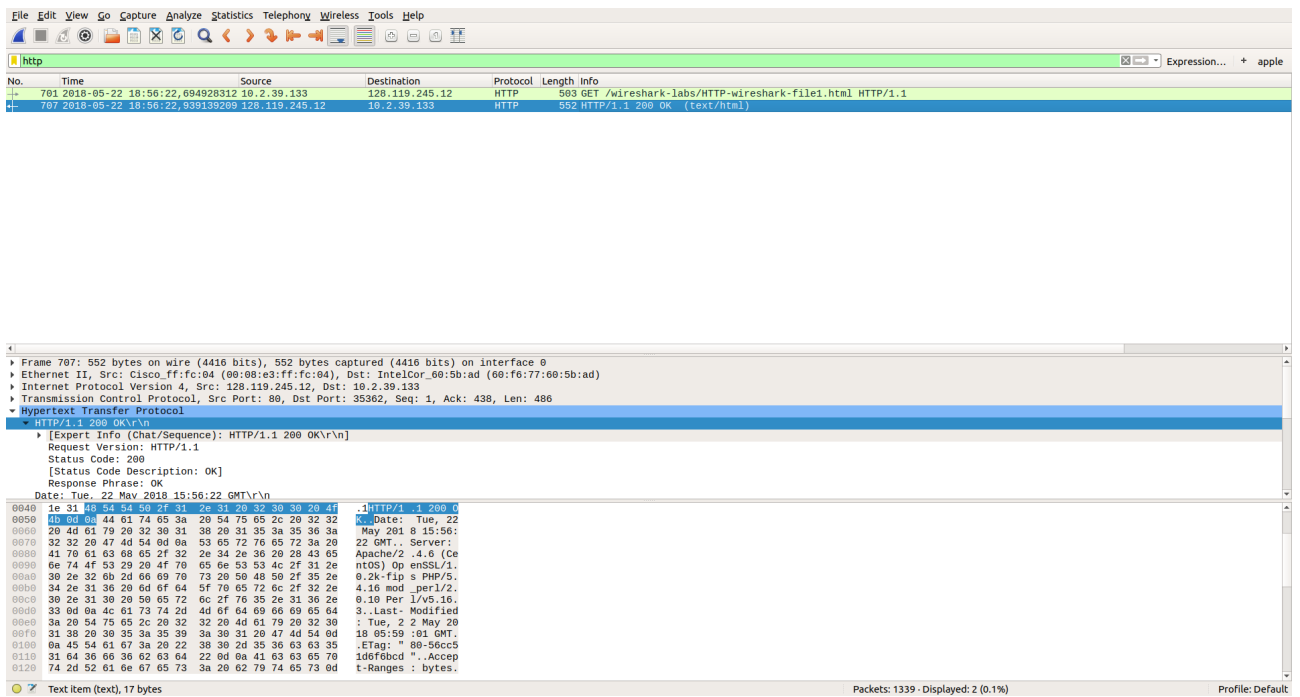
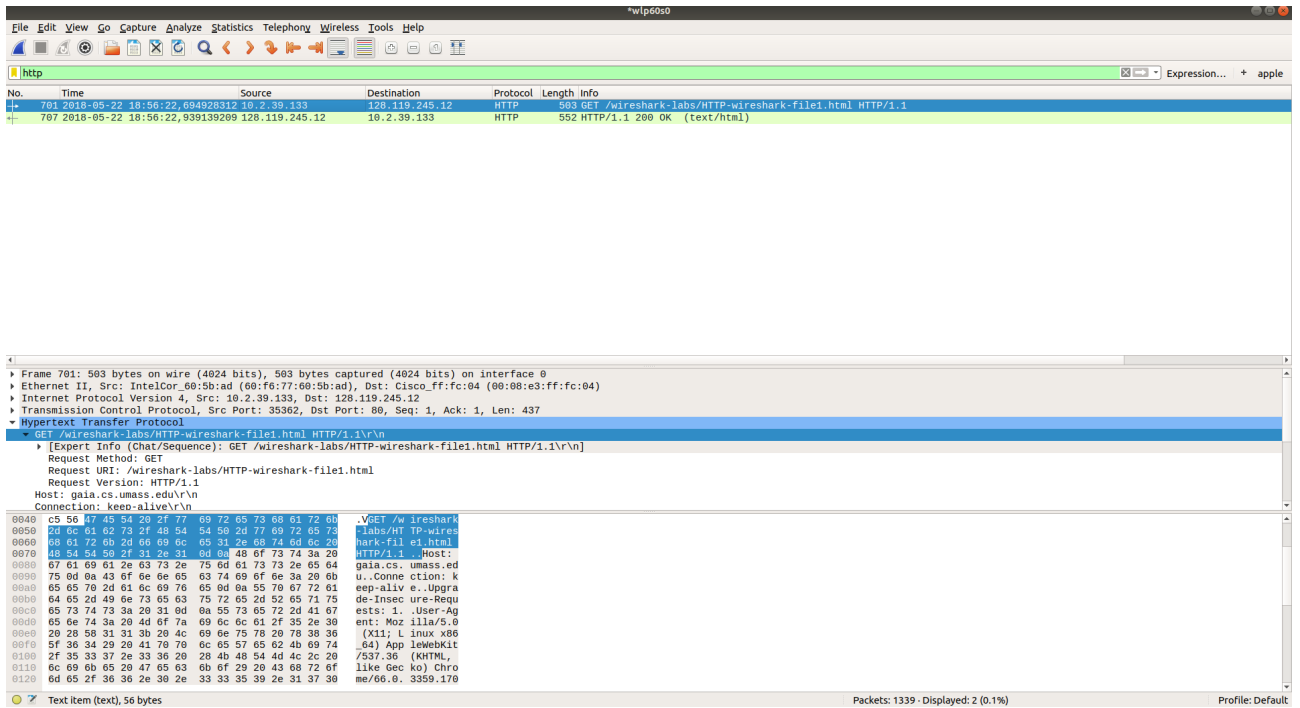


Bil 452 Hw-2

Fatih Furkan Has  
141101024



1) Yukarıdaki çıktılarda görüldüğü üzeri HTTP 1.1 versiyonu ile çalışmaktadırlar.

