

22100011015 Nursena Taşköprü

2024 – 2025 Bahar Dönemi Bilgisayar Ağları Dersi Ödev 2

1.① nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız

a. Tarayıcınız HTTP 1.0 veya HTTP 1.1 sürümlerinden hangisini kullanmaktadır.

Filtre kısmına http.request yazdıktan sonra get olan pakete tıklıyorum detaylarda request version gözüküyor. Tarayıcım http 1.1 kullanıyor.

http.request	
No.	Time
22	1.980071
54	3.198730
59	3.988836

Frame 22: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bit)

Ethernet II, Src: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef), Dst: 2e:

Internet Protocol Version 4, Src: 192.168.52.35, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 52682, Dst Port: 80, Seq: 1,

Hypertext Transfer Protocol

- GET /favicon.ico HTTP/1.1\r\n
- Request Method: GET
- Request URI: /favicon.ico
- Request Version: HTTP/1.1
- Host: gaia.cs.umass.edu\r\n
- Connection: keep-alive\r\n
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/5
- Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;
- Referer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-fi

b. Bilgisayarınızın IP adresi nedir?

Filtre çubuğuna arp || dhcp yazdıktan sonra en üstteki satırda info kısmında "Who has 192.168.52.35? Tell 192.168.52.109" yazıyor. Buradaki "Tell 192.168.52.109" kısmındaki 192.168.52.109 benim ip adresim oluyor.

arp dhcp						
	Time	Source	Destination	Protocol	Length	Info
74	6.918405	2e:30:aa:3a:da:4c	AzureWaveTec_50:07:...	ARP	42	Who has 192.168.52.35? Tell 192.168.52.109
75	6.918424	AzureWaveTec_50:07:...	2e:30:aa:3a:da:4c	ARP	42	192.168.52.35 is at b4:8c:9d:50:07:ef

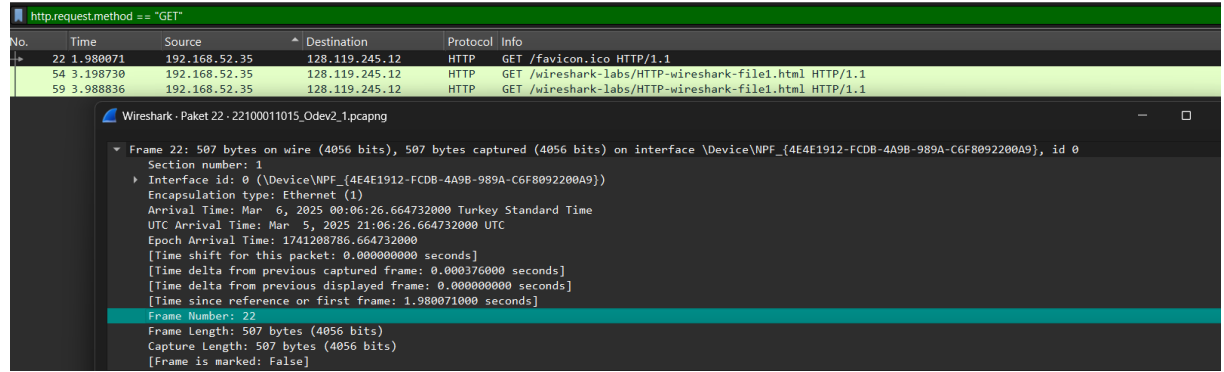
c. gaia.cs.umass.edu sunucusunun IP adresi nedir?

Filtre çubuğuna http.host contains "gaia.cs.umass.edu" yazıyorum çıkan sonuçtaki destination sütununda sunucunun adresini görürüm

http.host contains "gaia.cs.umass.edu"						
No.	Time	Source	Destination	Protocol	Info	
22	1.980071	192.168.52.35	128.119.245.12	HTTP	GET /favicon.ico HTTP/1.1	
54	3.198730	192.168.52.35	128.119.245.12	HTTP	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	
59	3.988836	192.168.52.35	128.119.245.12	HTTP	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1	

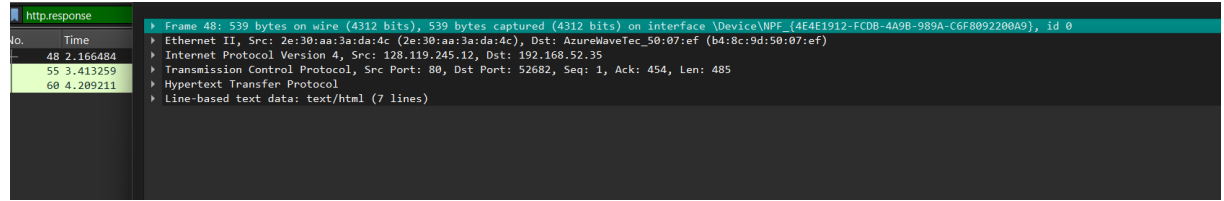
d. Sunucuya gönderilen ilk GET isteği ile bu isteğe verilen cevap bilgileri hangi paketlerde görülmektedir?

