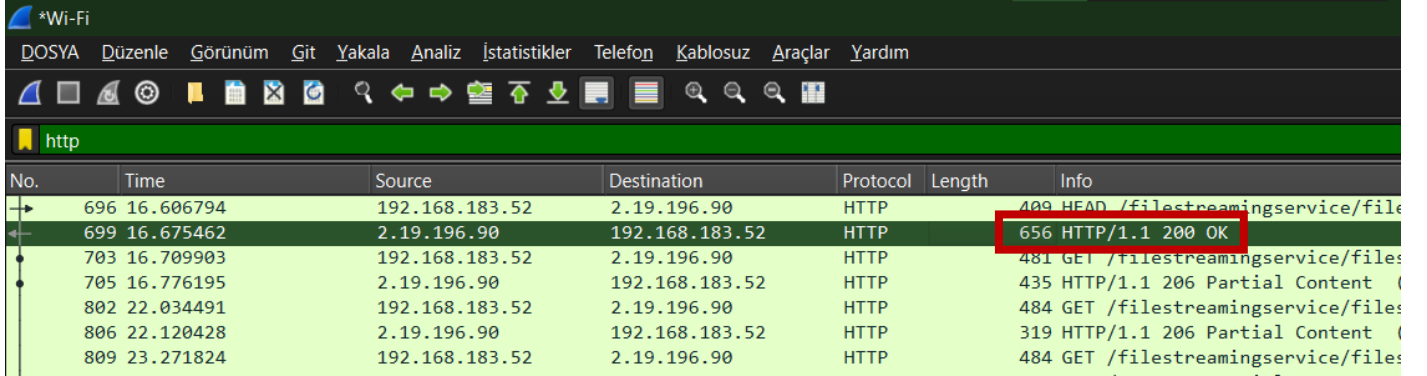


BİLGİSAYAR AĞLARI ÖDEV – II

1. ① nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız.
- a. Tarayıcınız HTTP 1.0 veya HTTP 1.1 sürümlerinden hangisini kullanmaktadır?
Kırmızı kutucukla 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	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	206 Partial Content
802	22.034491	192.168.183.52	2.19.196.90	HTTP	484	GET /filestreamingservice/files/...
806	22.120428	2.19.196.90	192.168.183.52	HTTP	319	206 Partial Content
809	23.271824	192.168.183.52	2.19.196.90	HTTP	484	GET /filestreamingservice/files/...

- b. Bilgisayarınızın IP adresi nedir?

