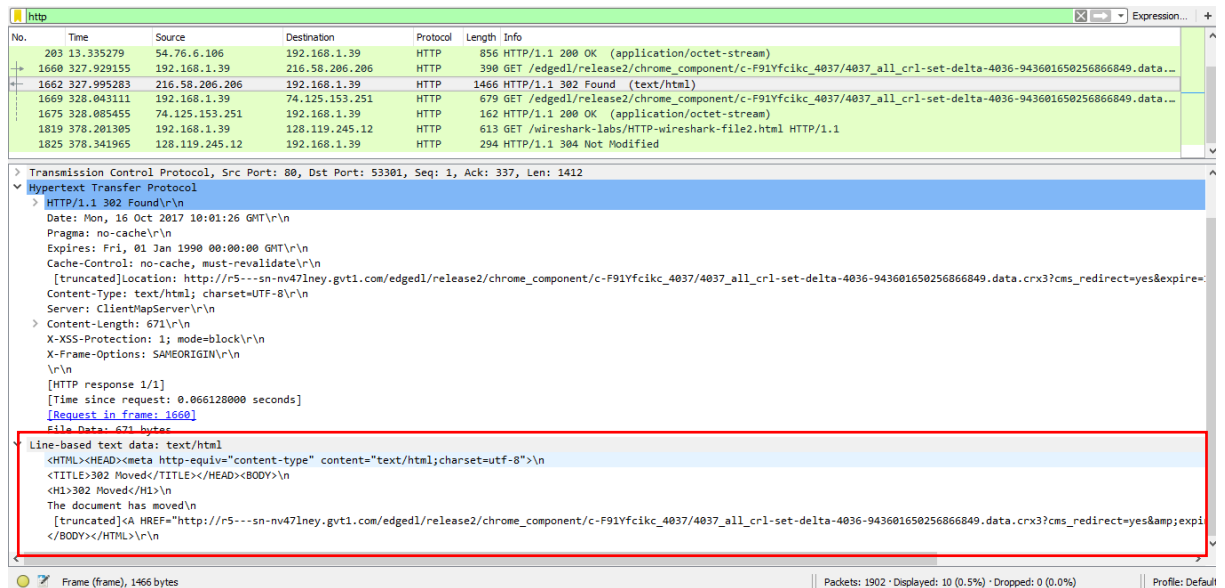
\r\n

7. No. I cannot see any different headings between them.

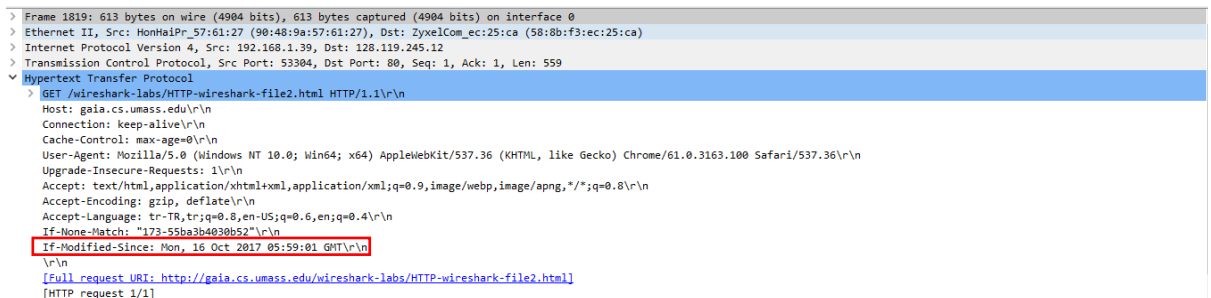
II.

8. No, I don't see any “IF-MODIFIED-SINCE” line in the first http_GET.

9. The server returned the contents of the file explicitly. There is a part called “Line-Based Text Data”, that means what the contents of server sending to my browser.



10. Yes, for the second http-get, there is a “IF-MODIFIED-SINCE” line.



- 11.

The status code “304 Not Modified” as its shown in the figure below.

The browser retrieved the contents from the cache, thats why the server didnt return the contents of the file. Had the file been modified since it was last accessed, it would have returned the contents of the file, instead it simply told my browser to retrieve the old file from its cached memory.

```

- 1825 378.341965 128.119.245.12 192.168.1.39 HTTP 294 HTTP/1.1 304 Not Modified
+
+ Frame 1825: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface 0
+ Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
+ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.39
+ Transmission Control Protocol, Src Port: 80, Dst Port: 53304, Seq: 1, Ack: 560, Len: 240
+ Hypertext Transfer Protocol
+   > HTTP/1.1 304 Not Modified\r\n
+     Date: Mon, 16 Oct 2017 10:02:16 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=100\r\n
+     ETag: "173-55ba3b4030b52"\r\n
+     \r\n
+     [HTTP response 1/1]
+     [Time since request: 0.140660000 seconds]
+     [Request in frame: 1819]

```

III.

