

1. ① nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız.
- a. Tarayıcınız HTTP 1.0 veya HTTP 1.1 sürümlerinden hangisini kullanmaktadır?
Belirtildiği gibi tarayıcı HTTP/1.1 sürümünü kullanmaktadır.

No.	Time	Source	Destination	Protocol	Length	Info
696	16.606794	192.168.183.52	2.19.196.90	HTTP	409	HEAD /filestreamingservice/files
699	16.675462	2.19.196.90	192.168.183.52	HTTP	656	HTTP/1.1 200 OK
703	16.709903	192.168.183.52	2.19.196.90	HTTP	481	GET /filestreamingservice/files
705	16.776195	2.19.196.90	192.168.183.52	HTTP	435	HTTP/1.1 206 Partial Content
802	22.034491	192.168.183.52	2.19.196.90	HTTP	484	GET /filestreamingservice/files

- b. Bilgisayarınızın IP adresi nedir?

IP adresi bilgisine sarıyla belirtilen "Source" bilgisinden ulaşabiliriz.

IP adresi: 192.168.183.52

- c. wireshark.grydeske.net sunucusunun IP adresi nedir?

Sunucunun IP adresine yeşille belirtilen "Destination" bilgisinden ulaşabiliriz.

IP adresi: 2.19.196.90

No.	Time	Source	Destination	Protocol	Length	Info
703	16.709903	192.168.183.52	2.19.196.90	HTTP	481	GET /filestreamingservice/files
802	22.034491	192.168.183.52	2.19.196.90	HTTP	484	GET /filestreamingservice/files
809	23.271824	192.168.183.52	2.19.196.90	HTTP	484	GET /filestreamingservice/files
816	24.349843	192.168.183.52	2.19.196.90	HTTP	485	GET /filestreamingservice/files
830	25.438374	192.168.183.52	2.19.196.90	HTTP	486	GET /filestreamingservice/files
843	26.529645	192.168.183.52	2.19.196.90	HTTP	486	GET /filestreamingservice/files
885	28.897902	192.168.183.52	2.19.196.90	HTTP	464	GET /filestreamingservice/files

- d. Sunucuya gönderilen ilk GET isteği ile bu isteğe verilen cevap bilgileri hangi paketlerde görülmektedir?

Sunucuya gönderilen GET isteklerini filtrelemek için filtreleme çubuğuna

"http.request.method==GET" yazdık ve ilk GET isteği 703 numaralı pakettir. Bu isteğe cevap verilen pakete [Response in frame] bilgisinden ulaşırız. → 705 numaralı paket

No.	Time	Host	Full request URI	HTTP request	Prev request in frame	Response in frame	Next request in frame
703	16.709903	msedge.b.tlu.dl.delivery.mp.microsoft.com	http://msedge.b.tlu.d	2/9	696	705	802

e. Sunucudan tarayıcınıza kaç byte boyutunda içerik gönderilmiştir?

Bu bilgiye seçilen paketin üstüne tıkladığımızda “Hypertext Transfer Protocol” sekmesinin altında yer alan Content- Length sekmesinde görebiliriz.

http.response.code==200						
No.	Time	Source	Destination	Protocol	Length	Info
699	16.675462	2.19.196.90	192.168.183.52	HTTP	656	HTTP/1.1 200 OK
883	28.875468	2.19.196.90	192.168.183.52	HTTP	655	HTTP/1.1 200 OK
888	28.976573	2.19.196.90	192.168.183.52	HTTP	819	HTTP/1.1 200 OK (application/x-chrome-extension)