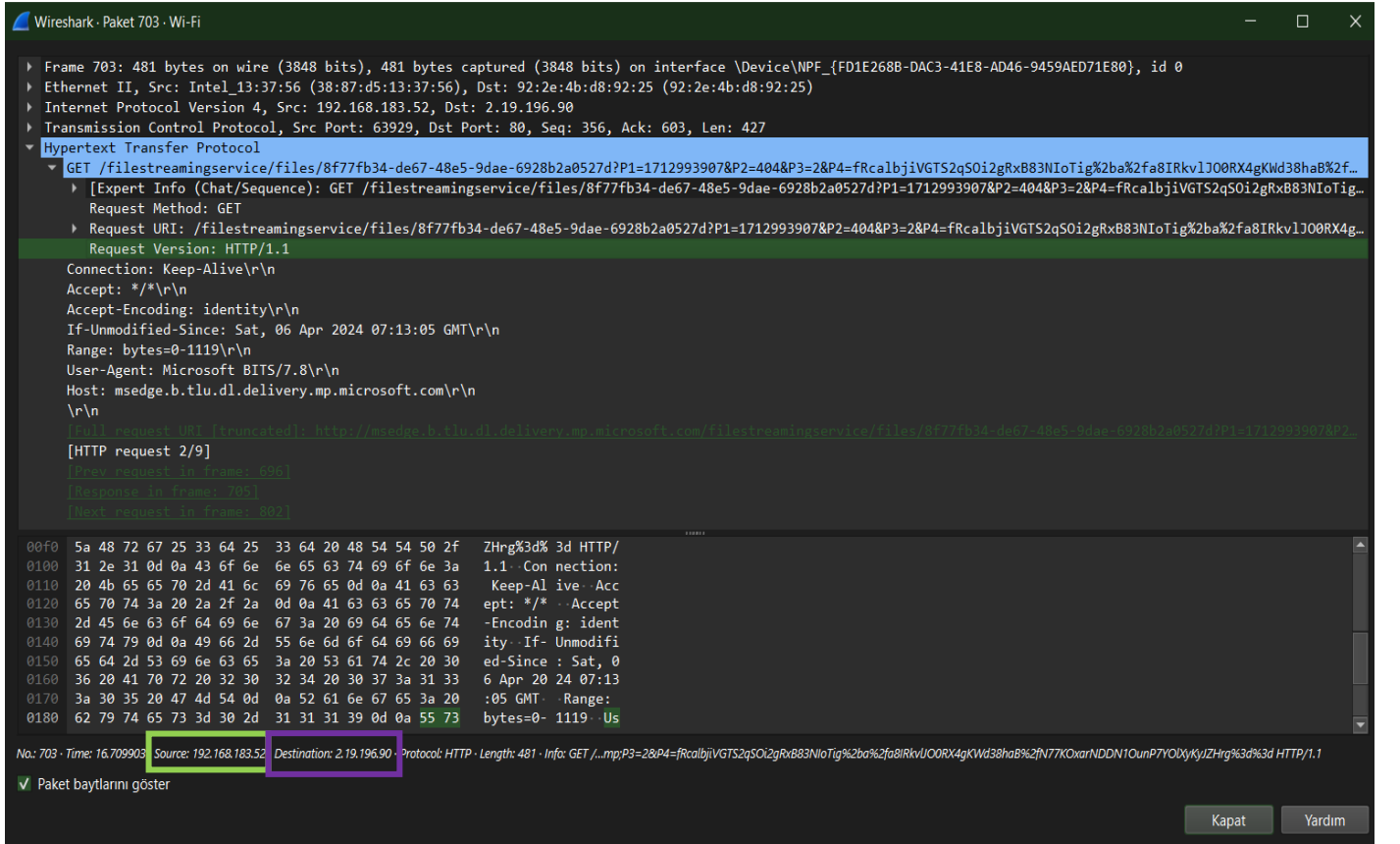
IP adresi bilgisine **yeşil** kutuyla belirtilen “Source” bilgisinden ulaşabiliriz.

IP adresi: 192.168.183.52

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

Sunucunun IP adresine **mor** kutuyla belirtilen “Destination” bilgisinden ulaşabiliriz.

IP adresi: 2.19.196.90



Wireshark - Paket 703 - Wi-Fi

Frame 703: 481 bytes on wire (3848 bits), 481 bytes captured (3848 bits) on interface \Device\NPF_{FD1E268B-DAC3-41E8-AD46-9459AED71E80}, id 0

Ethernet II, Src: Intel_13:37:56 (38:87:d5:13:37:56), Dst: 92:2e:4b:d8:92:25 (92:2e:4b:d8:92:25)

Internet Protocol Version 4, Src: 192.168.183.52, Dst: 2.19.196.90

Transmission Control Protocol, Src Port: 63929, Dst Port: 80, Seq: 356, Ack: 603, Len: 427

