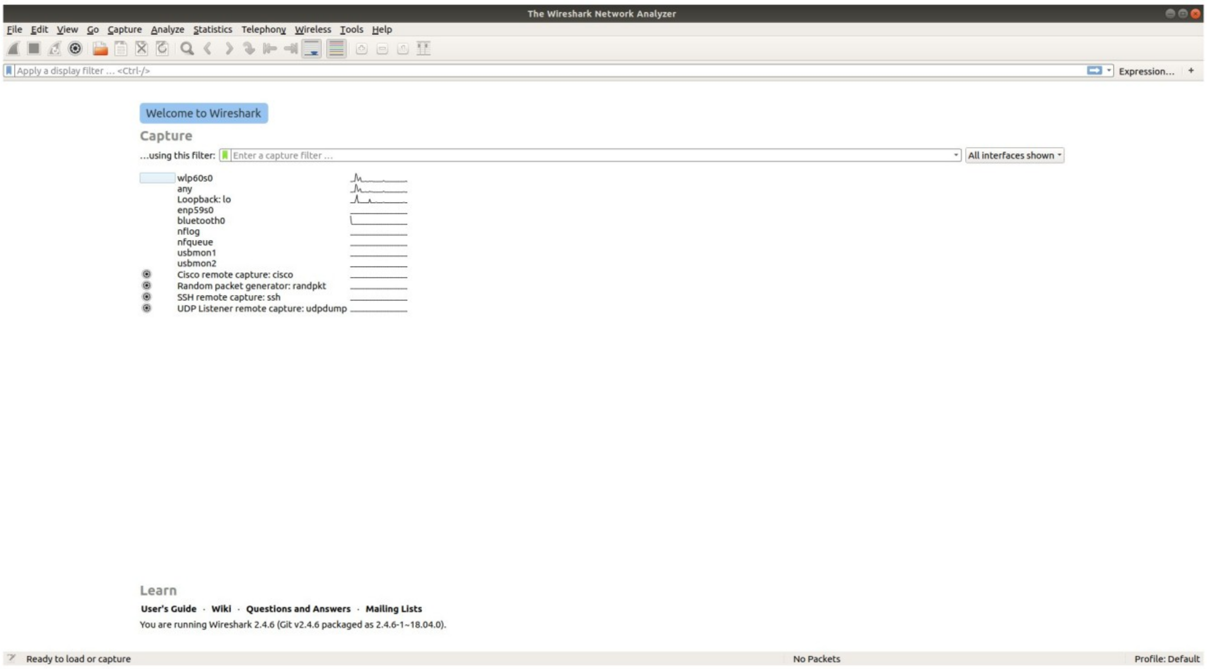
Bil-452
Ödev 1

Fatih Furkan Has
141101024


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

Welcome to Wireshark

Capture

…using this filter: Enter a capture filter … All interfaces shown

wlp60s0
any
Loopback: lo
enp59s0
bluetooth0
nflog
nfqueue
usbmon1
usbmon2
Cisco remote capture: cisco
Random packet generator: randpkt
SSH remote capture: ssh
UDP Listener remote capture: udpdump