Filtre çubuğuna `http.request.method == "GET"` yazarım ilkin tıklayıp frame numarasına bakarım

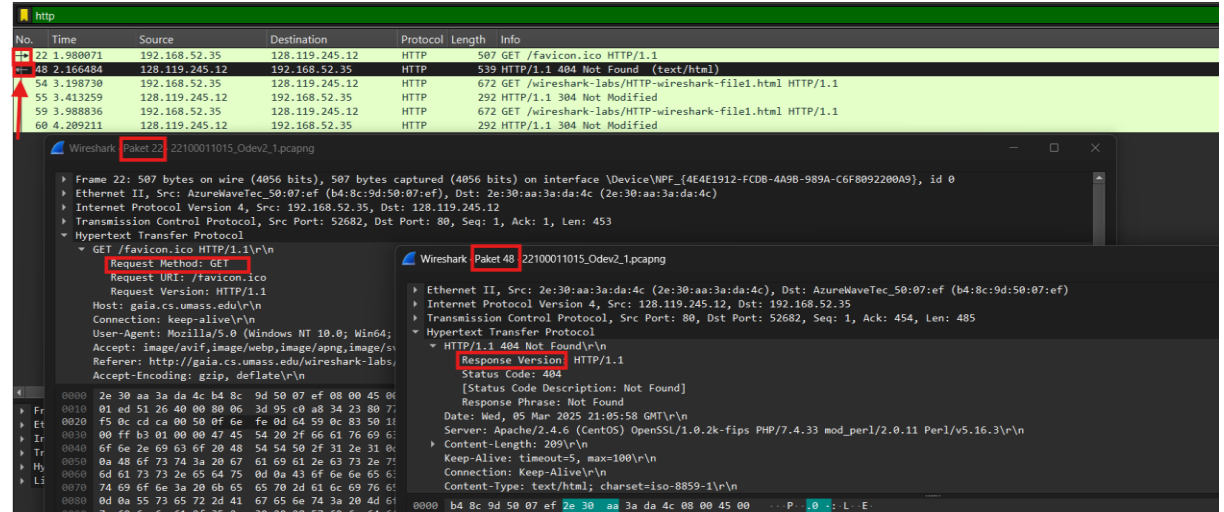


İstekte bulunan paketin destinationuna bakarız responsda bu adrese sahip olan olur.

`http.response` diyerek sunucu yanıtına bakarım



En son `http` diyerek ikisinin yan yana olduğu kısma bakarım.



e. Sunucudan tarayıcınıza kaç byte boyutunda içerik gönderilmiştir?

Filtre kısmına `http.response` yazarım. İlkine tıklarım bu da sunucunun get isteğine verdiği yanittır

No.	Time	Source	Destination	Protocol	Length	Info
48	2.166484	128.119.245.12	192.168.52.35	HTTP	539	HTTP/1.1 404 Not Found (text/html)
55	3.413259	128.119.245.12	192.168.52.35	HTTP	293	HTTP/1.1 304 Not Modified
60	4.209211	128.119.245.12	192.168.52.35	HTTP	293	HTTP/1.1 304 Not Modified

Wireshark - Paket 48 - 22100011015_Odev2_1.pcapng

Frame 48: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{4E4E1912-FCDB-4A9B-...}

Ethernet II, Src: 2e:30:aa:3a:da:4c (2e:30:aa:3a:da:4c), Dst: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.52.35

Transmission Control Protocol, Src Port: 80, Dst Port: 52682, Seq: 1, Ack: 454, Len: 485

Hypertext Transfer Protocol

HTTP/1.1 404 Not Found\r\n

Response Version: HTTP/1.1

Status Code: 404

[Status Code Description: Not Found]

Response Phrase: Not Found

Date: Wed, 05 Mar 2025 21:05:58 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n

Content-Length: 209\r\n

[Content length: 209]

Keep-Alive: timeout=5, max=100\r\n

content_length: 209 byte boyutunda içerik göndermiştir.