Hypertext Transfer Protocol

GET /filestreamingservice/files/8f77fb34-de67-48e5-9dae-6928b2a0527d?P1=1712993907&P2=404&P3=2&P4=fRcalbjivGTS2qSOi2gRx8B3NIoTig%2ba%2fa8IRkv1J00RX4gKwd38haB%2f... [Expert Info (Chat/Sequence): GET /filestreamingservice/files/8f77fb34-de67-48e5-9dae-6928b2a0527d?P1=1712993907&P2=404&P3=2&P4=fRcalbjivGTS2qSOi2gRx8B3NIoTig... Request Method: GET Request URI: /filestreamingservice/files/8f77fb34-de67-48e5-9dae-6928b2a0527d?P1=1712993907&P2=404&P3=2&P4=fRcalbjivGTS2qSOi2gRx8B3NIoTig%2ba%2fa8IRkv1J00RX4g... Request Version: HTTP/1.1 Connection: Keep-Alive\r\n Accept: */*\r\n Accept-Encoding: identity\r\n If-Unmodified-Since: Sat, 06 Apr 2024 07:13:05 GMT\r\n Range: bytes=0-1119\r\n User-Agent: Microsoft BITS/7.8\r\n Host: msedge.b.tlu.dl.delivery.mp.microsoft.com\r\n \r\n [Full request URI [truncated]: http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/8f77fb34-de67-48e5-9dae-6928b2a0527d?P1=1712993907&P2=404&P3=2&P4=fRcalbjivGTS2qSOi2gRx8B3NIoTig%2ba%2fa8IRkv1J00RX4gKwd38haB%2f... [HTTP request 2/9] [Prev request in frame: 696] [Response in frame: 705] [Next request in frame: 802]

00f0 5a 48 72 67 25 33 64 25 33 64 20 48 54 54 50 2f ZHrg%3d% 3d HTTP/
0100 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1.1. Con nection:
0110 20 4b 65 65 70 2d 41 6c 69 76 65 0d 0a 41 63 63 Keep-Al ive- Acc
0120 65 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63 65 70 74 ept: */* - Accep
0130 2d 45 6e 63 6f 64 69 6e 67 3a 20 69 64 65 6e 74 -Encodin g: ident
0140 69 74 79 0d 0a 49 66 2d 55 6e 6d 6f 64 69 66 69 ity -If- Unmodifi
0150 65 64 2d 53 69 6e 63 65 3a 20 53 61 74 2c 20 30 ed-Since : Sat, 0
0160 36 20 41 70 72 20 32 30 32 34 20 30 37 3a 31 33 6 Apr 20 24 07:13
0170 3a 30 35 20 47 4d 54 0d 0a 52 61 6e 67 65 3a 20 :05 GMT - Range:
0180 62 79 74 65 73 3d 30 2d 31 31 31 39 0d 0a 55 73 bytes=0- 1119 -Us

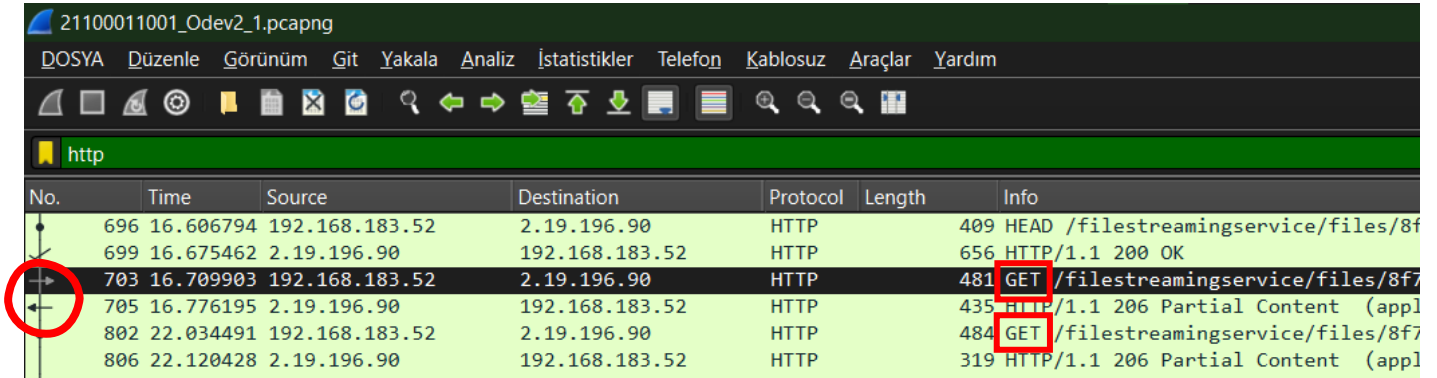
No: 703 · Time: 16.709903 · Source: 192.168.183.52 · Destination: 2.19.196.90 · Protocol: HTTP · Length: 481 · Info: GET /...mp;P3=2&P4=fRcalbjivGTS2qSOi2gRx8B3NIoTig%2ba%2fa8IRkv1J00RX4gKwd38haB%2fN77KOxarNDDN1OunP7Y0XyKjZHrg%3d%3d HTTP/1.1