No.	Time	Source	Destination	Protocol	Length	Info
701	2018-05-22 18:56:22.694928312	10.2.39.133	128.119.245.12	HTTP	503	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
707	2018-05-22 18:56:22.939139209	128.119.245.12	10.2.39.133	HTTP	552	HTTP/1.1 200 OK (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 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.170 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: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n	
\r\n	
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]	
[HTTP request 1/1]	
[Response in frame: 707]	

0040	c5 56 47 45 54 20 2f 77	69 72 65 73 08 61 72 08	.VGET /w ireshark
0050	2d 0c 01 02 73 2f 48 54	54 50 2d 77 09 72 65 73	labs/HT TP-wires
0060	48 01 72 0b 2d 66 09 0c	05 31 2e 09 74 6d 65 2b	ark-fil e1.html
0070	48 54 54 50 2f 31 2e 31	0d 0a 48 0f 73 74 3a 20	HTTP/1.1 Host:
0080	07 61 69 61 2e 63 73 2e	75 0d 61 73 73 2e 65 64	gaia.cs. umass.ed
0090	75 0d 0a 43 0f 6e 6e 65	63 74 69 0f 6e 3a 29 6b	u..Conne ction: k
00a0	65 05 79 2d 61 6c 69 76	65 0d 0a 55 78 07 72 61	ee-paliv e..Upgra
00b0	64 65 2d 49 6e 73 65 63	75 72 65 2d 52 65 71 75	de-Insec ure-Requ
00c0	65 73 74 73 3a 29 31 0d	0a 55 73 65 72 2d 41 67	ests: i. .User-Ag
00d0	65 0e 74 3a 29 4d 0f 7a	69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
00e0	29 28 58 31 31 3b 20 4c	69 6e 75 78 29 78 38 36	(X11; L inux x86
00f0	5f 36 34 29 29 41 70 70	6c 05 57 65 62 4b 69 74	64) App leWebKit
0100	2f 35 33 37 2e 33 36 20	28 4b 48 54 4d 4c 2c 29	/537.36 (KHTML,
0110	6c 69 69 65 29 47 65 63	6b 6f 29 29 43 69 72 6f	like Geck ko) chro
0120	6d 65 2f 36 36 2e 30 2e	33 33 35 39 2e 31 37 30	me/66.0. 3359.170

2) Çıktıda görüldüğü gibi Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n.

3) Bilgisayarımın ip adresi: 10.2.39.133  
Server'ın ip adresi: 128.119.245.12

707	2018-05-22 18:56:22.939139209	128.119.245.12	10.2.39.133	HTTP	552	HTTP/1.1 200 OK (text/html)
-----	-------------------------------	----------------	-------------	------	-----	-----------------------------

4) Status kodu 200 olarak döndürülmüştür.

```

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Tue, 22 May 2018 15:56:22 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, 22 May 2018 05:59:01 GMT\r\n
ETag: "80-56cc51d6f6bcd"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 128\r\n

```

5) Last-Modified: Tue, 22 May 2018 05:59:01 GMT\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: 0.244210897 seconds]
```

6) 128 bytes olarak görülmektedir.

7) Herhangi bir farklılık göremedim.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows a GET request from 10.2.39.133 to 128.119.245.12, which is a 200 OK response. The packet details pane shows the request method as GET, the URI as /wireshark-labs/HTTP-wireshark-file2.html, the host as gaia.cs.umass.edu, and the user agent as Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.170 Safari/537.36. The packet bytes pane shows the raw data of the request and response, including the status bar at the bottom indicating 1183 packets displayed (0.3%).

8) İlk request’e baktığımızda “IF-MODIFIED-SINCE” gibi satır görülmemektedir.