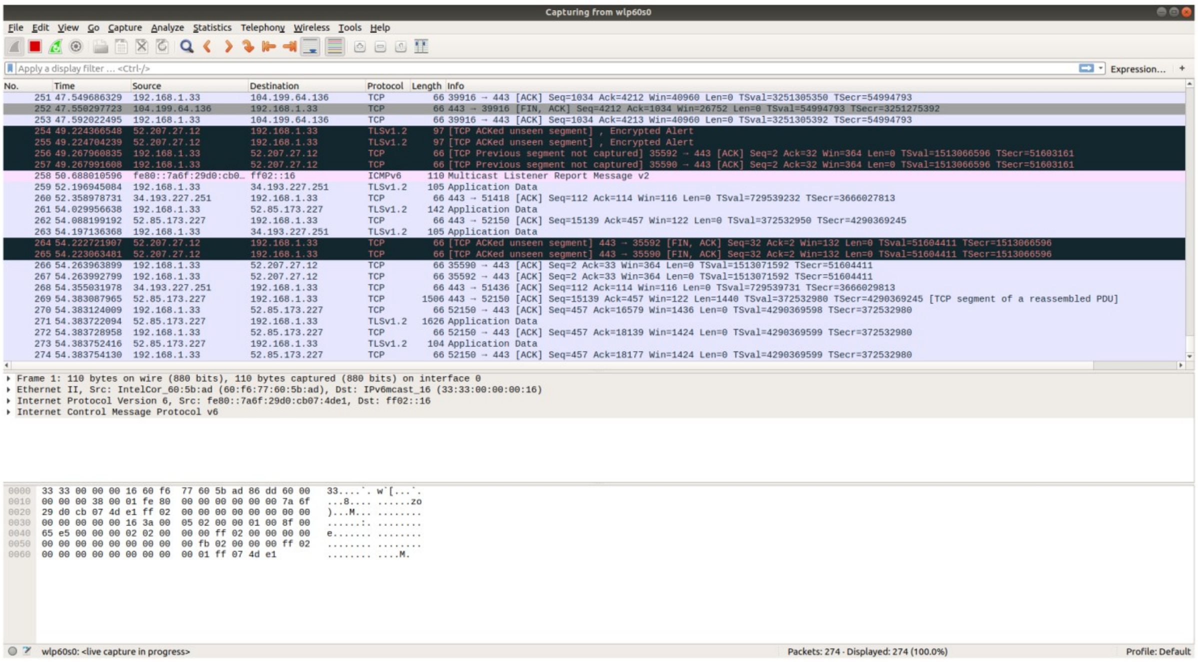
Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 2.4.6 (Git v2.4.6 packaged as 2.4.6-1~18.04.0).

Ready to load or capture
No Packets
Profile: Default

Tüm interfaceleri gördüğümüz açılış ekranı.


Capturing from wlp60s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Expression…
+