✓ Paket baytlarını göster

Kapat Yardım

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

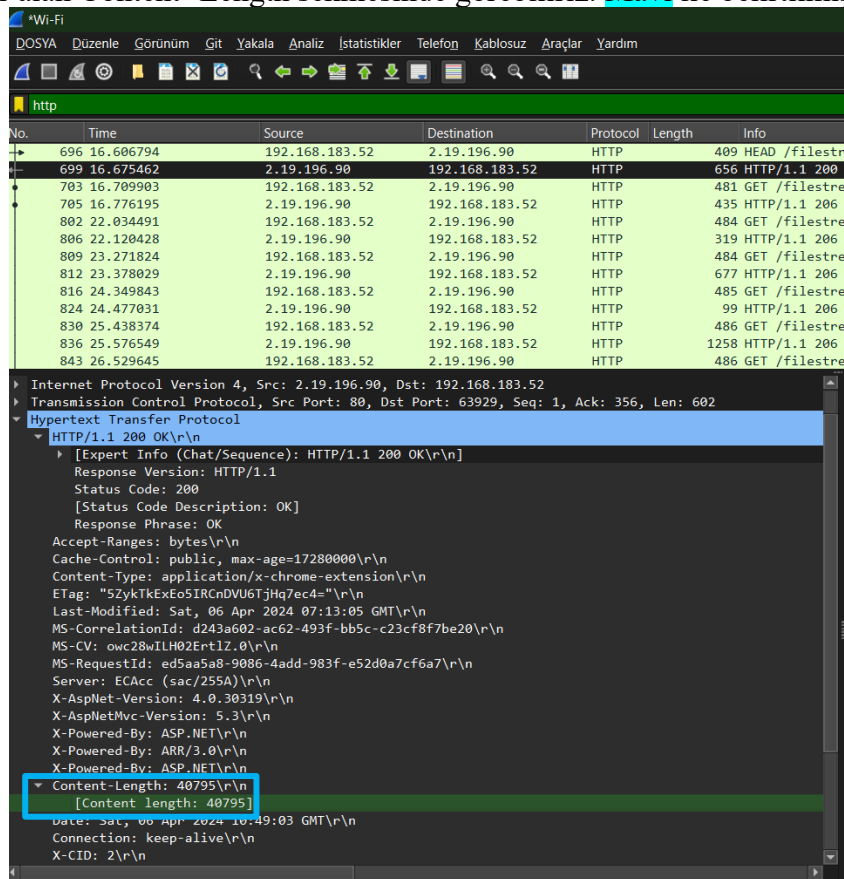
Sunucuya gönderilen GET isteklerini filtrelemek için filtreleme çubuğuna “*http.request.method==GET*” yazdık ve ilk GET isteği 703 numaralı pakettir. Bu isteğe cevap verilen paket 705 numaralı pakettir.



No.	Time	Source	Destination	Protocol	Length	Info
696	16.606794	192.168.183.52	2.19.196.90	HTTP	409	HEAD /filestreamingservice/files/8f7
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/8f7
705	16.776195	2.19.196.90	192.168.183.52	HTTP	435	HTTP/1.1 206 Partial Content (appl
802	22.034491	192.168.183.52	2.19.196.90	HTTP	484	GET /filestreamingservice/files/8f7
806	22.120428	2.19.196.90	192.168.183.52	HTTP	319	HTTP/1.1 206 Partial Content (appl

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. **Mavi** ile belirtilmiştir.



