



## **Laboratuvar Raporu 1**

**Eskişehir Osmangazi Üniversitesi**

**Bilgisayar Ağları**

**152116028**

**Ferdi İslam Yılmaz**

**152120191055**

**Dr. Öğr. Üyesi İlker Özçelik**

**2022-2023**

# **1 İindekiler**

2	Giriş.....	3
3	Laboratuvar Uygulaması.....	3
3.1	The Basic HTTP GET/response interaction .....	3
3.2	The HTTP CONDITIONAL GET/response interaction .....	4
3.3	Retrieving Long Documents.....	5
3.4	HTML Documents with Embedded Objects .....	5
3.5	HTTP Authentication .....	6
4	Kaynaka.....	6

## 2 Giriş

Bu labaratuvarıda basit http kodlarını deneyeceğiz. Kullanacağımız sitelerdeki GET OK kodlarını göreceğiz.

## 3 Laboratuvar Uygulaması

### 3.1 The Basic HTTP GET/response interaction

Tarayıcımızdan basit bir http dosyası indirdik. Daha sonra indirdiğimiz dosyanın paketlerini WireShark uygulaması ile yakalayıp incelemeye başladık.

The image shows a Wireshark network traffic capture window. The top pane displays a list of captured packets. The second pane shows the details of the selected packet (No. 39696), which is an HTTP 200 OK response. The third pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
39673	325.089918	192.168.0.105	128.119.245.12	HTTP	466	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
39696	325.218933	128.119.245.12	192.168.0.105	HTTP	540	HTTP/1.1 200 OK (text/html)

Details of packet 39696 (HTTP/1.1 200 OK):

- Date: Thu, 23 Mar 2023 14:05:32 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 m\r\n
- Last-Modified: Thu, 23 Mar 2023 05:59:01 GMT\r\n
- Etag: "80-5f78af92f7965"\r\n
- Accept-Ranges: bytes\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

Raw packet data (hexadecimal):