No.	Time	Source	Destination	Protocol	Length	Info
911	2018-05-22 19:05:05	421278036 10.2.39.133	128.119.245.12	HTTP	503	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
917	2018-05-22 19:05:05	665085473 128.119.245.12	10.2.39.133	HTTP	796	HTTP/1.1 200 OK (text/html)
1025	2018-05-22 19:05:08	952787848 10.2.39.133	128.119.245.12	HTTP	615	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1026	2018-05-22 19:05:09	182291328 128.119.245.12	10.2.39.133	HTTP	305	HTTP/1.1 304 Not Modified

[Request in frame: 911]  
[Next request in frame: 1025]  
[Next response in frame: 1026]  
File Data: 371 bytes

Line-based text data: text/html  
<html>  
<html>  
Congratulation again! Now you've downloaded the file lab2-2.html. <br>  
This file's last modification date will not change. <p>  
Thus if you download this multiple times on your browser, a complete copy <br>  
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>  
field in your browser's HTTP GET request to the server.<br>  
</html>

0130 0d 0a 43 0f 0e 74 65 6e 74 2d 4c 65 6e 67 74 68  
0140 3a 20 33 37 31 6d 6a 4b 65 65 70 2d 41 6c 69 76  
0150 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 29 6d 61  
0160 78 3d 31 30 38 6d 0a 43 6f 6e 6e 65 63 74 69 6f  
0170 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 6d 0a 43  
0180 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 74 65 78  
0190 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d  
01a0 55 54 46 2d 38 6d 0a 6d 0a 6a 3c 68 74 6d 6c 3e  
01b0 0a 0a 43 0f 0e 67 72 61 74 75 6c 61 74 69 6f 6e  
01c0 73 28 61 67 61 69 6e 21 20 20 4e 6f 77 20 79 6f  