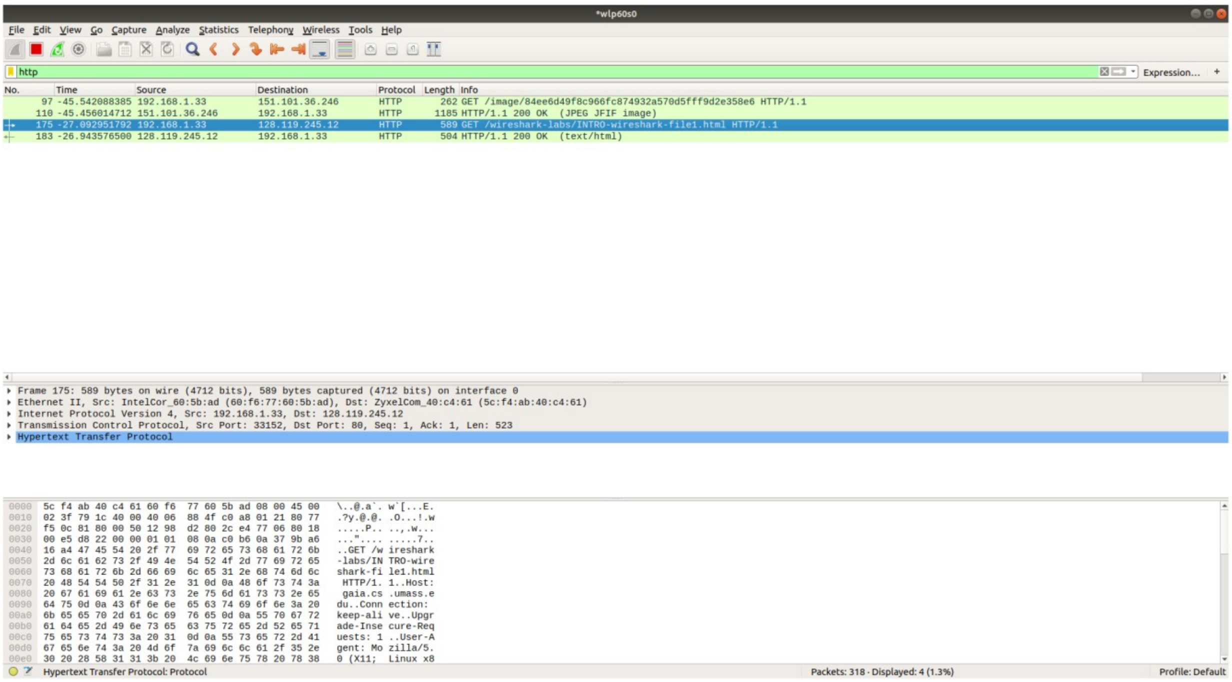
```
No.   Time          Source                 Destination      Protocol  Length Info
  251 47.549686329  192.168.1.33           104.199.64.136   TCP         66 39916 → 443 [ACK] Seq=1034 Ack=4212 Win=40960 Len=0 TSval=3251305350 TSecr=54994793
  252 47.550297723  104.199.64.136         192.168.1.33     TCP         66 443 → 39916 [FIN, ACK] Seq=4212 Ack=1034 Win=26752 Len=0 TSval=54994793 TSecr=3251275392
  253 47.592022495  192.168.1.33           104.199.64.136   TCP         66 39916 → 443 [ACK] Seq=1034 Ack=4213 Win=40960 Len=0 TSval=3251305392 TSecr=54994793
  254 49.224366548  52.207.27.12           192.168.1.33     TLSv1.2     97 [TCP ACKed unseen segment] , Encrypted Alert
  255 49.224704239  52.207.27.12           192.168.1.33     TLSv1.2     97 [TCP ACKed unseen segment] , Encrypted Alert
  256 49.267960835  192.168.1.33           52.207.27.12     TCP         66 [TCP Previous segment not captured] 35592 → 443 [ACK] Seq=2 Ack=32 Win=364 Len=0 TSval=1513066596 TSecr=51603161
  257 49.267991608  192.168.1.33           52.207.27.12     TCP         66 [TCP Previous segment not captured] 35590 → 443 [ACK] Seq=2 Ack=32 Win=364 Len=0 TSval=1513066596 TSecr=51603161
  258 50.688010596  fe80::7a6f:29d0:cb0…   ff02::16         ICMPv6     110 Multicast Listener Report Message v2
  259 52.196945084  192.168.1.33           34.193.227.251   TLSv1.2    105 Application Data
  260 52.358978731  34.193.227.251         192.168.1.33     TCP         66 443 → 51418 [ACK] Seq=112 Ack=114 Win=116 Len=0 TSval=729539232 TSecr=3666027813
  261 54.029956638  192.168.1.33           52.85.173.227    TLSv1.2    142 Application Data
  262 54.088199192  52.85.173.227          192.168.1.33     TCP         66 443 → 52150 [ACK] Seq=15139 Ack=457 Win=122 Len=0 TSval=372532950 TSecr=4290369245
  263 54.197136368  192.168.1.33           34.193.227.251   TLSv1.2    105 Application Data
  264 54.222721907  52.207.27.12           192.168.1.33     TCP         66 [TCP ACKed unseen segment] 443 → 35592 [FIN, ACK] Seq=32 Ack=2 Win=132 Len=0 TSval=51604411 TSecr=1513066596
  265 54.223063481  52.207.27.12           192.168.1.33     TCP         66 [TCP ACKed unseen segment] 443 → 35590 [FIN, ACK] Seq=32 Ack=2 Win=132 Len=0 TSval=51604411 TSecr=1513066596