> Frame 699: 656 bytes on wire (524)	> Frame 883: 655 bytes on wire (524)	> Frame 888: 819 bytes on wire (65
> Ethernet II, Src: 92:2e:4b:d8:92:	> Ethernet II, Src: 92:2e:4b:d8:92:	> Ethernet II, Src: 92:2e:4b:d8:92:
> Internet Protocol Version 4, Src:	> Internet Protocol Version 4, Src:	> Internet Protocol Version 4, Src:
> Transmission Control Protocol, Sr	> Transmission Control Protocol, Sr	> Transmission Control Protocol, S
✓ Hypertext Transfer Protocol	✓ Hypertext Transfer Protocol	✓ Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n	> HTTP/1.1 200 OK\r\n	> HTTP/1.1 200 OK\r\n
Accept-Ranges: bytes\r\n	Accept-Ranges: bytes\r\n	Accept-Ranges: bytes\r\n
Cache-Control: public, max-age:	Cache-Control: public, max-age:	Cache-Control: public, max-age:
Content-Type: application/x-ch	Content-Type: application/x-ch	Content-Type: application/x-cl
ETag: "5ZykTkExEo5IRCnDVU6TjHq	ETag: "92E7uYNtT159Zrps3Nj6DLk	ETag: "92E7uYNtT159Zrps3Nj6DLI
Last-Modified: Sat, 06 Apr 2024	Last-Modified: Fri, 05 Apr 202	Last-Modified: Fri, 05 Apr 20:
MS-CorrelationId: d243a602-ac6	MS-CorrelationId: ba7d0e5c-22f	MS-CorrelationId: ba7d0e5c-22:
MS-CV: owc28wILH02Ert1Z.0\r\n	MS-CV: jDJ6BdkdUkKdXHZ2.0\r\n	MS-CV: jDJ6BdkdUkKdXHZ2.0\r\n
MS-RequestId: ed5aa5a8-9086-4a	MS-RequestId: aaa8c5b1-58e1-48	MS-RequestId: aaa8c5b1-58e1-4:
Server: ECAcc (sac/255A)\r\n	Server: ECAcc (mic/9A98)\r\n	Server: ECAcc (mic/9A98)\r\n
X-AspNet-Version: 4.0.30319\r\	X-AspNet-Version: 4.0.30319\r\	X-AspNet-Version: 4.0.30319\r\
X-AspNetMvc-Version: 5.3\r\n	X-AspNetMvc-Version: 5.3\r\n	X-AspNetMvc-Version: 5.3\r\n
X-Powered-By: ASP.NET\r\n	X-Powered-By: ASP.NET\r\n	X-Powered-By: ASP.NET\r\n
X-Powered-By: ARR/3.0\r\n	X-Powered-By: ARR/3.0\r\n	X-Powered-By: ARR/3.0\r\n
X-Powered-By: ASP.NET\r\n	X-Powered-By: ASP.NET\r\n	X-Powered-By: ASP.NET\r\n
> Content-Length: 40795\r\n	> Content-Length: 8552\r\n	> Content-Length: 8552\r\n

Toplam Content – Length: 40795+8552+8552= 57 899

2. ② nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız.

a. Tarayıcınız sunucuya kaç tane GET isteği göndermiştir? → 1 tane

Aynı zamanda Wireshark programında sunucuya gönderilen GET isteklerini görebilmek için *İstatistikler* kısmında bulunan “HTTP” protokolüne tıklayıp “Paket Sayacı” kısmından da bu bilgiye ulaşabiliriz.

http.request.method==GET						
No.	Time	Source	Destination	Protocol	Length	Info
1137	25.570559	192.168.67.52	195.175.176.113	HTTP	340	GET /msdownload/update/v3/st

b. Sunucunun ilk GET isteğine gönderdiği cevap nedir?

→ Yakalanan ilk GET isteği 1137 numaralı pakettir. Bu pakete gelen mesaj, [Response in frame]’den veya görselde oklarla görüldüğü gibi 1139 numaralı pakettir. Yanıt, bir **304 Not Modified** durumuyla gelmiştir. Bu, istemcinin belirtilen kaynağın son değiştirilme tarihinden beri değişmediğini belirtir.