01d0 75 27 76 65 29 64 6f 77 6e 6c 6f 61 64 65 64 20

Content-Length: 371  
Keep-Alive: timeout=5, max=100  
Connection: Keep-Alive  
Content-Type: text/html; charset=UTF-8  
Congratulation again! Now you've downloaded

HTTP Content-Length header (http.content\_length\_header), 21 bytes
Packets: 1183 - Displayed: 4 (0.3%)
Profile: Default

9) Tüm içerik yukarıdaki ekran görüntüsünde görüldüğü gibi Line-based text data: text/html başlığı altında bulunmaktadır.

No.	Time	Source	Destination	Protocol	Length	Info
911	2018-05-22 19:05:05	421278036 10.2.39.133	128.119.245.12	HTTP	503	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
917	2018-05-22 19:05:05	665085473 128.119.245.12	10.2.39.133	HTTP	796	HTTP/1.1 200 OK (text/html)
1025	2018-05-22 19:05:08	952787848 10.2.39.133	128.119.245.12	HTTP	615	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1026	2018-05-22 19:05:09	182291328 128.119.245.12	10.2.39.133	HTTP	305	HTTP/1.1 304 Not Modified

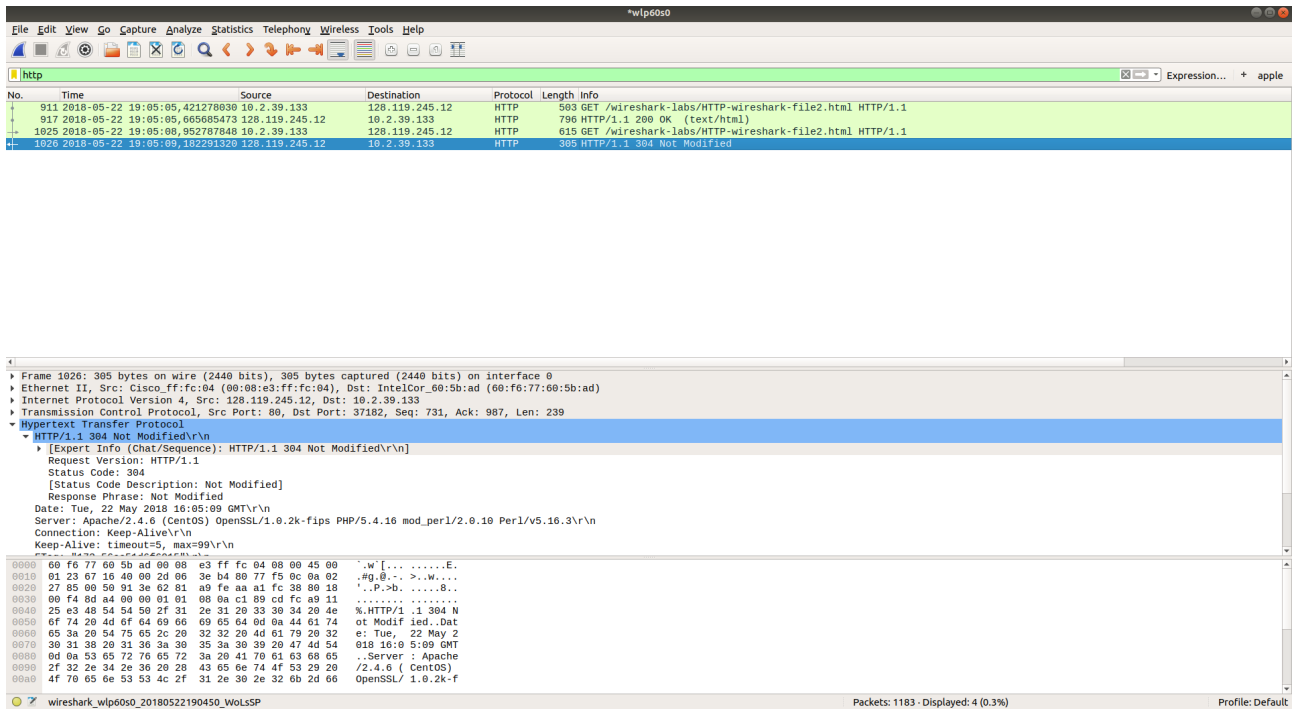
  

Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.170 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "173-56cc51d6f6015"\r\n
If-Modified-Since: Tue, 22 May 2018 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
[HTTP request 2/2]  
[Prev request in frame: 911]  
[Response in frame: 1026]

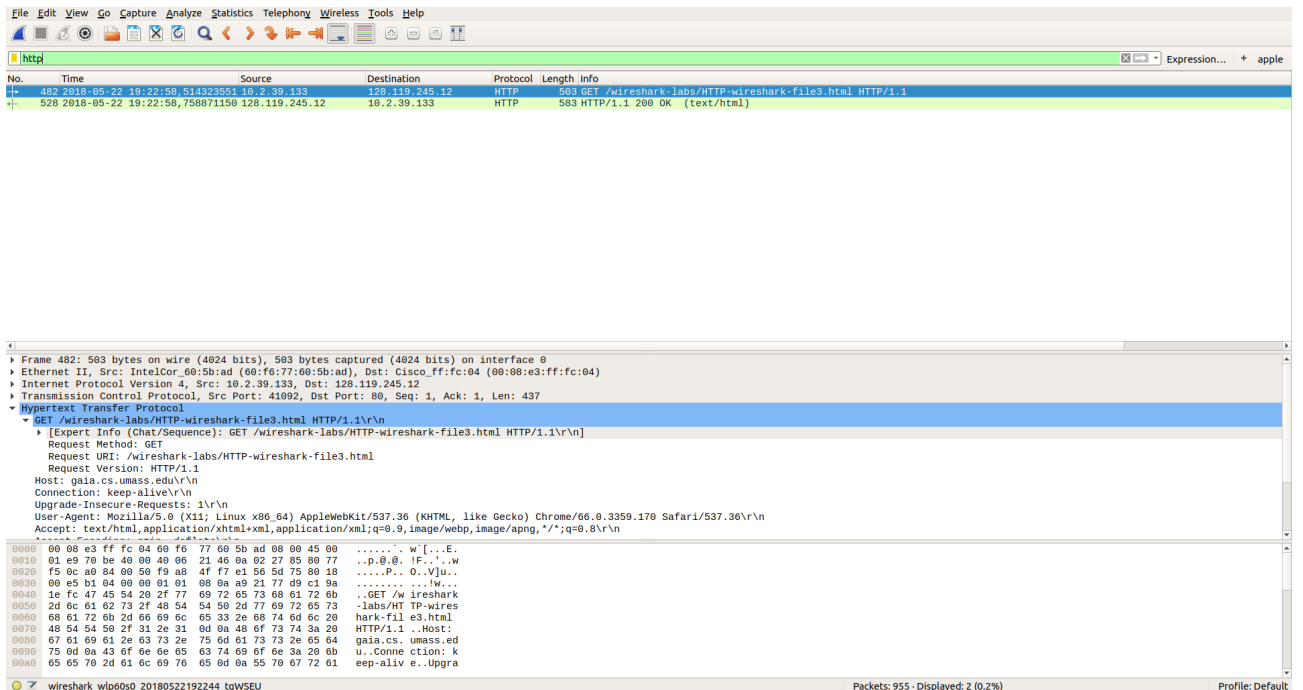
0000 00 00 e3 ff fc 04 60 f6 77 60 5b ad 08 00 45 00 .....w[...E.  
0010 02 59 df 08 40 00 40 06 b2 0b 0a 02 27 85 80 77 .Y..@. ....w  
0020 f5 0c 91 3e 00 50 aa a1 fa 13 02 81 a9 fe 80 18 ...>P.. .B.....  
0030 00 f0 88 57 00 00 01 01 08 0a a9 11 25 e3 c1 89 ..M....%...  