  266 54.263963899  192.168.1.33           52.207.27.12     TCP         66 35590 → 443 [ACK] Seq=2 Ack=33 Win=364 Len=0 TSval=1513071592 TSecr=51604411
  267 54.263992799  192.168.1.33           52.207.27.12     TCP         66 35592 → 443 [ACK] Seq=2 Ack=33 Win=364 Len=0 TSval=1513071592 TSecr=51604411
  268 54.355031978  34.193.227.251         192.168.1.33     TCP         66 443 → 51436 [ACK] Seq=112 Ack=114 Win=116 Len=0 TSval=729539731 TSecr=3666029813
  269 54.383087965  52.85.173.227          192.168.1.33     TCP       1506 443 → 52150 [ACK] Seq=15139 Ack=457 Win=122 Len=1440 TSval=372532980 TSecr=4290369245 [TCP segment of a reassembled PDU]
  270 54.383124009  192.168.1.33           52.85.173.227    TCP         66 52150 → 443 [ACK] Seq=457 Ack=16579 Win=1436 Len=0 TSval=4290369598 TSecr=372532980
  271 54.383722094  52.85.173.227          192.168.1.33     TLSv1.2   1626 Application Data
  272 54.383728958  192.168.1.33           52.85.173.227    TCP         66 52150 → 443 [ACK] Seq=457 Ack=18139 Win=1424 Len=0 TSval=4290369599 TSecr=372532980
  273 54.383752416  52.85.173.227          192.168.1.33     TLSv1.2    104 Application Data
  274 54.383754130  192.168.1.33           52.85.173.227    TCP         66 52150 → 443 [ACK] Seq=457 Ack=18177 Win=1424 Len=0 TSval=4290369599 TSecr=372532980
```

```
▸ Frame 1: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
▸ Ethernet II, Src: IntelCor_60:5b:ad (60:f6:77:60:5b:ad), Dst: IPv6mcast_16 (33:33:00:00:00:16)
▸ Internet Protocol Version 6, Src: fe80::7a6f:29d0:cb07:4de1, Dst: ff02::16
▸ Internet Control Message Protocol v6
```

```
0000  33 33 00 00 00 16 60 f6  77 60 5b ad 86 dd 60 00   33....`. w`[...`.
0010  00 00 00 38 00 01 fe 80  00 00 00 00 00 00 7a 6f   ...8.... ......zo
0020  29 d0 cb 07 4d e1 ff 02  00 00 00 00 00 00 00 00   )...M... ........
0030  00 00 00 00 00 16 3a 00  05 02 00 00 01 00 8f 00   ......:. ........
0040  65 e5 00 00 00 02 02 00  00 00 ff 02 00 00 00 00   e....... ........
0050  00 00 00 00 00 00 00 00  00 fb 02 00 00 00 ff 02   ........ ........
0060  00 00 00 00 00 00 00 00  00 01 ff 07 4d e1         ........ ....M.
```

