# **HOMEWORK 1**

# Hale Şahin – 150116841

I.

**1.** HTTP server 1.1 is running on my server. Source 192.168.1.39

			0					
٧o.	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)			
> Fr	ame 40: 540 bytes	on wire (4320 bits),	540 bytes captured (	4320 bit	s) on interface 0			
> Et	hernet II, Src: Z	yxelCom_ec:25:ca (58:	8b:f3:ec:25:ca), Dst:	HonHaiP	r_57:61:27 (90:48:9a:57:61:27)			
> In	Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.39							
			80, Dst Port: 54975,	Seq: 1,	Ack: 448, Len: 486			
Ну	Y Hypertext Transfer Protocol							
>	> HTTP/1.1 200 0K\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 Content-Type: text/ntml; charactering on which [HTTP response 1/1]
[Time since request: 0.138427000 seconds]
[Request in frame: 35]
File Data: 128 bytes
> Line-based text data: text/html

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) AppleWe
   Upgrade-Insecure-Requests: 1\r\n
   Accept: text/html,application/xhtml+xml,application/xml;q=0.9
   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
```

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

٧c		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
H	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".

```
Destination
                                                                                                                                                       Protocol Length Info
         35 7.021953
                                                   192.168.1.39
                                                                                                     128.119.245.12
                                                                                                                                                                                 501 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
      40 7.160380
236 61.005491
                                                                                                    192.168.1.39
23.209.100.127
                                                                                                                                                 HTTP 540 HTTP/1.1 200 OK (text/html)
HTTP 212 GET /cgtile/vl/tr-TR/HealthAndFitness/Home.xml?cgversion=v6 HTTP/1.1
                                                 128.119.245.12
                                                   192.168.1.39
                                                                                                                                                                       212 UET / CERTIEVY/ ET TA / CERTIFVI ET 
      239 61.007164
                                                 192,168,1,39
                                                                                                     195.175.112.112
                                                                                                                                                       HTTP
                                                                                                    192.168.1.39
192.168.1.39
       242 61.018710
                                                 23.209.100.127
                                                                                                                                                      HTTP 1340 HTTP/1.1 200 OK (application/json)
HTTP 271 GET /singletile/summary/alias/expers
      245 61.022330
                                                 195.175.112.112
       880 271.584185
                                             192.168.1.39
                                                                                                    23.209.102.106
                                                                                                                                                                             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/X... 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: \dot{\text{text/html}}; charset=UTF-8\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
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.

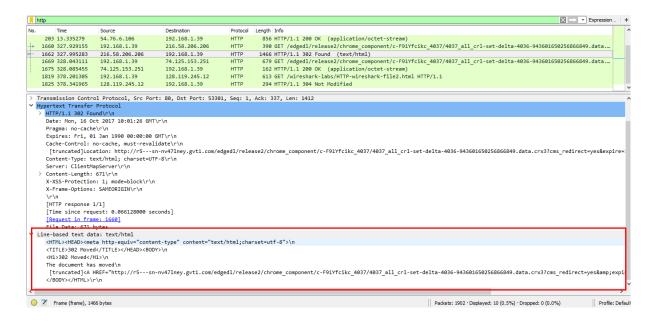
```
Last-Modified: Mon, 16 Oct 2017 05:59:01 GMT\r\n
ETag: "80-55ba3b4031322"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html; charset=UTF-8\r\n
```

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

II.

**8.** No, I dont 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.

```
Frame 1819: 613 bytes on wire (4904 bits), 613 bytes captured (4904 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: 53304, Dst Port: 80, Seq: 1, Ack: 1, Len: 559

***Mypertext Transfer Protocol

**SET Vinteshark-labs/HITP-wireshark-file2.html HTTP/1.1\r\n

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

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

User-Agent: Mozilla/5.0 (kindows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36\r\n

Ubgrade-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-Language: traft, trj=0-8, en-U5;q=0.6, en;q=0.4\r\n

If-Mode-Natch: '173-55ba30403052'\r\n

If-Mode-Natch: '173-55ba30403052'\r\n

If-Mode-Natch: '173-55ba30403052'\r\n

If-Mode-Natch: '173-55ba30403052'\r\n

If-Ul request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

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

[HTTP request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

#### 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.