0040 c9 38 47 45 54 20 2f 77 69 72 05 73 68 61 72 6b .GET /w ireshark  
0050 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 72 65 73 -labs/HT TP-wires  
0060 08 61 72 6b 2d 66 69 6c 65 32 2e 68 74 6d 6c 20 hark-fil e2.html  
0070 48 54 50 2f 31 2e 31 6d 0a 4b 6f 73 74 3a 20 HTTP/1.1 .Host:  
0080 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64 gaia.cs. umass.ed  
0090 75 0d 0a 43 0f 0e 6e 65 63 74 69 6f 6e 3a 20 6b u..connec tion: k  
00a0 65 65 70 2d 61 6c 69 76 65 6d 0a 43 61 63 68 65 eep-aliv e..Cache

wireshark\_wlp60s0\_20180522190450\_WoLsSP
Packets: 1183 - Displayed: 4 (0.3%)
Profile: Default

10) İkinci request’e baktığımızda “IF-MODIFIED-SINCE” bilgisini If-Modified-Since: Tue, 22 May 2018 05:59:01 GMT\r\n şeklinde görebilmekteyiz.

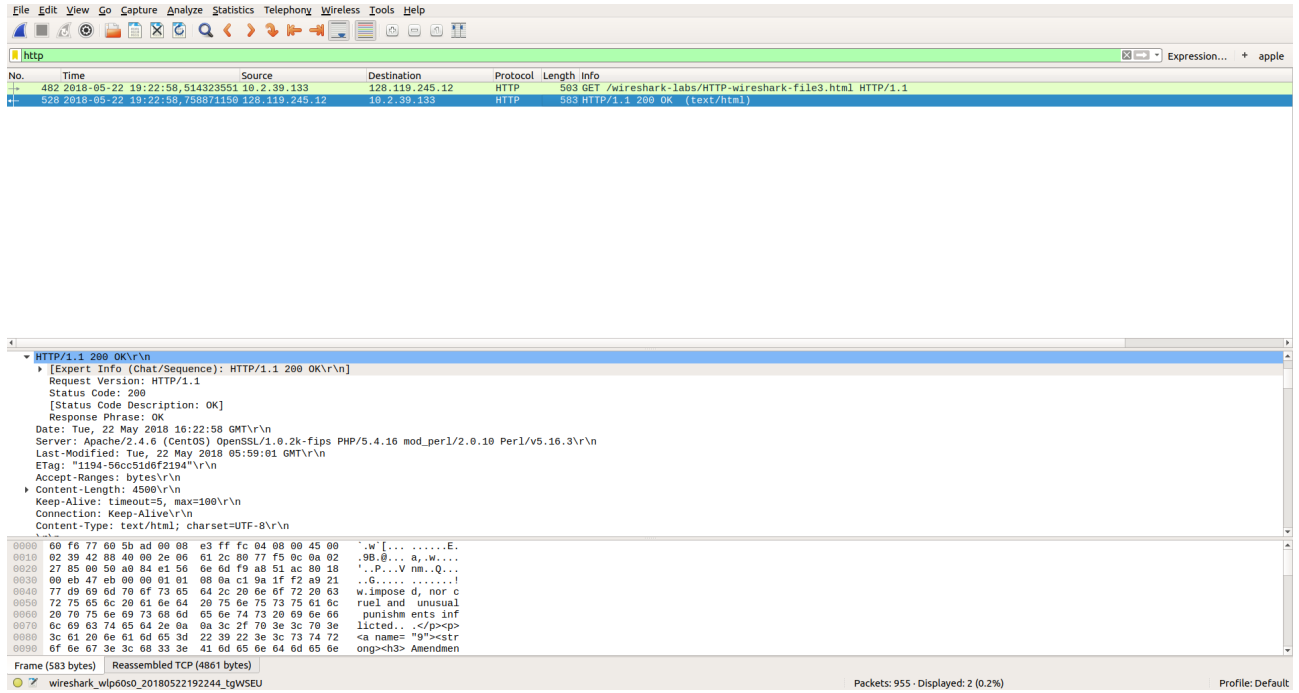


11) İkinci response’a baktığımızda 304 Not Modified cevabını görmekteyiz. Bu sebepten dolayı içeriği göremiyoruz çünkü herhangi bir değişiklik olmadığı için bilgiler cache’den alınmıştır.