wlp60s0: <live capture in progress>
Packets: 274 · Displayed: 274 (100.0%)
Profile: Default

wlp60s0 için sniffing işlemimizi başlattık.



*wlp60s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

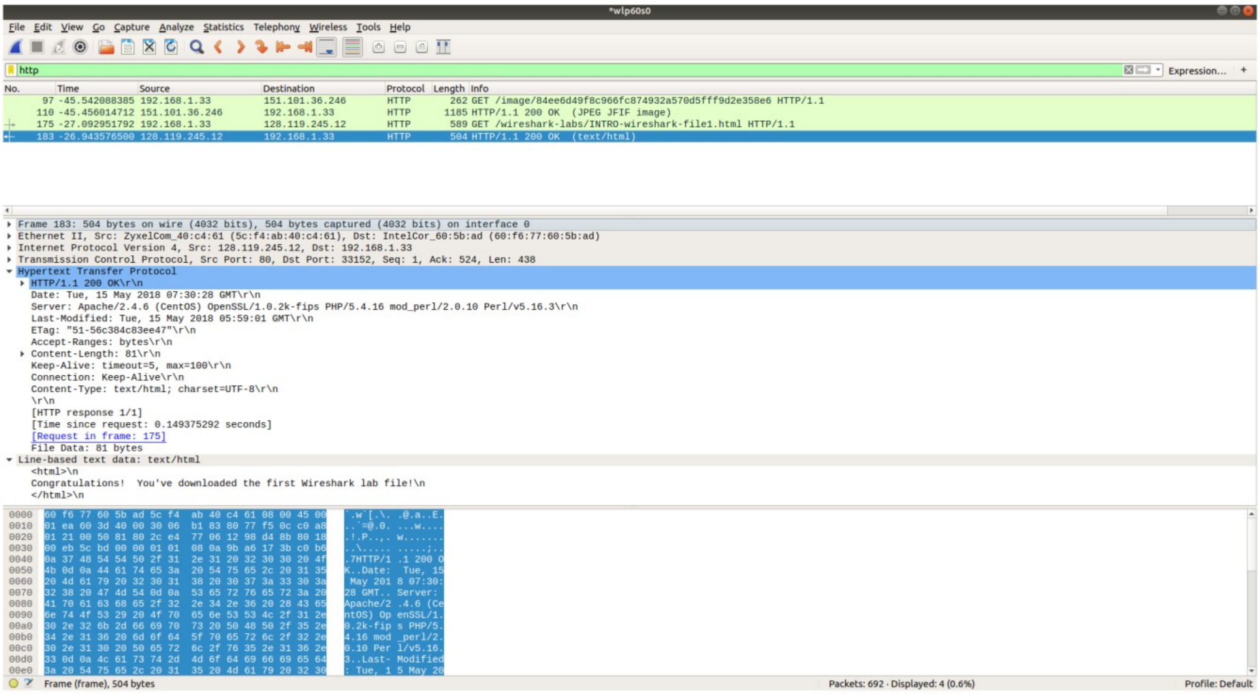
```
No.   Time          Source          Destination     Protocol Length Info
   97 -45.542088385 192.168.1.33    151.101.36.246  HTTP      262 GET /image/84ee6d49f8c966fc874932a570d5fff9d2e358e6 HTTP/1.1
  110 -45.456014712 151.101.36.246  192.168.1.33    HTTP     1185 HTTP/1.1 200 OK  (JPEG JFIF image)
  175 -27.092951792 192.168.1.33    128.119.245.12  HTTP      589 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  183 -26.943576500 128.119.245.12  192.168.1.33    HTTP      504 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 175: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface 0
▸ Ethernet II, Src: IntelCor_60:5b:ad (60:f6:77:60:5b:ad), Dst: ZyxelCom_40:c4:61 (5c:f4:ab:40:c4:61)
▸ Internet Protocol Version 4, Src: 192.168.1.33, Dst: 128.119.245.12
▸ Transmission Control Protocol, Src Port: 33152, Dst Port: 80, Seq: 1, Ack: 1, Len: 523
▸ Hypertext Transfer Protocol
```

```
0000  5c f4 ab 40 c4 61 60 f6  77 60 5b ad 08 00 45 00   \..@.a`. w`[...E.
0010  02 3f 79 1c 40 00 40 06  88 4f c0 a8 01 21 80 77   .?y.@.@. .O...!.w
0020  f5 0c 81 80 00 50 12 98  d2 80 2c e4 77 06 80 18   .....P.. ..,.w...
0030  00 e5 d8 22 00 00 01 01  08 0a c0 b6 0a 37 9b a6   ...".... .....7..
0040  16 a4 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ..GET /w ireshark
0050  2d 6c 61 62 73 2f 49 4e  54 52 4f 2d 77 69 72 65   -labs/IN TRO-wire
0060  73 68 61 72 6b 2d 66 69  6c 65 31 2e 68 74 6d 6c   shark-fi le1.html
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0080  20 67 61 69 61 2e 63 73  2e 75 6d 61 73 73 2e 65    gaia.cs .umass.e
0090  64 75 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20   du..Conn ection:
00a0  6b 65 65 70 2d 61 6c 69  76 65 0d 0a 55 70 67 72   keep-ali ve..Upgr
00b0  61 64 65 2d 49 6e 73 65  63 75 72 65 2d 52 65 71   ade-Inse cure-Req
00c0  75 65 73 74 73 3a 20 31  0d 0a 55 73 65 72 2d 41   uests: 1 ..User-A
00d0  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
00e0  30 20 28 58 31 31 3b 20  4c 69 6e 75 78 20 78 38   0 (X11;  Linux x8
```

Hypertext Transfer Protocol: Protocol   Packets: 318 · Displayed: 4 (1.3%)   Profile: Default

http filtreleme yaptığımızda http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html adresine atmış olduğumuz get request’i görebiliyoruz.