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

a. Tarayıcınız sunucuya kaç tane GET isteği göndermiştir?

Filtre kısmına `http.request.method == "GET"` yazıp get isteklerini görüntülerim

No.	Time	Source	Destination	Protocol	Length	Info
31	0.692307	192.168.52.35	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
90	0.904954	192.168.52.35	128.119.245.12	HTTP	507	GET /favicon.ico HTTP/1.1
1...	5.243455	192.168.52.35	128.119.245.12	HTTP	674	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1...	7.082104	192.168.52.35	128.119.245.12	HTTP	674	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

4 adet get isteği var.

No.	Time	Source	Destination	Protocol	Length	Info
31	0.692307	192.168.52.35	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
90	0.904954	192.168.52.35	128.119.245.12	HTTP	507	GET /favicon.ico HTTP/1.1
1...	5.243455	192.168.52.35	128.119.245.12	HTTP	674	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1...	7.082104	192.168.52.35	128.119.245.12	HTTP	674	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1

Request Type

Count Average Min Val Max Val Rate (ms) Percent Burst Rate Burst Start

HTTP Requests by HTTP Host

4 0.0006 100% 0.0100 0.692

gaia.cs.umass.edu

4 0.0006 100.00% 0.0100 0.692

/wireshark-labs/HTTP-wireshark-file3.html 3 0.0005 75.00% 0.0100 0.692

/favicon.ico 1 0.0002 25.00% 0.0100 0.905

Buradan da görebiliriz.

b. Sunucunun bu get isteğine gönderdiği cevap kodu ve açıklaması nedir?

Filtre çubuğuna `http.response` yazıp http yanıtlarını görürüm

No.	Time	Source	Destination	Protocol	Length	Info
78	0.880959	128.119.245.12	192.168.52.35	HTTP	898	HTTP/1.1 200 OK (text/html)
1...	1.084542	128.119.245.12	192.168.52.35	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1...	5.466329	128.119.245.12	192.168.52.35	HTTP	294	HTTP/1.1 304 Not Modified
1...	7.304923	128.119.245.12	192.168.52.35	HTTP	294	HTTP/1.1 304 Not Modified

Sonrasında ilkinde tıklayıp status code kısmına bakarız. Kodun karşılığı açıklaması olur

No.	Time	Source	Destination	Protocol	Length	Info
78	0.880959	128.119.245.12	192.168.52.35	HTTP	898	HTTP/1.1 200 OK (text/html)
1..	1.084542	128.119.245.12	192.168.52.35	Wireshark - Paket 78 - 22100011015_Odev2_2.pcapng		
1..	5.466329	128.119.245.12	192.168.52.35			
1..	7.384923	128.119.245.12	192.168.52.35			

Frame 78: 898 bytes on wire (7184 bits), 898 bytes captured (7184 bits) on interface \Device\NPF_{4E4E1912-FCDB-4A9B-989A-C6F8092200A9}, id 0
 Ethernet II, Src: 2e:30:aa:3a:da:4c (2e:30:aa:3a:da:4c), Dst: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef)
 Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.52.35
 Transmission Control Protocol, Src Port: 80, Dst Port: 52718, Seq: 4018, Ack: 508, Len: 844
 [4 Reassembled TCP Segments (4861 bytes): #72(1339), #73(1339), #77(1339), #78(844)]
 Hypertext Transfer Protocol
 HTTP/1.1 200 OK\r\n
 Status Code: 200
 [Status Code Description: OK]
 Response Phrase: OK
 Date: Wed, 05 Mar 2025 21:07:19 GMT\r\n
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n

200 OK → Başarılı demektir

3. ③ nolu dosyada HTTP paketlerini görüntüleyerek aşağıdaki soruları cevaplandırınız.

a. Tarayıcınız sunucuya kaç tane GET isteği göndermiştir? Her bir GET isteği hangi internet adreslerine gönderilmiştir?