No.	Time	Source	Destination	Protocol	Length	Info
1137	25.570559	192.168.67.52	195.175.176.113	HTTP	340	GET /msdownload/update/v3/s
1139	25.644066	195.175.176.113	192.168.67.52	HTTP	320	HTTP/1.1 304 Not Modified

> Frame 1139: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface \Device\NPF_{FD1E268B-DAC3-41E2-8000-000000000000} on Ethernet II, Src: 1e:26:8a:8a:ee:3b (1e:26:8a:8a:ee:3b), Dst: Intel_13:37:56 (38:87:d5:13:37:56)

> Internet Protocol Version 4, Src: 195.175.176.113, Dst: 192.168.67.52

> Transmission Control Protocol, Src Port: 80, Dst Port: 60108, Seq: 1, Ack: 287, Len: 266

▼ 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

Content-Type: application/vnd.ms-cab-compressed\r\n

Last-Modified: Tue, 26 Sep 2023 18:01:51 GMT\r\n

ETag: "746787a3f0d91:0"\r\n

Cache-Control: public,max-age=900\r\n

Date: Sat, 06 Apr 2024 12:03:40 GMT\r\n

Connection: keep-alive\r\n

X-CCC: TR\r\n

X-CID: 2\r\n

\r\n

[HTTP response 1/1]

[Time since request: 0.073507000 seconds]

[Request in frame: 1137]

[Request URI: http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?41683a4]

3. ③ nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız.
- a. Tarayıcınız sunucuya kaç tane GET isteği göndermiştir? GET istekleri hangi internet adresine gönderilmiştir? → 3 tane yakalanmıştır.
- GET istekleri 54.247.69.169 IP adresli internet sitesine gönderilmiştir.

No.	Time	Source	Destination	Protocol	Length	Info
111	7.122500	192.168.67.52	54.247.69.169	HTTP	559	GET /file4.html HTTP/1.1
195	7.668303	192.168.67.52	54.247.69.169	HTTP	513	GET /images/SDU.png HTTP/1.1
196	7.668461	192.168.67.52	54.247.69.169	HTTP	515	GET /images/dave.jpeg HTTP/1.1

- Birinci yakalanan paket (111) için: [Full request URI: <http://wireshark.grydeske.net/file4.html>]

> Frame 111: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{FD1E268B-DAC3-41E2-8000-000000000000} on Ethernet II, Src: Intel_13:37:56 (38:87:d5:13:37:56), Dst: 1e:26:8a:8a:ee:3b (1e:26:8a:8a:ee:3b)

> Internet Protocol Version 4, Src: 192.168.67.52, Dst: 54.247.69.169

> Transmission Control Protocol, Src Port: 60179, Dst Port: 80, Seq: 1, Ack: 1, Len: 505

▼ Hypertext Transfer Protocol

> GET /file4.html HTTP/1.1\r\n

Host: wireshark.grydeske.net\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/119.0.0.0 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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,de;q=0.6,ckb;q=0.5,ay;q=0.4,ku;q=0.3\r\n

\r\n

[Full request URI: <http://wireshark.grydeske.net/file4.html>]

[HTTP request 1/2]

[Response in frame: 154]

[Next request in frame: 195]

- İkinci yakalanan paket (195) için: [Full request URI: <http://wireshark.grydeske.net/images/SDU.png>]

```
> Frame 195: 513 bytes on wire (4104 bits), 513 bytes captured (4104 bits) on interface \Device\NPF_{FD1E2
> Ethernet II, Src: Intel_13:37:56 (38:87:d5:13:37:56), Dst: 1e:26:8a:8a:ee:3b (1e:26:8a:8a:ee:3b)
> Internet Protocol Version 4, Src: 192.168.67.52, Dst: 54.247.69.169
> Transmission Control Protocol, Src Port: 60179, Dst Port: 80, Seq: 506, Ack: 1354, Len: 459
▼ Hypertext Transfer Protocol
  > GET /images/SDU.png HTTP/1.1\r\n
    Host: wireshark.grydeske.net\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/1
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://wireshark.grydeske.net/file4.html\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,de;q=0.6,ckb;q=0.5,ay;q=0.4,ku;q=0.3\r\n
    \r\n
    [Full request URI: http://wireshark.grydeske.net/images/SDU.png]
    [HTTP request 2/2]
    [Prev request in frame: 111]
    [Response in frame: 206]
```