Internet Protocol Version 4, Src: 2.19.196.90, Dst: 192.168.183.52

Transmission Control Protocol, Src Port: 80, Dst Port: 63929, Seq: 1, Ack: 356, Len: 602

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

Response Version: HTTP/1.1

Status Code: 200

[Status Code Description: OK]

Response Phrase: OK

Accept-Ranges: bytes\r\n

Cache-Control: public, max-age=1728000\r\n

Content-Type: application/x-chrome-extension\r\n

ETag: "5ZykTkExEoSIRcndVUGtJHq7ec4="\r\n

Last-Modified: Sat, 06 Apr 2024 07:13:05 GMT\r\n

MS-CorrelationId: d243a602-ac62-493f-bb5c-c23cf8f7be20\r\n

MS-CV: owc28wILH02Ert1Z.0\r\n

MS-RequestId: ed5aa5a8-9086-4add-983f-e52d0a7cf6a7\r\n

Server: ECACC (sac/255A)\r\n

X-AspNet-Version: 4.0.30319\r\n

X-AspNetMvc-Version: 5.3\r\n

X-Powered-By: ASP.NET\r\n

X-Powered-By: ARR/3.0\r\n

X-Powered-By: ASP.NET\r\n

Content-Length: 40795\r\n

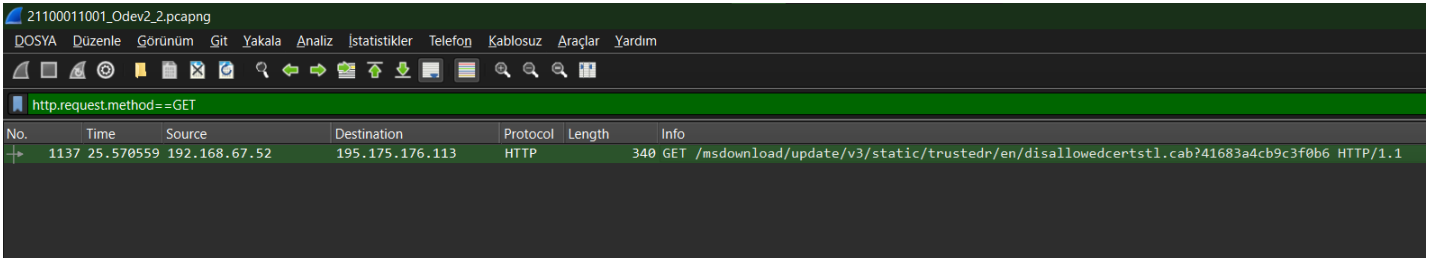
[Content length: 40795]

Date: Sat, 06 Apr 2024 10:49:03 GMT\r\n

Connection: keep-alive\r\n

X-CID: 2\r\n

2. ② nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız.
- Tarayıcınız sunucuya kaç tane GET isteği göndermiştir? → 1 tane
 - Sunucunun ilk GET isteğine gönderdiği cevap nedir?
→ "GET msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?41683a4cb9c3f0b6 HTTP/1.1



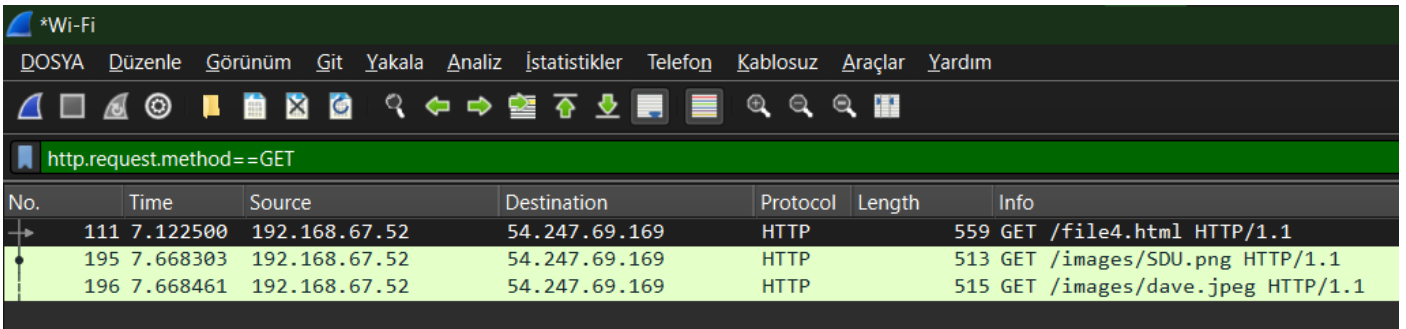
21100011001_Odev2_2.pcapng

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

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/static/trustedr/en/disallowedcertstl.cab?41683a4cb9c3f0b6 HTTP/1.1