```
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

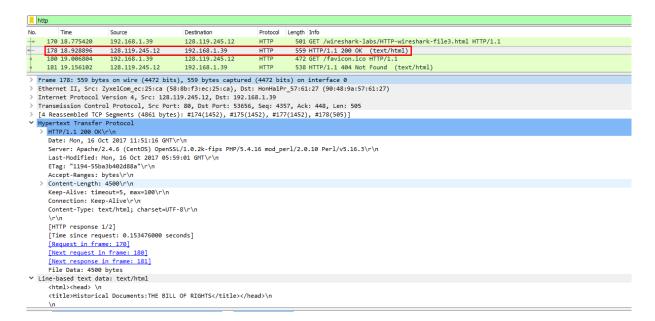
HTTP/1.1 304 Not Modified\n\n
Date: Mon, 16 Oct 2017 10:82:16 GMT\n\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\n\n
Connection: Keep-Alive\n\n
Keep-Alive: timeout-5, max=100\n\n
ETag: "173-55ba3b4030b52"\n\n
\n\n
[HTTP response 1/1]
[Time since request: 0.140660000 seconds]
[Request in frame: 1819]
```

## III.

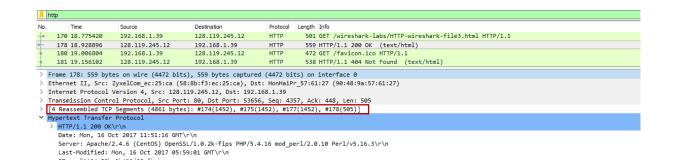
**12.** There is only 1 sended HTTP GET request to the server. And its packet number is 170.

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		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)									
\ E.	170. E01 but-	wine (4000 bits)	, 501 bytes captured	/4000 bi	+=\ ==	laborina A									
		, ,		•		:ca (58:8b:f3:ec:25:ca)									
			8.1.39, Dst: 128.119.		m_ec:25	:ca (56:00:15:ec:25:ca)									
		*	53656, Dst Port: 80,		Ack. 1	len: 447									
	pertext Transfer		55050, DSC FOI C. 00,	3eq. 1,	ACK. I	, cen. 447									
. 119		abs/HTTP-wireshark-fi	le3 html HTTD/1 1\r\n												
	Host: gaia.cs.um		103.110111 1111171.11(1)												
	Connection: keep														
			9 0. Win64: v64) Annle	-WehKi+/	537 36	(KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36\r\n									
	Upgrade-Insecure		0.0, WINO+, XO+/ Appl	LWCDKIC/	337.30	(MITTLE, 11KC decko) elifolile/01.0.5105.100 541411/357.50(1(II									
			ml application/vml:d=6	a G imag	e/wehn	image/apng,*/*;q=0.8\r\n									
		gzip, deflate\r\n	mijuppiicucion/ xmijq-	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	c/ wcop,	mage/ aprile; / jq-0.0 \( \( \)									
		tr-TR,tr;q=0.8,en-US	:a=0 6 en:a=0 4\r\n												
	\r\n	ci injerja-010jen 05	,q-0.0,cn,q-0.+(r (n												
	v vi [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]															
									0000	-	ca 90 48 9a 57 61 27	00 00 15 00 V V	H Wa'		

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



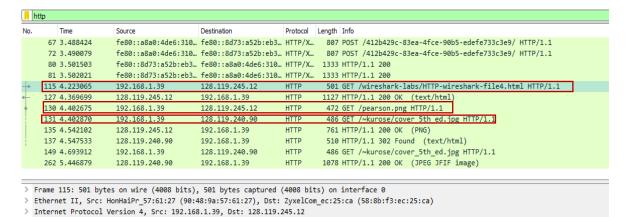
- **14.** The code and phrase at the response is 200 OK.
- **15.** Data is sended in 4 TCP segments to the browser and then reassembled.



## 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.

Inital page address: 128.119.245.12
Logo address: 128.119.245.12
Cover address: 128.119.240.90



> 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. Thats 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.

	http	)						
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
-	- 1	115	4.223065	192.168.1.39	128.119.245.12	HTTP	501	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
4	- 1	127	4.369699	128.119.245.12	192.168.1.39	HTTP	1127	HTTP/1.1 200 OK (text/html)
+	F	130	4.402675	192.168.1.39	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
	- 1	131	4.402870	192.168.1.39	128.119.240.90	HTTP	486	GET /~kurose/cover_5th_ed.jpg HTTP/1.1
	Ŀ	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)
	F	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)

V.

No. Time + 45 3.853899

192.168.1.39

18. Server's response to my browser's GET request is "401 Unauthorized".

HTTP

128.119.245.12

<b>⊬</b> 50	3.992541	128.119.245.12	192.168.1.39	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)				
96	17.605575	192.168.1.39	128.119.245.12	HTTP	575 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1				