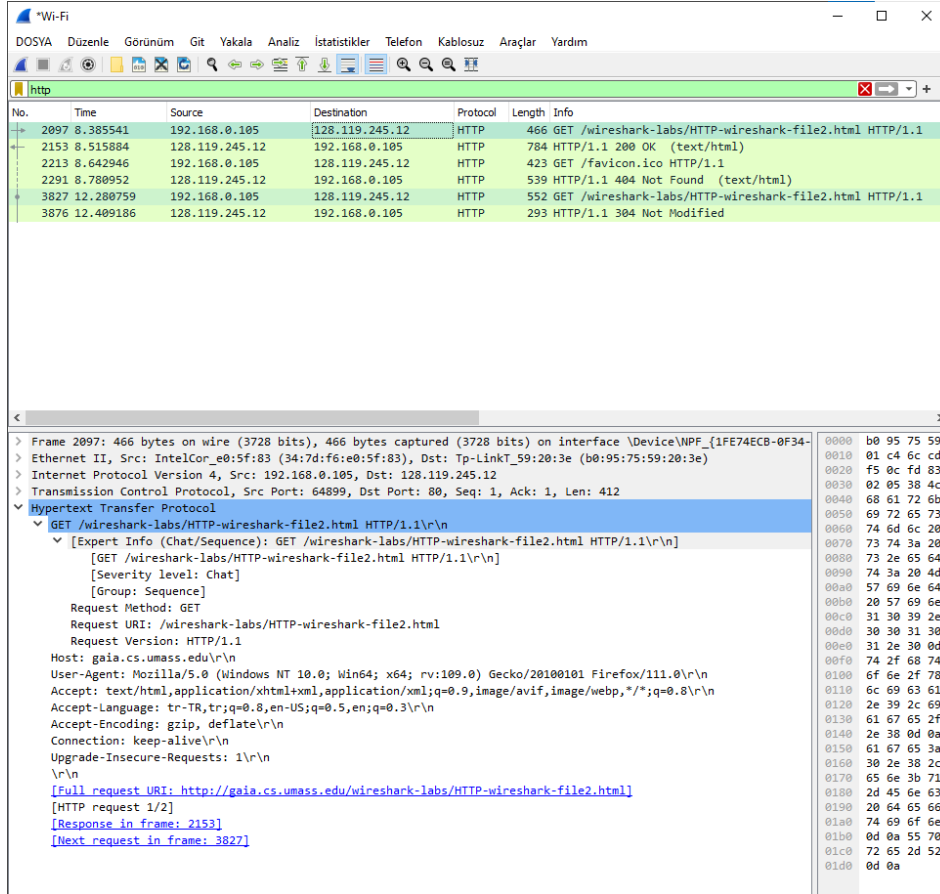
```
0000 34 7d f6 e0 5f 83 b0 95 75 59 20 3e 08 00 45 00 4d 72 80 77 f5 0c c0 a8  
0010 02 0e 05 e3 40 00 2f 06 0d 72 80 77 f5 0c c0 a8 30 0e 20 b5 3d c1 50 18  
0020 00 69 00 50 c0 91 a7 f4 30 0e 20 b5 3d c1 50 18 00 ed d9 25 00 00 48 54  
0030 54 50 2f 31 2e 31 20 32 61 74 65 3a 20 54 68 75 2c 20 32 33 20 31 34  
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 2c 20 32 33 20 31 34  
0050 2c 20 32 33 20 4d 61 72 20 32 30 32 33 20 31 34 3a 30 35 3a 33 32 20 47  
0060 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36  
0070 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 2d 66 69 70 73 20 50 48  
0080 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e 33 33  
0090 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35  
00a0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 75 2c 20 32 33 20 4d 61  
00b0 66 69 65 64 3a 20 54 68 75 2c 20 32 33 20 4d 61 35 3a 35 39 3a 30 31 20  
00c0 72 20 32 30 32 33 20 30 35 3a 35 39 3a 30 31 20 47 4d 54 0d 0a 54 54 61  
00d0 67 3a 20 22 38 30 2d 35 67 3a 20 22 38 30 2d 35 67 3a 20 22 38 30 2d 35  
00e0 66 37 38 61 66 39 32 66 37 39 36 35 22 0d 0a 41 6e 67 65 73 3a 20 62 79  
00f0 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e  
0100 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 74 65 6e 74 2d 4c 65 6e  
0110 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 6d 65 6f 75 74 3d 35 2c  
0120 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c 20 6d 61 78 3d 31 30 30  
0130 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65  
0140 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 65 70 2d 41 6c 3b 20 63  
0150 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6c 3b 20 63 68 61 72 73  
0160 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 0d 0a 0d 0a 3c 68 74 6d  
0170 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 0a 43 6f 6e 67 72  
0180 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f 6e 73 2e 20 20 59 6f 75  
0190 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e 6c 6f 61 64 65 64 20 74  
01a0 68 65 20 66 69 6c 65 20 0a 68 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e  
01b0 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 61 72 6b 2d 6c 61 62 73  
01c0 2f 48 54 50 2d 77 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74  
01d0 6d 6c 21 0a 3c 2f 68 74 6d 6c 3e 0a
```

İlk dosyayı indirdikten sonra uygulamamız böyle gözüküyordu.

Tarayıcı ve server http'nin 1.1 versiyonunu kullanmaktadır. Tarayıcının hangi dili kabul ettiği hakkında bir yorumda bulunamadım. Bilgisayarımın IP adresi 192.168.0.105 , sunucunun IP adresi ise 128.119.245.12'dir. GET kodu yolladığımda bilgisayarına OK durum kodu döndü.

HTML dosyasının son değiştirilme tarihi 23 Mart 2023 05:59:01 dir. Tarayıcıma 128 Byte boyutunda içerik dönüş yapmış.

### 3.2 The HTTP CONDITIONAL GET/response interaction



The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 3827), which is an HTTP GET request. The packet is from 192.168.0.105 to 128.119.245.12. The details pane shows the request method as GET, the request URI as /wireshark-labs/HTTP-wireshark-file2.html, and the request version as HTTP/1.1. The response is a 304 Not Modified status code.