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



*Wi-Fi

DOSYA Düzenle Görünüm Git Yakala Analiz İstatistikler Telefon Kablosuz Araçlar Yardım

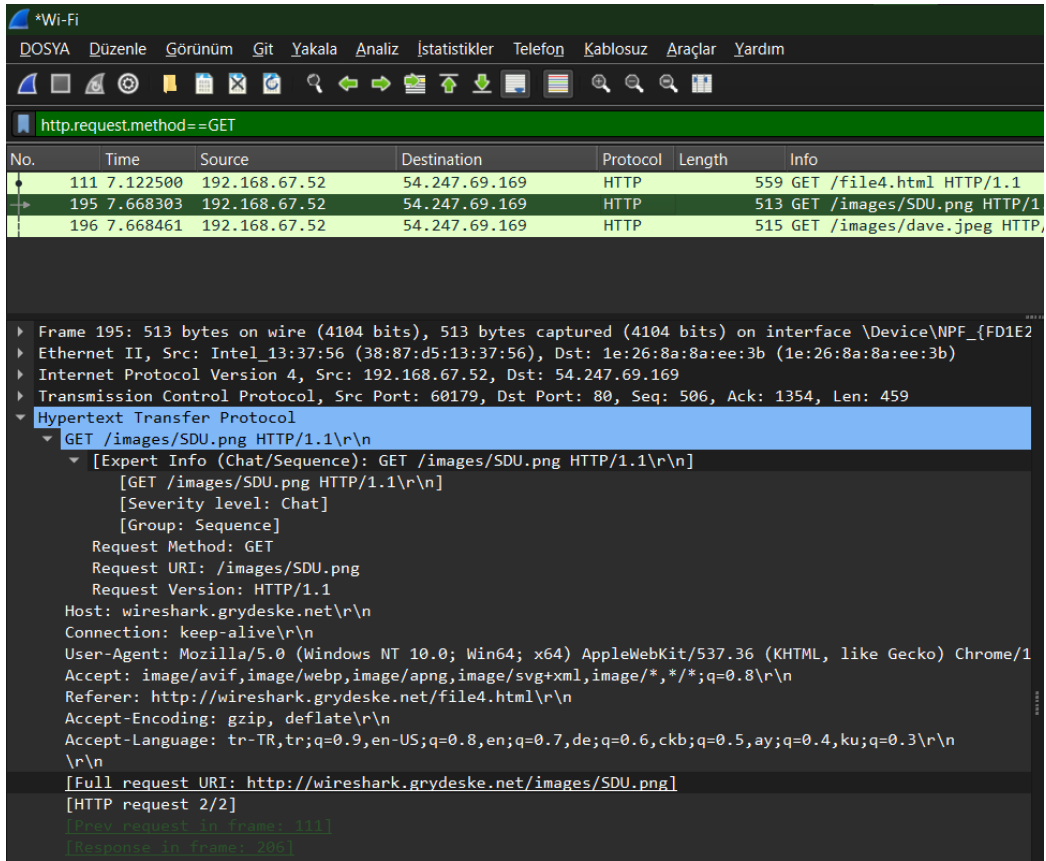
http.request.method==GET

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

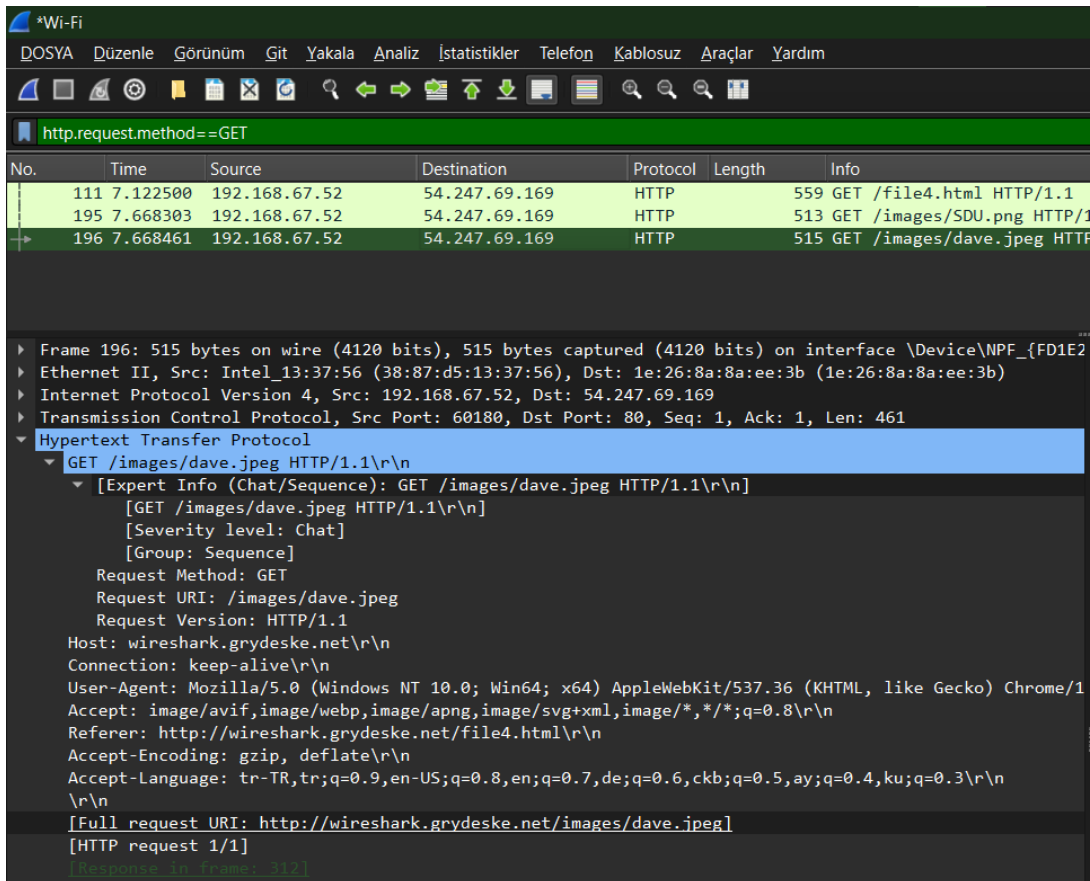
- Birinci yakalanan paket (111) için: [Full request URI: <http://wireshark.grydeske.net/file4.html>]

```
Frame 111: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{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: 1, Ack: 1, Len: 505
Hypertext Transfer Protocol
  GET /file4.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /file4.html HTTP/1.1\r\n]
    [GET /file4.html HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: GET
    Request URI: /file4.html
    Request Version: HTTP/1.1
    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/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
    \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>]