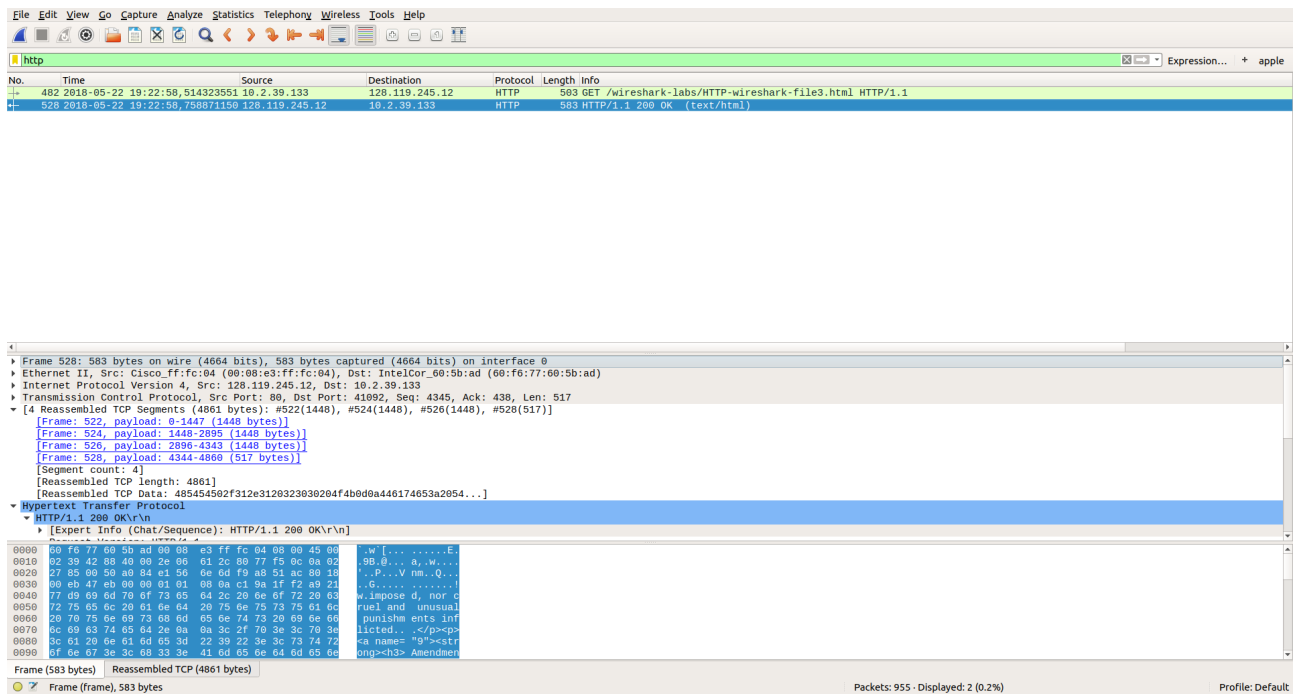


12) Bir adet GET request görebiliyoruz bunun da numarası 482’dir.

13) Bir önceki soru için eklemiş olduğum ekran görüntüsüne bakarsak eğer response için paket numarası 528’dir.



14) Status code 200’dür. Response Phrase ise OK olarak görülmektedir.



15) 4 adet TCP segment gerekmektedir.

No.	Time	Source	Destination	Protocol	Length	Info
132	19:48:44,484122296	10.2.39.133	128.119.245.12	HTTP	503	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
134	19:48:44,734463921	128.119.245.12	10.2.39.133	HTTP	1139	HTTP/1.1 200 OK (text/html)
136	19:48:44,752478798	10.2.39.133	128.119.245.12	HTTP	474	GET /pearson.png HTTP/1.1
143	19:48:45,002484732	128.119.245.12	10.2.39.133	HTTP	781	HTTP/1.1 200 OK (PNG)
148	19:48:45,276632825	10.2.39.133	128.119.240.90	HTTP	488	GET /-kurose/cover_5th_ed.jpg HTTP/1.1
150	19:48:45,521550481	128.119.240.90	10.2.39.133	HTTP	522	HTTP/1.1 302 Found (text/html)
158	19:48:45,772492369	10.2.39.133	128.119.240.90	HTTP	488	GET /-kurose/cover_5th_ed.jpg HTTP/1.1

<p>[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n]</p> <p>Request Method: GET</p> <p>Request URI: /wireshark-labs/HTTP-wireshark-file4.html</p> <p>Request Version: HTTP/1.1</p> <p>Host: gaia.cs.umass.edu\r\n</p> <p>Connection: keep-alive\r\n</p> <p>Upgrade-Insecure-Requests: 1\r\n</p> <p>User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.170 Safari/537.36\r\n</p> <p>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n</p> <p>Accept-Encoding: gzip, deflate\r\n</p> <p>Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7\r\n</p> <p>\r\n</p> <p>[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html]</p> <p>[HTTP request 1/2]</p> <p>[Response in frame: 134]</p>	<pre> 0000  00 08 e3 ff fc 04 60 f6 77 60 5b ad 08 00 45 00  ....w[...E. 0010  01 e9 20 ee 40 00 40 06 6b 16 0a 02 27 85 00 77  ..8.@.K...'W 0020  f5 0c bb fe 00 50 24 6d 03 ea 45 f5 9c b0 80 18  ....PSm..E.... 0030  00 e5 e4 e6 00 00 01 01 08 0a a9 39 0e cc c1 b1  .......9.... 0040  b5 ec 47 45 54 20 2f 77 69 72 65 73 08 01 72 6b  ..GET /w ireshark 0050  2d 6c 01 62 73 2f 48 54 54 50 2d 77 69 72 65 73  -labs/HT TP-wires 0060  68 61 72 6b 2d 66 69 6c 65 34 2e 68 74 6d 6c 20  hark-fil e4.html 0070  48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20  HTTP/1.1 ..Host: 0080  67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e 65 64  gaia.cs. umass.ed 0090  75 0d 0a 43 6f 6e 65 63 74 69 6f 6e 3a 29 6b  u..Conne ction: k 00a0  65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61  eep-aliv e..Upgra </pre>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

16) 4 adet GET request atıldı.  