No.	Time	Source	Destination	Protocol	Length	Info
2097	8.385541	192.168.0.105	128.119.245.12	HTTP	466	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
2153	8.515884	128.119.245.12	192.168.0.105	HTTP	784	HTTP/1.1 200 OK (text/html)
2213	8.642946	192.168.0.105	128.119.245.12	HTTP	423	GET /favicon.ico HTTP/1.1
2291	8.780952	128.119.245.12	192.168.0.105	HTTP	539	HTTP/1.1 404 Not Found (text/html)
3827	12.280759	192.168.0.105	128.119.245.12	HTTP	552	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
3876	12.409186	128.119.245.12	192.168.0.105	HTTP	293	HTTP/1.1 304 Not Modified

Frame 3827: 552 bytes on wire (4416 bits) captured (4416 bits) on interface \Device\NPF\_{1F74ECB-0F34-...} Ethernet II, Src: IntelCor\_e0:5f:83 (34:d:f6:e0:5f:83), Dst: Tp-LinkT\_59:20:3e (b0:95:75:59:20:3e) Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12 Transmission Control Protocol, Src Port: 64899, Dst Port: 80, Seq: 1, Ack: 1, Len: 412

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1]

[GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1]

[Severity level: Chat]

[Group: Sequence]

Request Method: GET

Request URI: /wireshark-labs/HTTP-wireshark-file2.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Connection: keep-alive

Upgrade-Insecure-Requests: 1

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

[HTTP request 1/2]

[Response in frame: 2153]

[Next request in frame: 3827]

İkinci dosyayı indirdik tarayıcıma. Sonra sayfayı yeniden yükledik ve paket yakalamayı durdurduk.

HTTP GET satırının içeriğinde if-modified-since ile alakalı hiçbir şey göremedim.

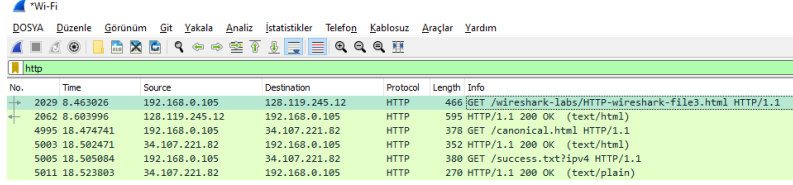
Serverın cevabını incelediğimde dosyanın içeriğini bana gönderdiğini gördüm, çünkü metin verisine dayalı satırda sitenin bana html kodlarını gönderdiğini gördüm.

Sayfayı yeniledikten sonra gönderdiğimiz GET methodunu incelediğimizde IF-MODIFIED-SINCE satırını görmüş olduk. Burada da sitenin son düzenlenme(modified) tarihini görüyoruz.

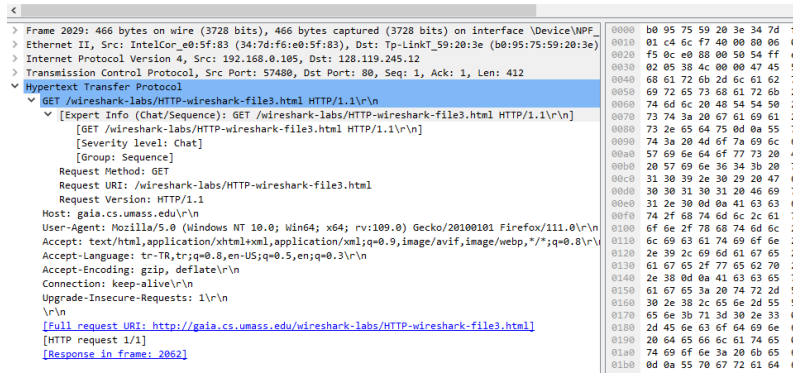
Dönüş aldığımız yanıt kod 304 NOT-MODIFIED yani değiştirilmedi anlamında kod döndürdü. Sitede yeni içerik olmadığı için yeni içerik döndürmedi muhtemelen.