*wlp60s0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression…
+

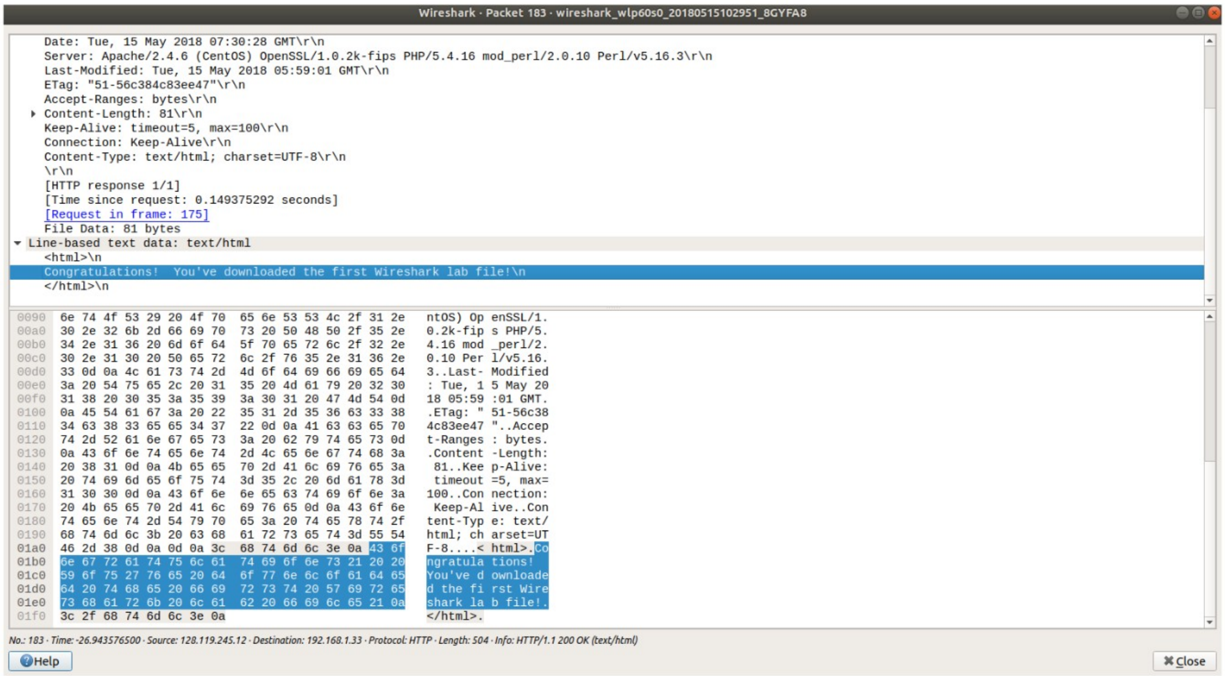
```
No.   Time          Source          Destination     Protocol Length Info
   97 -45.542088385 192.168.1.33    151.101.36.246  HTTP      262 GET /image/84ee6d49f8c966fc874932a570d5fff9d2e358e6 HTTP/1.1
  110 -45.456014712 151.101.36.246  192.168.1.33    HTTP     1185 HTTP/1.1 200 OK  (JPEG JFIF image)
  175 -27.092951792 192.168.1.33    128.119.245.12  HTTP      589 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  183 -26.943576500 128.119.245.12  192.168.1.33    HTTP      504 HTTP/1.1 200 OK  (text/html)
```

```
▸ Frame 183: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface 0
▸ Ethernet II, Src: ZyxelCom_40:c4:61 (5c:f4:ab:40:c4:61), Dst: IntelCor_60:5b:ad (60:f6:77:60:5b:ad)
▸ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.33
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 33152, Seq: 1, Ack: 524, Len: 438
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Tue, 15 May 2018 07:30:28 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 May 2018 05:59:01 GMT\r\n
    ETag: "51-56c384c83ee47"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 81\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: 0.149375292 seconds]
    [Request in frame: 175]
    File Data: 81 bytes
▾ Line-based text data: text/html
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