Filtreye `http.request.method == "GET"` yazalım

No.	Time	Source	Destination	Protocol	Length	Info
52	1.986654	192.168.52.35	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
78	2.163302	192.168.52.35	128.119.245.12	HTTP	507	GET /pearson.png HTTP/1.1
1..	2.307097	192.168.52.35	178.79.137.164	HTTP	474	GET /8E_cover_small.jpg HTTP/1.1
7..	3.457894	192.168.52.35	128.119.245.12	HTTP	507	GET /favicon.ico HTTP/1.1
7..	7.090042	192.168.52.35	128.119.245.12	HTTP	673	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
7..	10.711355	192.168.52.35	128.119.245.12	HTTP	608	GET /kurose_ross HTTP/1.1
8..	10.889057	192.168.52.35	128.119.245.12	HTTP	609	GET /kurose_ross/ HTTP/1.1
8..	11.097603	192.168.52.35	128.119.245.12	HTTP	618	GET /kurose_ross/index.php HTTP/1.1
8..	11.271946	192.168.52.35	128.119.245.12	HTTP	453	GET /kurose_ross/custom.css HTTP/1.1
8..	11.272818	192.168.52.35	128.119.245.12	HTTP	437	GET /kurose_ross/script.js HTTP/1.1
8..	11.446702	192.168.52.35	128.119.245.12	HTTP	517	GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1

Satır sayısı kadar get isteği vardır. -> 11 tane get isteği var

1. istek

No.	Time	Source	Destination	Protocol	Length	Info
52	1.986654	192.168.52.35	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
78	2.163302	192.168.52.35	128.119.245.12	HTTP	507	GET /pearson.png HTTP/1.1
1..	2.307097	192.168.52.35	178.79.137.164	HTTP	474	GET /8E_cover_small.jpg HTTP/1.1
7..	3.457894	192.168.52.35	128.119.245.12	HTTP	507	GET /favicon.ico HTTP/1.1
7..	7.090042	192.168.52.35	128.119.245.12	HTTP	673	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
7..	10.711355	192.168.52.35	128.119.245.12	HTTP	608	GET /kurose_ross HTTP/1.1
8..	10.889057	192.168.52.35	128.119.245.12	HTTP	609	GET /kurose_ross/ HTTP/1.1
8..	11.097603	192.168.52.35	128.119.245.12	HTTP	618	GET /kurose_ross/index.php HTTP/1.1
8..	11.271946	192.168.52.35	128.119.245.12	HTTP	453	GET /kurose_ross/custom.css HTTP/1.1
8..	11.272818	192.168.52.35	128.119.245.12	HTTP	437	GET /kurose_ross/script.js HTTP/1.1
8..	11.446702	192.168.52.35	128.119.245.12	HTTP	517	GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1

Wireshark - Paket 52 - 22100011015_Odev2_2.pcapng
 Frame 52: 561 bytes on wire (4488 bits), 561 bytes captured (4488 bits) on interface \Device\NPF_{4E4E1912-FCDB-4A9B-989A-C6F8092200A9}, id 0
 Ethernet II, Src: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef), Dst: 2e:30:aa:3a:da:4c (2e:30:aa:3a:da:4c)
 Internet Protocol Version 4, Src: 192.168.52.35, Dst: 128.119.245.12
 Transmission Control Protocol, Src Port: 52744, Dst Port: 80, Seq: 1, Ack: 1, Len: 507
 Hypertext Transfer Protocol
 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n
 Request Method: GET
 Request URI: /wireshark-labs/HTTP-wireshark-file4.html
 Request Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n
 Connection: keep-alive\r\n

2. istek

No.	Time	Source	Destination	Protocol	Length	Info
52	1.986654	192.168.52.35	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file4.html
78	2.163302	192.168.52.35	128.119.245.12	HTTP	507	GET /pearson.png HTTP/1.1
1...	2.307097	192.168.52.35	128.119.245.12	Wireshark - Paket 78 - 22100011015_Odev2_3.pcapng		
7...	3.457894	192.168.52.35	128.119.245.12			
7...	7.090042	192.168.52.35	128.119.245.12			
7...	10.711355	192.168.52.35	128.119.245.12			
8...	10.889057	192.168.52.35	128.119.245.12			
8...	11.097603	192.168.52.35	128.119.245.12			
8...	11.271946	192.168.52.35	128.119.245.12			
8...	11.272818	192.168.52.35	128.119.245.12			
8...	11.446702	192.168.52.35	128.119.245.12			

Frame 78: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface 0
Ethernet II, Src: AzureWaveTec_50:07:ef (b4:8c:9d:50:07:ef), Dst: 2e:30:aa:38:00:00
Internet Protocol Version 4, Src: 192.168.52.35, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 52744, Dst Port: 80, Seq: 508, Ack: 3495
Hypertext Transfer Protocol