95	17.745990	128.119.245.12	192.168.1.39	HTTP	583 HTTP/1.1 404 Not Found (text/html)				
> Frame	50: 771 bytes	on wire (6168 bits)	, 771 bytes captured	(6168 bits)	on interface 0				
> Ether	net II, Src: Zy	xelCom_ec:25:ca (58	:8b:f3:ec:25:ca), Ds	t: HonHaiPr	57:61:27 (90:48:9a:57:61:27)				
> Inter	net Protocol Ve	ersion 4, Src: 128.1	19.245.12, Dst: 192.	168.1.39					
> Trans	mission Control	Protocol, Src Port	: 80, Dst Port: 5413	1, Seq: 1, /	ick: 463, Len: 717				
✓ Hyper	text Transfer F	rotocol							
> HT	TP/1.1 401 Unau	thorized\r\n							
Dat	te: Mon, 16 Oct	2017 13:03:46 GMT\	r\n						
					1/2.0.10 Perl/v5.16.3\r\n				
			hark-students only"\	r\n					
	ntent-Length: 3								
		ut=5, max=100\r\n							
	nnection: Keep-								
		t/html; charset=iso	-8859-1\r\n						
\r'									
	TTP response 1/								
		st: 0.138642000 sec	onds]						
	equest in frame								
	File Data: 381 bytes								
	✓ Line-based text data: text/html								
	HTML PUBLIC "-//IETF//DTD HTML 2.0//EN" \n								
	<html><head>\n</head></html>								
	<title>401 Unauthorized</title> \n								
1</td <td>head&gt;<body>\n</body></td> <td></td> <td></td> <td></td> <td></td>	head> <body>\n</body>								

516 GET /wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html HTTP/1.1

**19.** The new field includes the authorization field because now I sent the server the username and the password along with my request stating that I was authorized to receive the page.

```
45 3.853899
50 3.992541
                    192.168.1.39
128.119.245.12
                                                                                  516 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1 771 HTTP/1.1 401 Unauthorized (text/html)
                                             128.119.245.12
                                                                      HTTP
                                             192.168.1.39
                                                                      HTTP
90 17.605575
                    192.168.1.39
                                             128.119.245.12
                                                                      HTTP
                                                                                  575 GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
                                                                                  583 HTTP/1.1 404 Not Found (text/html)
95 17,745990
                    128,119,245,12
                                             192.168.1.39
                                                                      HTTP
```

```
Frame 90: 575 bytes on wire (4600 bits), 575 bytes captured (4600 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: 54133, Dst Port: 80, Seq: 1, Ack: 1, Len: 521
Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\n
   Host: gaia.cs.umass.edu\r\n
   Connection: keep-alive\r\n
 Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\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-Encoding: gzip, deflate\r\n
   \label{eq: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/protected_pages/HTTP-wiresharkfile5.html]
   [HTTP request 1/1]
   [Response in frame: 95]
```