```
0000  60 f6 77 60 5b ad 5c f4  ab 40 c4 61 08 00 45 00   `.w`[.\. .@.a..E.
0010  01 ea 60 3d 40 00 30 06  b1 83 80 77 f5 0c c0 a8   ..`=@.0. ...w....
0020  01 21 00 50 81 80 2c e4  77 06 12 98 d4 8b 80 18   .!.P..,. w.......
0030  00 eb 5c bd 00 00 01 01  08 0a 9b a6 17 3b c0 b6   ..\..... .....;..
0040  0a 37 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   .7HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 54 75 65 2c 20 31 35   K..Date:  Tue, 15
0060  20 4d 61 79 20 32 30 31  38 20 30 37 3a 33 30 3a    May 201 8 07:30:
0070  32 38 20 47 4d 54 0d 0a  53 65 72 76 65 72 3a 20   28 GMT.. Server: 
0080  41 70 61 63 68 65 2f 32  2e 34 2e 36 20 28 43 65   Apache/2 .4.6 (Ce
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-fip s PHP/5.
00b0  34 2e 31 36 20 6d 6f 64  5f 70 65 72 6c 2f 32 2e   4.16 mod _perl/2.
00c0  30 2e 31 30 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.10 Per l/v5.16.
00d0  33 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   3..Last- Modified
00e0  3a 20 54 75 65 2c 20 31  35 20 4d 61 79 20 32 30   : Tue, 1 5 May 20
```

Frame (frame), 504 bytes   Packets: 692 · Displayed: 4 (0.6%)   Profile: Default

Göndermiş olduğumz get request’ine karşılık bize döndürülen cevap yukarıda şekildedir.



Wireshark · Packet 183 · wireshark_wlp60s0_20180515102951_8GYFA8

```
    Date: Tue, 15 May 2018 07:30:28 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 May 2018 05:59:01 GMT\r\n
    ETag: "51-56c384c83ee47"\r\n
    Accept-Ranges: bytes\r\n
  ▸ Content-Length: 81\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: 0.149375292 seconds]
    [Request in frame: 175]
    File Data: 81 bytes
▾ Line-based text data: text/html
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```

```
0090  6e 74 4f 53 29 20 4f 70  65 6e 53 53 4c 2f 31 2e   ntOS) Op enSSL/1.
00a0  30 2e 32 6b 2d 66 69 70  73 20 50 48 50 2f 35 2e   0.2k-fip s PHP/5.
00b0  34 2e 31 36 20 6d 6f 64  5f 70 65 72 6c 2f 32 2e   4.16 mod _perl/2.
00c0  30 2e 31 30 20 50 65 72  6c 2f 76 35 2e 31 36 2e   0.10 Per l/v5.16.
00d0  33 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   3..Last- Modified
00e0  3a 20 54 75 65 2c 20 31  35 20 4d 61 79 20 32 30   : Tue, 1 5 May 20
00f0  31 38 20 30 35 3a 35 39  3a 30 31 20 47 4d 54 0d   18 05:59 :01 GMT.
0100  0a 45 54 61 67 3a 20 22  35 31 2d 35 36 63 33 38   .ETag: " 51-56c38
0110  34 63 38 33 65 65 34 37  22 0d 0a 41 63 63 65 70   4c83ee47 "..Accep
0120  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes.
0130  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   .Content -Length:
0140  20 38 31 0d 0a 4b 65 65  70 2d 41 6c 69 76 65 3a    81..Kee p-Alive:
0150  20 74 69 6d 65 6f 75 74  3d 35 2c 20 6d 61 78 3d    timeout =5, max=
0160  31 30 30 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   100..Con nection:
0170  20 4b 65 65 70 2d 41 6c  69 76 65 0d 0a 43 6f 6e    Keep-Al ive..Con
0180  74 65 6e 74 2d 54 79 70  65 3a 20 74 65 78 74 2f   tent-Typ e: text/
0190  68 74 6d 6c 3b 20 63 68  61 72 73 65 74 3d 55 54   html; ch arset=UT
01a0  46 2d 38 0d 0a 0d 0a 3c  68 74 6d 6c 3e 0a 43 6f   F-8....< html>.Co
01b0  6e 67 72 61 74 75 6c 61  74 69 6f 6e 73 21 20 20   ngratula tions!  
01c0  59 6f 75 27 76 65 20 64  6f 77 6e 6c 6f 61 64 65   You've d ownloade
01d0  64 20 74 68 65 20 66 69  72 73 74 20 57 69 72 65   d the fi rst Wire
01e0  73 68 61 72 6b 20 6c 61  62 20 66 69 6c 65 21 0a   shark la b file!.
01f0  3c 2f 68 74 6d 6c 3e 0a                            </html>.
```