- Üçüncü yakalanan paket (196) için: [Full request URI: <http://wireshark.grydeske.net/images/dave.jpeg>]

```
> Frame 196: 515 bytes on wire (4120 bits), 515 bytes captured (4120 bits) on interface \Device\NPF_{FD1E2
> Ethernet II, Src: Intel_13:37:56 (38:87:d5:13:37:56), Dst: 1e:26:8a:8a:ee:3b (1e:26:8a:8a:ee:3b)
> Internet Protocol Version 4, Src: 192.168.67.52, Dst: 54.247.69.169
> Transmission Control Protocol, Src Port: 60180, Dst Port: 80, Seq: 1, Ack: 1, Len: 461
▼ Hypertext Transfer Protocol
  > GET /images/dave.jpeg HTTP/1.1\r\n
    Host: wireshark.grydeske.net\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/1
    Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://wireshark.grydeske.net/file4.html\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,de;q=0.6,ckb;q=0.5,ay;q=0.4,ku;q=0.3\r\n
    \r\n
    [Full request URI: http://wireshark.grydeske.net/images/dave.jpeg]
    [HTTP request 1/1]
    [Response in frame: 312]
```

b. Adreste bulunan iki resim dosyası seri olarak mı yoksa paralel olarak mı indirilmiştir?

Birinci resim dosyası indirilirken (195-206 aralığında) , ikinci resim dosyası da indirilmeye başlanmıştır (196-312 aralığı). Bu yüzden dosyalar paralel olarak indirilmiştir.

http						
No.	Time	Source	Destination	Protocol	Length	Info
111	7.122500	192.168.67.52	54.247.69.169	HTTP	559	GET /file4.html HTTP/1.1
154	7.333099	54.247.69.169	192.168.67.52	HTTP	167	HTTP/1.1 200 OK (text/html)
195	7.668303	192.168.67.52	54.247.69.169	HTTP	513	GET /images/SDU.png HTTP/1.1
196	7.668461	192.168.67.52	54.247.69.169	HTTP	515	GET /images/dave.jpeg HTTP/1.1
206	7.800372	54.247.69.169	192.168.67.52	HTTP	706	HTTP/1.1 200 OK (text/plain)
312	8.185307	54.247.69.169	192.168.67.52	HTTP	471	HTTP/1.1 200 OK (text/plain)

http						
No.	Time	Source	Destination	Protocol	Length	Info
111	7.122500	192.168.67.52	54.247.69.169	HTTP	559	GET /file4.html HTTP/1.1
154	7.333099	54.247.69.169	192.168.67.52	HTTP	167	HTTP/1.1 200 OK (text/html)
195	7.668303	192.168.67.52	54.247.69.169	HTTP	513	GET /images/SDU.png HTTP/1.1
196	7.668461	192.168.67.52	54.247.69.169	HTTP	515	GET /images/dave.jpeg HTTP/1.1
206	7.800372	54.247.69.169	192.168.67.52	HTTP	706	HTTP/1.1 200 OK (text/plain)
312	8.185307	54.247.69.169	192.168.67.52	HTTP	471	HTTP/1.1 200 OK (text/plain)

4. ④ nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız.

a. Sunucunun ilk GET isteğine gönderdiği cevap nedir? → İlk GET isteği 404 numaralı pakettir.