İp adresleri: 128.119.245.12, 128.119.240.90

17) pearson.png için GET isteği 19:48:44,75248 de atılmış response ise 19:48:45,002484 zamanında gelmiş.  
cover\_5th\_ed.jpg için GET isteği 19:48:45,276632 de atılmış response ise 19:48:45,521550 zamanında gelmiş.  
Buradan görüyoruz ki ilk resim için cevap geldikten sonra ikinci resim için istek atılmış yani seri olarak atıldığını söyleyebiliriz.

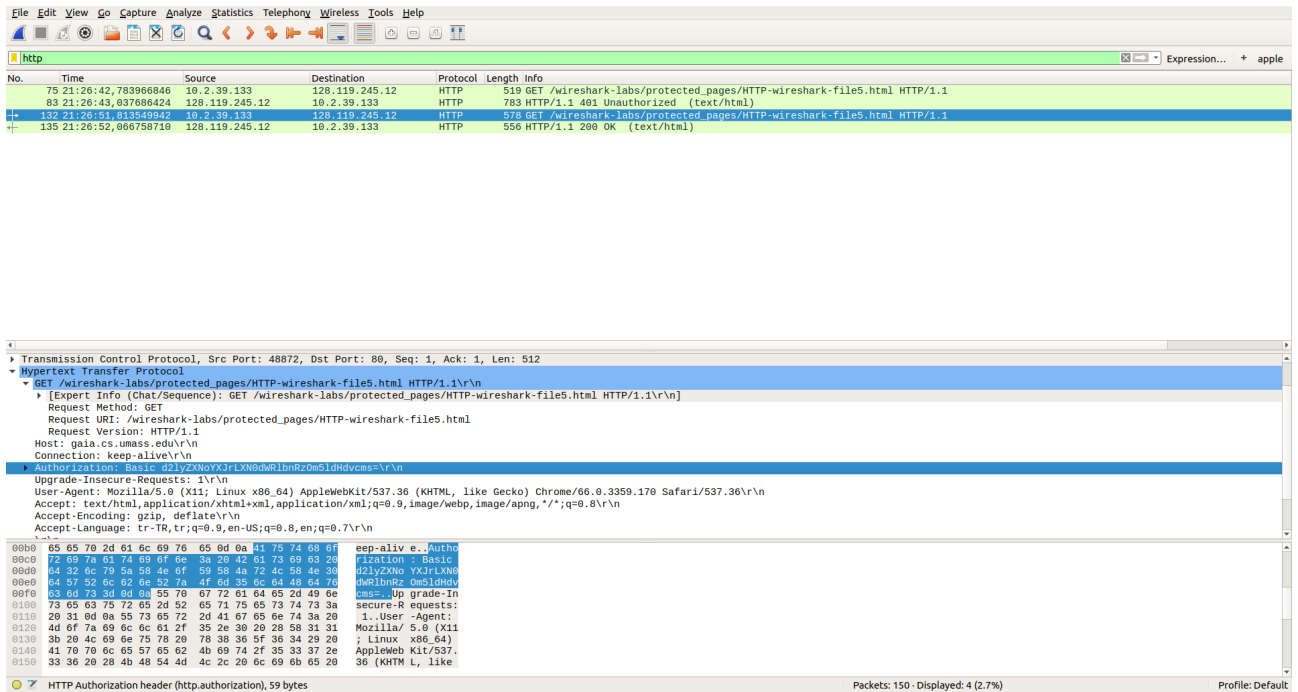


No.	Time	Source	Destination	Protocol	Length	Info
75	21:26:42,783966846	10.2.39.133	128.119.245.12	HTTP	519	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
83	21:26:43,037666424	128.119.245.12	10.2.39.133	HTTP	783	HTTP/1.1 401 Unauthorized (text/html)
132	21:26:51,813549942	10.2.39.133	128.119.245.12	HTTP	578	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
135	21:26:52,066758710	128.119.245.12	10.2.39.133	HTTP	556	HTTP/1.1 200 OK (text/html)

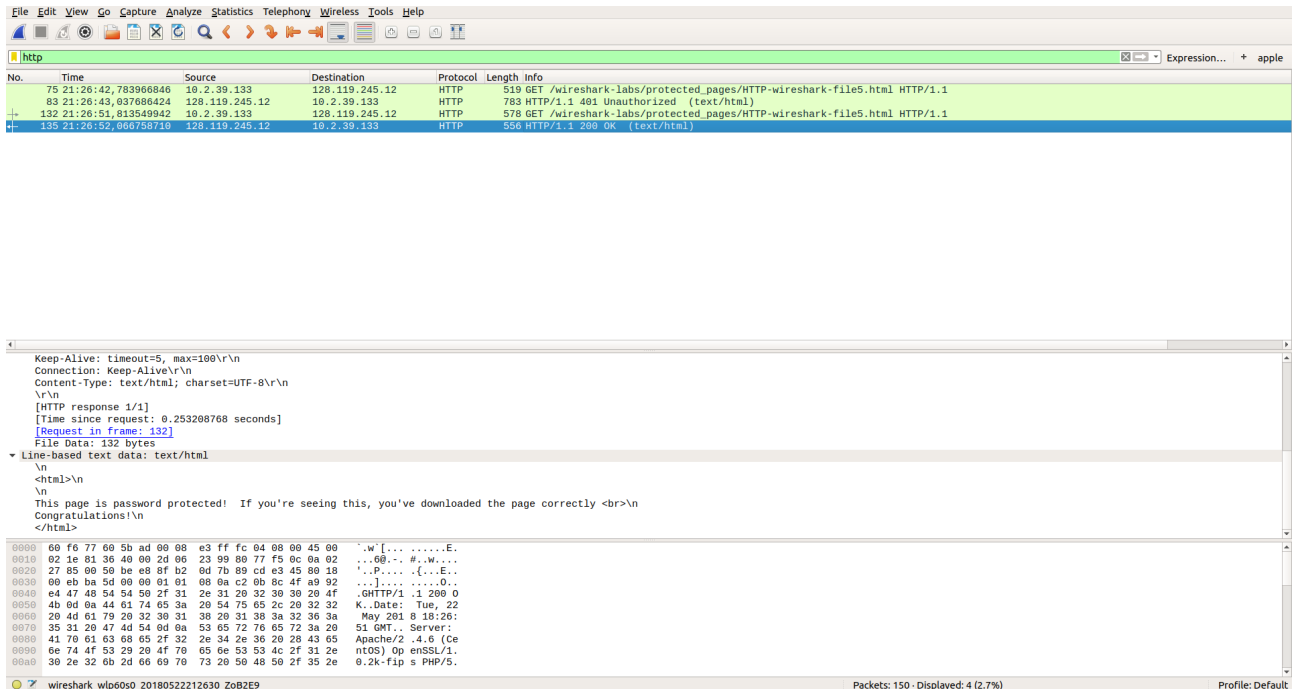
  

▼ HTTP/1.1 401 Unauthorized\r\n	
▶ [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]	
Request Version: HTTP/1.1	
Status Code: 401	
[Status Code Description: Unauthorized]	
Response Phrase: Unauthorized	
Date: Tue, 22 May 2018 18:26:42 GMT\r\n	
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_perl/2.0.10 Perl/v5.16.3\r\n	
WWW-Authenticate: Basic realm="wireshark-students only"\r\n	