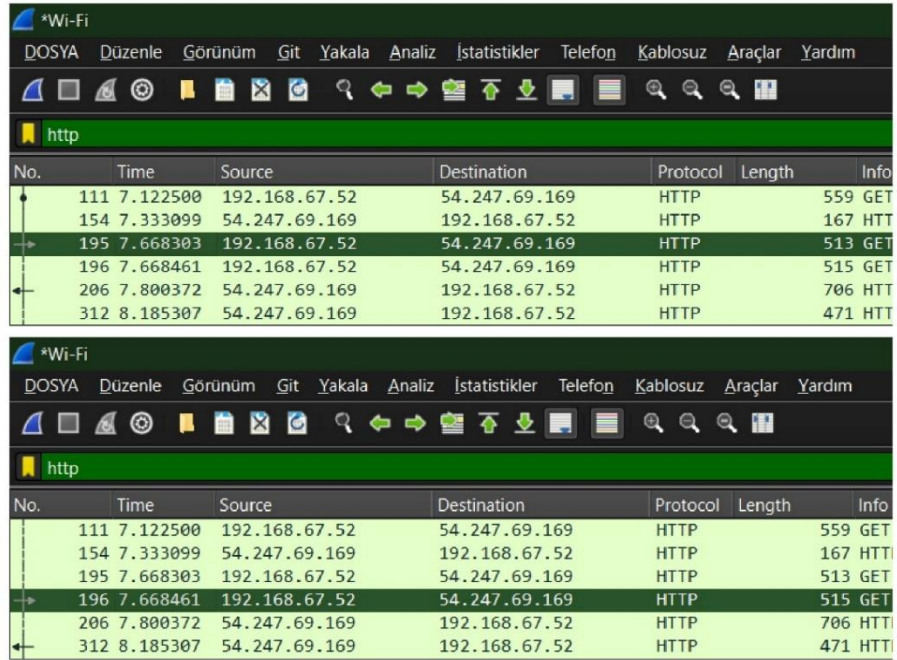


- Üçüncü yakalanan paket (196) için: [Full request URI: <http://wireshark.grydeske.net/images/dave.jpeg>]



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.



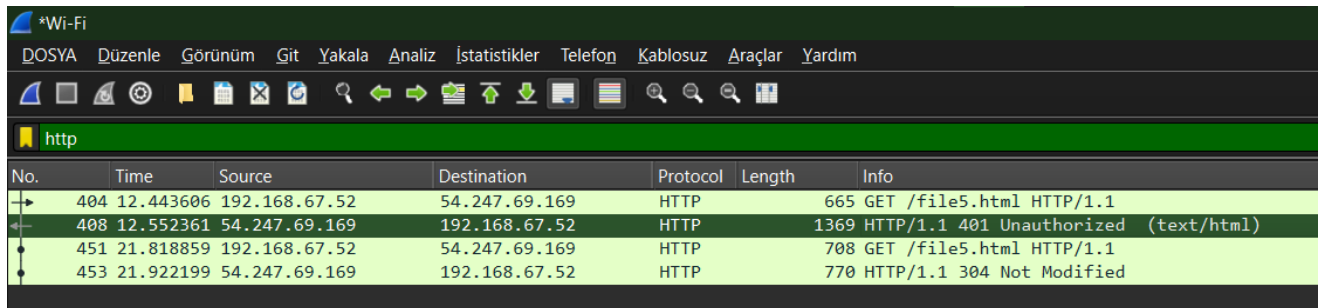
The image shows two screenshots of a Wi-Fi network traffic capture tool. The top screenshot shows a list of HTTP GET requests. The bottom screenshot shows the same list with additional details for the first two requests.

No.	Time	Source	Destination	Protocol	Length	Info
111	7.122500	192.168.67.52	54.247.69.169	HTTP	559	GET
154	7.333099	54.247.69.169	192.168.67.52	HTTP	167	HTT
195	7.668303	192.168.67.52	54.247.69.169	HTTP	513	GET
196	7.668461	192.168.67.52	54.247.69.169	HTTP	515	GET
206	7.800372	54.247.69.169	192.168.67.52	HTTP	706	HTT
312	8.185307	54.247.69.169	192.168.67.52	HTTP	471	HTT

No.	Time	Source	Destination	Protocol	Length	Info
111	7.122500	192.168.67.52	54.247.69.169	HTTP	559	GET
154	7.333099	54.247.69.169	192.168.67.52	HTTP	167	HTT
195	7.668303	192.168.67.52	54.247.69.169	HTTP	513	GET
196	7.668461	192.168.67.52	54.247.69.169	HTTP	515	GET
206	7.800372	54.247.69.169	192.168.67.52	HTTP	706	HTT
312	8.185307	54.247.69.169	192.168.67.52	HTTP	471	HTT

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

- a. Sunucunun ilk GET isteğine gönderdiği cevap nedir? → İlk GET isteğine dönen cevap (408): "HTTP/1.1 401 Unauthorized (text/html)" olmuştur.



The image shows a screenshot of a Wi-Fi network traffic capture tool. The table below shows the details of the captured packets.

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

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

Wi-Fi
DOSYA
Düzenle
Görünüm
Git
Yakala
Analiz
İstatistikler
Telefon
Kablosuz
Araçlar
Yardım

http

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
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 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]