Bu pakete gelen cevaba [Response in frame] bilgisinden de ulaşabiliriz. → 408

No.	Time	Source	Destination	Protocol	Length	Info
404	12.443606	192.168.67.52	54.247.69.169	HTTP	665	GET /file5.html HTTP/1.1
408	12.552361	54.247.69.169	192.168.67.52	HTTP	1369	HTTP/1.1 401 Unauthorized (text/html)
451	21.818859	192.168.67.52	54.247.69.169	HTTP	708	GET /file5.html HTTP/1.1
453	21.922199	54.247.69.169	192.168.67.52	HTTP	770	HTTP/1.1 304 Not Modified

```
> Frame 408: 1369 bytes on wire (10952 bits), 1369 bytes captured (10952 bits) on interface \Device\NPF_{F
> Ethernet II, Src: 1e:26:8a:8a:ee:3b (1e:26:8a:8a:ee:3b), Dst: Intel_13:37:56 (38:87:d5:13:37:56)
> Internet Protocol Version 4, Src: 54.247.69.169, Dst: 192.168.67.52
> Transmission Control Protocol, Src Port: 80, Dst Port: 60489, Seq: 1, Ack: 612, Len: 1315
> Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Report-To: {"group":"heroku-nel","max_age":3600,"endpoints":[{"url":"https://nel.heroku.com/reports?t
    Reporting-Endpoints: heroku-nel=https://nel.heroku.com/reports?ts=1712407851&sid=c4c9725f-1ab0-44d8-8
    Nel: {"report_to":"heroku-nel","max_age":3600,"success_fraction":0.005,"failure_fraction":0.05,"respo
    Connection: keep-alive\r\n
    Server: nginx\r\n
    Date: Sat, 06 Apr 2024 12:50:51 GMT\r\n
    Content-Type: text/html\r\n
  > Content-Length: 574\r\n
    Www-Authenticate: Basic realm="You need authentication to see this"\r\n
    Via: 1.1 vegur\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.108755000 seconds]
    [Request in frame: 404]
    [Next request in frame: 451]
    [Next response in frame: 453]
    [Request URI: http://wireshark.grydeske.net/file5.html]
    File Data: 574 bytes
  > Line-based text data: text/html (13 lines)
```

b. Tarayıcımız ikinci kez GET isteği gönderdiğinde, bu HTML GET mesajında fazladan hangi bilgiler bulunmaktadır?

İkinci GET isteği (451) gönderdiğimizde “Authorization” bilgisi bulunmaktadır. Bunun sebebi 4 nolu dosyayı açtığımızda sayfada kullanıcı adı ve şifre bilgileriyle giriş yapmamızdır.

No.	Time	Source	Destination	Protocol	Length	Info
404	12.443606	192.168.67.52	54.247.69.169	HTTP	665	GET /file5.html
451	21.818859	192.168.67.52	54.247.69.169	HTTP	708	GET /file5.html


```
> Frame 451: 708 bytes on wire (5664 bits), 708 bytes captured (5664 bits) on interface \Device\NPF_{FD1E2
> Ethernet II, Src: Intel_13:37:56 (38:87:d5:13:37:56), Dst: 1e:26:8a:8a:ee:3b (1e:26:8a:8a:ee:3b)
> Internet Protocol Version 4, Src: 192.168.67.52, Dst: 54.247.69.169
> Transmission Control Protocol, Src Port: 60489, Dst Port: 80, Seq: 612, Ack: 1316, Len: 654
> Hypertext Transfer Protocol
  > GET /file5.html HTTP/1.1\r\n
    Host: wireshark.grydeske.net\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
  > Authorization: Basic ZG01NTc6bmV0d29yaw==\r\n
    Credentials: dm557:network
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/1
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7,de;q=0.6,ckb;q=0.5,ay;q=0.4,ku;q=0.3\r\n
    If-None-Match: "5d3f4f55-82"\r\n
    If-Modified-Since: Mon, 29 Jul 2019 19:56:05 GMT\r\n
    \r\n
    [Full request URI: http://wireshark.grydeske.net/file5.html]
    [HTTP request 2/2]
    [Prev request in frame: 404]
    [Response in frame: 453]
```