Content-Length: 381\r\n	
Keep-Alive: timeout=5, max=100\r\n	
Connection: Keep-Alive\r\n	
Content-Type: text/html; charset=iso-8859-1\r\n	
\r\n	
[HTTP response 1/1]	
0000 00 f6 77 60 5b ad 00 08 e3 ff fc 04 08 00 45 00	.w[... ..E.
0010 03 01 2e 77 40 00 2d 00 75 75 00 77 f5 0e 0a 02	..w0.-. uu.W....
0020 27 85 00 50 be e2 e7 38 47 7f fd 59 fe 4a 80 18	..P...8 G..Y.J..
0030 00 eb a6 ef 00 00 01 01 08 0a c2 0b 09 0a a9 92	.....i...
0040 c1 02 40 54 54 50 2f 31 2e 31 20 34 30 31 20 55	..HTTP/1.1 401 U
0050 6e 61 75 74 68 6f 72 09 7a 65 64 0d 0a 44 61 74	authori zed..Dat
0060 65 3a 20 54 75 65 2c 20 32 32 20 4d 61 79 20 32	e: Tue, 22 May 2
0070 30 31 38 20 31 38 3a 32 36 3a 34 32 20 47 4d 54	018 18:2 6:42 GMT
0080 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65	..Server : Apache
0090 2f 32 2e 34 2e 36 20 28 43 65 6e 74 4f 53 29 20	/2.4.6 ( CentOS)
00a0 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e 32 6b 2d 66	OpenSSL/ 1.0.2k-f

18) Resimde görüldüğü gibi 401 Unauthorized cevabı gelmiştir.



19) Üstteki ekran görüntüsü görüldüğü üzere GET request te Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=\r\n olarak görülmektedir.



Bu ekran görüntüsünde ise gelen cevabı görüyoruz 200 status kodu ile gelmiştir ve Line-based text data: text/html kısmında sayfanın içeriğini görebilmekteyiz.