### 3.3 Retrieving Long Documents

Büyük boyutlu dosyaları incelemek için üçüncü siteye tarayıcımızdan giriş yaptık ve Wire Shark uygulamamızdan paketlerini yakaladık aşağıda görüldüğü üzere.



No.	Time	Source	Destination	Protocol	Length	Info
2029	8.463926	128.119.245.12	192.168.0.105	HTTP	466	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
2062	8.603996	128.119.245.12	192.168.0.105	HTTP	595	HTTP/1.1 200 OK (text/html)
4995	18.474741	192.168.0.105	34.107.221.82	HTTP	378	GET /canonical.html HTTP/1.1
5003	18.502471	34.107.221.82	192.168.0.105	HTTP	352	HTTP/1.1 200 OK (text/html)
5005	18.505084	192.168.0.105	34.107.221.82	HTTP	380	GET /success.txt?ip=4 HTTP/1.1
5011	18.523803	34.107.221.82	192.168.0.105	HTTP	270	HTTP/1.1 200 OK (text/plain)



```
<<
> Frame 2029: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface \Device\NPF...
> Ethernet II, Src: IntelCor_e0:5f:83 (34:7d:f6:e0:5f:83), Dst: Tp-LinkT_59:20:3e (b0:95:75:59:20:3e)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 57480, Dst Port: 80, Seq: 1, Ack: 1, Len: 412
> Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n
    [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
    [GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
  Request Method: GET
  Request URI: /wireshark-labs/HTTP-wireshark-file3.html
  Request Version: HTTP/1.1
  Host: gaia.cs.umass.edu\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
  Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  \r\n
  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
  [HTTP request 1/1]
  [Response in frame: 2062]
```

Tarayıcımızdan 2029 numaralı paket 1 tane GET mesajı yolladı.

2062 numaralı paket 200 OK durum koduyla yanıtlandı.

### 3.4 HTML Documents with Embedded Objects

Tarayıcım 3 tane GET mesajı yolladı. Birisi sayfanın başlatılması, diğeri sayfanın logosu ve öbürü ise kitabın fotoğrafı için istek gönderdi.

128.119.245.12 Sayfaya ilk giriş için IP

128.119.245.12 pearson logosu

178.79.137.164 kitabın fotosu

Sayfadaki resimler sırayla indirildi çünkü indirme istekleri sırasıyla gönderilmiş. Aralarında zaman farkı var aynı anda indirilme ihtimali yok.

107	6.359563	192.168.0.105	128.119.245.12	HTTP	423 GET /pearson.png HTTP/1.1
122	6.499262	128.119.245.12	192.168.0.105	HTTP	786 HTTP/1.1 200 OK (PNG)
133	6.562881	192.168.0.105	178.79.137.164	HTTP	390 GET /8E_cover_small.jpg HTTP/1.1

Ekran görüntüsünde belirtildiği gibi GET isteklerinin arasında zaman farkı vardır.

### 3.5 HTTP Authentication

İlk GET mesajı gönderdiğimizde site bize 401 koduyla cevap verdi. Bunun anlamı yetkisiz giriştir. Daha sonra kullanıcı adı ve şifreyi girdiğimizde tarayıcımız bir GET mesajı daha yolladı ve bunun sonucunda site bize OK mesajıyla yanıt verdi.

54	9.019688	192.168.0.105	128.119.245.12	HTTP	482 GET /wireshark-labs/protected_pages/HTTP-wireshark-fil...
58	9.157640	128.119.245.12	192.168.0.105	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)
78	21.306352	192.168.0.105	128.119.245.12	HTTP	541 GET /wireshark-labs/protected_pages/HTTP-wireshark-fil...
81	21.439938	128.119.245.12	192.168.0.105	HTTP	544 HTTP/1.1 200 OK (text/html)

## 4 Kaynakça

Raporumu tamamen verilen pdf ve wireshark üzerinde kendi deneyimlerimle yazdım.