GET /pearson.png HTTP/1.1\r\n

Request Method: GET

Request URI: /pearson.png

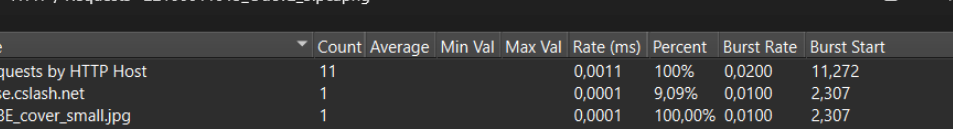
Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\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/104.0.0.0 Safari/537.36

hepsine tek tek tıklayıp bakabiliriz. Farklı olarak İstatistikler -> http -> istekler kısmından toplu da görebiliriz



Wireshark · HTTP / Requests · 22100011015_Odev2_3.pcapng

Request Type	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
HTTP Requests by HTTP Host	11				0,0011	100%	0,0200	11,272
kurose.cslash.net	1				0,0001	9,09%	0,0100	2,307
/8E_cover_small.jpg	1				0,0001	100,00%	0,0100	2,307
gaia.cs.umass.edu	10				0,0010	90,91%	0,0200	11,272
/wireshark-labs/HTTP-wireshark-file4.html	2				0,0002	20,00%	0,0100	1,987
/pearson.png	1				0,0001	10,00%	0,0100	2,163
/kurose_ross/script.js	1				0,0001	10,00%	0,0100	11,273
/kurose_ross/index.php	1				0,0001	10,00%	0,0100	11,098
/kurose_ross/header_graphic_book_8E_3.jpg	1				0,0001	10,00%	0,0100	11,447
/kurose_ross/custom.css	1				0,0001	10,00%	0,0100	11,272
/kurose_ross/	1				0,0001	10,00%	0,0100	10,889
/kurose_ross	1				0,0001	10,00%	0,0100	10,711
/favicon.ico	1				0,0001	10,00%	0,0100	3,458

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

Filtre kısmına `http.request.method == "GET"` yazarız. `.jpg`, `.png`, `.gif` gibi uzantılara sahip olan resim dosyalarını görebiliriz info kısmına bakarak

No.	Time	Source	Destination	Protocol	Length	Info
52	1.986654	192.168.52.35	128.119.245.12	HTTP	561	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
78	2.163302	192.168.52.35	128.119.245.12	HTTP	507	GET pearson.png HTTP/1.1
1.	2.307097	192.168.52.35	178.79.137.164	HTTP	474	GET /3E_cover_small.jpg HTTP/1.1
7.	3.457894	192.168.52.35	128.119.245.12	HTTP	507	GET favicon.ico HTTP/1.1
7.	7.090042	192.168.52.35	128.119.245.12	HTTP	673	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
7.	10.711355	192.168.52.35	128.119.245.12	HTTP	608	GET /kurose_ross HTTP/1.1
8.	10.889057	192.168.52.35	128.119.245.12	HTTP	609	GET /kurose_ross/ HTTP/1.1
8.	11.097603	192.168.52.35	128.119.245.12	HTTP	618	GET /kurose_ross/index.php HTTP/1.1
8.	11.271946	192.168.52.35	128.119.245.12	HTTP	453	GET /kurose_ross/custom.css HTTP/1.1
8.	11.272818	192.168.52.35	128.119.245.12	HTTP	437	GET /kurose_ross/script.js HTTP/1.1
8.	11.446702	192.168.52.35	128.119.245.12	HTTP	517	GET /kurose_ross/header_graphic_book_8E_3.jpg HTTP/1.1

Time kısımlarına bakarak seri mi paralel mi indirilmiş görebiliriz. Aynı zamanda indirilmişse paralel farklı zamanlarda indirilmişse seri.

Burda farklı zamanlarda indirilmiş o yüzden seri indirme.