No.: 183 · Time: -26.943576500 · Source: 128.119.245.12 · Destination: 192.168.1.33 · Protocol: HTTP · Length: 504 · Info: HTTP/1.1 200 OK (text/html)

Bu response’u incelersek eğer siteye bağlandığımızda karşımıza gelen mesajın içeriğini de yukarıdaki şekilde görebildik.

Soru 1:

- -TCP
- -SSDP
- -TLSv1.2
- -DNS
- -QUIC

Soru 2:

Yaklaşık olarak 0.14 saniye sürmüştür.

Soru 3:

wwwnet.cs.umass.edu ip adresi: 128.119.245.12
kendi ip adresim: 192.168.1.35

Soru 4:

GET:

```
34 2018-05-15 11:24:56,062973823 192.168.1.35
128.119.245.12
HTTP
589
GET /
wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 34: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface
0
Ethernet II, Src: IntelCor_60:5b:ad (60:f6:77:60:5b:ad), Dst: ZyxelCom_40:c4:61 (
5c:f4:ab:40:c4:61)
Internet Protocol Version 4, Src: 192.168.1.35, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60568, Dst Port: 80, Seq: 1, Ack: 1, Len:
523
Hypertext Transfer Protocol
GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
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
If-None-Match: "51-56c384c83ee47"\r\n
If-Modified-Since: Tue, 15 May 2018 05:59:01 GMT\r\n
\r\n
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-
file1.html]
[HTTP request 1/2]
[Response in frame: 38]
[Next request in frame: 52]
```

OK:

```
572 2018-05-15 11:26:36,278146115 128.119.245.12
192.168.1.35
HTTP
197
HTTP/1.1
200 OK (text/html)
Frame 572: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface 0
Ethernet II, Src: ZyxelCom_40:c4:61 (5c:f4:ab:40:c4:61), Dst: IntelCor_60:5b:ad (60:f6:77:60:5b:ad)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.35
Transmission Control Protocol, Src Port: 80, Dst Port: 60576, Seq: 2881, Ack: 395, Len: 131
[3 Reassembled TCP Segments (3011 bytes): #568(1440), #570(1440), #572(131)]
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Date: Tue, 15 May 2018 08:26:36 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, 01 Mar 2016 18:57:50 GMT\r\n
ETag: "a5b-52d015789ee9e"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 2651\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 1/3]
[Time since request: 0.149504772 seconds]
[Request in frame: 564]
[Next request in frame: 574]
[Next response in frame: 619]
File Data: 2651 bytes
Line-based text data: text/html
```