12. There is only 1 send HTTP GET request to the server. And its packet number is 170.

No.	Time	Source	Destination	Protocol	Length	Info
170	18.775420	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
178	18.928896	128.119.245.12	192.168.1.39	HTTP	559	HTTP/1.1 200 OK (text/html)
180	19.006804	192.168.1.39	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
181	19.156102	128.119.245.12	192.168.1.39	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```

+
+ Frame 170: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
+ Ethernet II, Src: HonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
+ Internet Protocol Version 4, Src: 192.168.1.39, Dst: 128.119.245.12
+ Transmission Control Protocol, Src Port: 53656, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
+ Hypertext Transfer Protocol
+   > GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
+     Host: gaia.cs.umass.edu\r\n
+     Connection: keep-alive\r\n
+     User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36\r\n
+     Upgrade-Insecure-Requests: 1\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: tr-TR,tr;q=0.8,en-US;q=0.6,en;q=0.4\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: 178]
+     [Next request in frame: 180]

```

13. Status code and phrase that server sent as response is in the packet numbered 178.

No.	Time	Source	Destination	Protocol	Length	Info
170	18.775420	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
178	18.928896	128.119.245.12	192.168.1.39	HTTP	559	HTTP/1.1 200 OK (text/html)
180	19.006804	192.168.1.39	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
181	19.156102	128.119.245.12	192.168.1.39	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```

+
+ Frame 178: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface 0
+ Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: HonHaiPr_57:61:27 (90:48:9a:57:61:27)
+ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.39
+ Transmission Control Protocol, Src Port: 80, Dst Port: 53656, Seq: 4357, Ack: 448, Len: 505
+ [4 Reassembled TCP Segments (4861 bytes): #174(1452), #175(1452), #177(1452), #178(505)]
+ Hypertext Transfer Protocol
+   > HTTP/1.1 200 OK\r\n
+     Date: Mon, 16 Oct 2017 11:51:16 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: Mon, 16 Oct 2017 05:59:01 GMT\r\n
+     ETag: "1194-55ba3b402d88a"\r\n
+     Accept-Ranges: bytes\r\n
+     Content-Length: 4500\r\n
+     Keep-Alive: timeout=5, max=100\r\n
+     Connection: Keep-Alive\r\n
+     Content-Type: text/html; charset=UTF-8\r\n
+     \r\n
+     [HTTP response 1/2]
+     [Time since request: 0.153476000 seconds]
+     [Request in frame: 170]
+     [Next request in frame: 180]
+     [Next response in frame: 181]
+     File Data: 4500 bytes
+
+ Line-based text data: text/html
+   <html><head> \n
+   <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
+   \n

```

14. The code and phrase at the response is 200 OK.

15. Data is sent in 4 TCP segments to the browser and then reassembled.

No.	Time	Source	Destination	Protocol	Length	Info
170	18.775420	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
178	18.928896	128.119.245.12	192.168.1.39	HTTP	559	HTTP/1.1 200 OK (text/html)
180	19.006804	192.168.1.39	128.119.245.12	HTTP	472	GET /favicon.ico HTTP/1.1
181	19.156102	128.119.245.12	192.168.1.39	HTTP	538	HTTP/1.1 404 Not Found (text/html)

> Frame 178: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface 0
> Ethernet II, Src: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca), Dst: MonHaiPr_57:61:27 (90:48:9a:57:61:27)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.39
> Transmission Control Protocol, Src Port: 80, Dst Port: 53656, Seq: 4357, Ack: 448, Len: 505
> 4 Reassembled TCP Segments (4861 bytes): #174(1452), #175(1452), #177(1452), #178(505)
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Date: Mon, 16 Oct 2017 11:51:16 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: Mon, 16 Oct 2017 05:59:01 GMT\r\n

IV.

16. My browser sent 3 HTTP GET message requests. They are in order, the initial page, pearson logo.png, and the cover of the pearson book 5th ed.

- ❖ Initial page address : 128.119.245.12
- ❖ Logo address : 128.119.245.12
- ❖ Cover address : 128.119.240.90

No.	Time	Source	Destination	Protocol	Length	Info
67	3.488424	fe80::a8a0:4de6:310...	fe80::8d73:a52b:eb3...	HTTP/X...	807	POST /412b429c-83ea-4fce-90b5-edefe733c3e9/ HTTP/1.1
72	3.490079	fe80::a8a0:4de6:310...	fe80::8d73:a52b:eb3...	HTTP/X...	807	POST /412b429c-83ea-4fce-90b5-edefe733c3e9/ HTTP/1.1
80	3.501503	fe80::8d73:a52b:eb3...	fe80::a8a0:4de6:310...	HTTP/X...	1333	HTTP/1.1 200
81	3.502021	fe80::8d73:a52b:eb3...	fe80::a8a0:4de6:310...	HTTP/X...	1333	HTTP/1.1 200
115	4.223065	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
127	4.369699	128.119.245.12	192.168.1.39	HTTP	1127	HTTP/1.1 200 OK (text/html)
130	4.402675	192.168.1.39	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
131	4.402870	192.168.1.39	128.119.240.90	HTTP	486	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
135	4.542102	128.119.245.12	192.168.1.39	HTTP	761	HTTP/1.1 200 OK (PNG)
137	4.547533	128.119.240.90	192.168.1.39	HTTP	510	HTTP/1.1 302 Found (text/html)
149	4.693912	192.168.1.39	128.119.240.90	HTTP	486	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
262	5.446879	128.119.240.90	192.168.1.39	HTTP	1078	HTTP/1.1 200 OK (JPEG JFIF image)

> Frame 115: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface 0
> Ethernet II, Src: MonHaiPr_57:61:27 (90:48:9a:57:61:27), Dst: ZyxelCom_ec:25:ca (58:8b:f3:ec:25:ca)
> Internet Protocol Version 4, Src: 192.168.1.39, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53795, Dst Port: 80, Seq: 1, Ack: 1, Len: 447
> Hypertext Transfer Protocol

17. I thought that my browser downloaded the images in serially. That's because first images was requested and send, when it is came back then second image is requested by the browser. If they had downloaded parallel then the requests would have been in the same time, but they didnt.