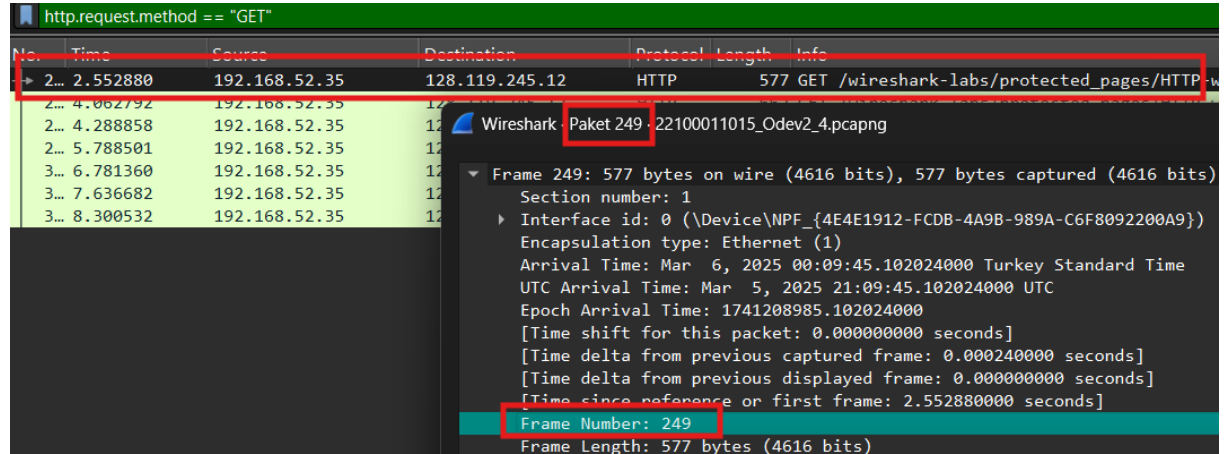
İlk get isteği tamamlandıktan sonra ikinci get isteği başlamış

Paralel indirme olsaydı, iki get isteği neredeyse aynı anda olurdu.

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

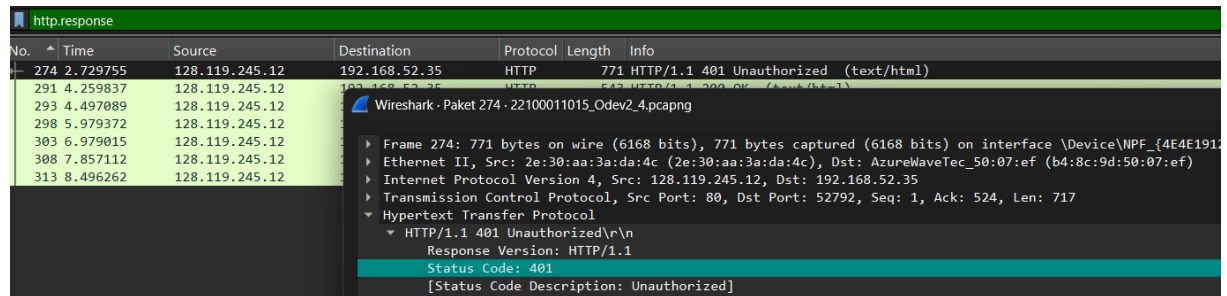
a. Sunucunun ilk GET isteğine gönderdiği cevap nedir?

http.request.method == "GET" yazarak filtreye ilki ilk get isteği. Frame numarası 249



sunucunun bu get isteğine yanıtını görmek için http.response yazarak filtreye

ilk get isteğindeki destinationa bakarız ordaki status code kısmına bakarak cevabı görürüz



Status code: 401 -> Unauthorized -> erişim için kimlik doğrulama gerekiyor

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

http.request.method == "GET" yazıp ilkinde tıklarız.

Sırayla önce ilk sonra ikinci isteğin Frame No, Packet Details , başlık bilgilerini (Headers) inceleriz. İkinciye neler eklenmiş görürüz

```
http.request.method == "GET"

No.  Time  Source  Destination  Protocol  Length  Info
249  2.552880  192.168.52.35  128.119.245.12  HTTP  577  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1

289  4.0627  Wireshark - Paket 249 - 22100011015_Odev2_4.pcapng  Wireshark - Paket 289 - 22100011015_Odev2_4.pcapng

Hypertext Transfer Protocol
  GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
  Request Method: GET
  Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\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/133.0.0.0 Safari/537.36 Edg/133.0.0.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
  Accept-Encoding: gzip, deflate\r\n
  Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
  \r\n
  [Response in frame: 274]
  [Full request URI: http://gaia.cs.umass.edu/protected_pages/HTTP-wireshark-file5.html]

Request Method: GET
Request URI: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZXNoVXJrLXN0dWk1bnRzOm5ldHdvcm0=\r\n
Credentials: wireshark-students: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/133.0.0.0 Safari/537.36 Edg/133.0.0.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: tr,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
\r\n
[Response in frame: 291]
```

ortadaki kısım authorization(Kimlik doğrulama) ikinci istekte eklenmiş.