



Laboratuvar Raporu 1

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Özlem Kayıkcı

152120191043

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İçindekiler

2	Giriş.....	3
3	Laboratuvar Uygulaması.....	3
3.1	The Basic HTTP GET/response interaction	3
3.1.1	Version	3
3.1.2	Languages.....	3
3.1.3	IP addresses	3
3.1.4	Return status code	4
3.1.5	Last modified.....	4
3.1.6	Bytes of content.....	4
3.1.7	Headers.....	4
3.2	The HTTP CONDITIONAL GET/response interaction	5
3.2.1	First GET	5
3.2.2	HTML content.....	6
3.2.3	IF-MODIFIED-SINCE.....	6
3.2.4	Second GET response	6
3.3	Retrieving Long Documents.....	7
3.3.1	Number of Request.....	7
3.3.2	Packet with phrase.....	7
3.3.3	Status code question	7
3.3.4	Data-containing TCP segments	7
3.4	HTML Documents with Embedded Objects	7
3.4.1	Number of get request messages in the list	7
3.4.2	Serial or parallel	7
3.5	HTTP Authentication	8
3.5.1	Server's response.....	8
3.5.2	HTTP GET message for the second time.....	8
4	LABORATUVAR UYGULAMASI SONUCU	8

2 Giriş

HTTP (Hyper Text Transfer Protocol), ağ üzerinde kullanılan bir iletişim protokolüdür. HTTP sayesinde ağ üzerindeki web sayfaları görüntülenir. İstemci ile sunucu-server arasındaki iletişim kuralları HTTP protokolü ile belirlenir ve bu ikili arasındaki alışveriş trafiğine bu protokol sayesinde ulaşabiliriz. HTTP protokolu 80 portunu kullanır ve tarayıcı farketmeksizin aranan herhangi bir web sitesi için domain girildikten sonra otomatik olarak başına eklenir. İstemciyle sunucu arasında HTTP sayesinde belli kurallar vardır. HTTP durum kodları, alışveriş sonucunda cevabın başarılı ya da başarısız olduğunu anlamamızda rol oynar.

3 Laboratuvar Uygulaması

3.1 The Basic HTTP GET/response interaction

3.1.1 Version

```
> Frame 2586: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface \Device\NPF_{B26...}
> Ethernet II, Src: Sagemcom_e2:e6:10 (68:15:90:e2:e6:10), Dst: IntelCor_d7:85:ac (5c:87:9c:d7:85:ac)
> Internet Protocol Version 4, Src: 77.234.45.60, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 52485, Seq: 3059, Ack: 1, Len: 467
> [4 Reassembled TCP Segments (3525 bytes): #2569(154), #2570(1452), #2572(1452), #2586(467)]
Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
Content-type: application/octet-stream\r\n
Pragma: no-cache\r\n
Cache-control: no-cache\r\n
Connection: keep-alive\r\n
Transfer-Encoding: chunked\r\n
\r\n
[HTTP response 1/2]
[Next request in frame: 2592]
[Request URI: http://su.ff.avast.com/R/A3sKIDIzN2YyNDA2MjUxNDNRmYTk5Y2ZjZmM3OTdiYTU0MTcyEgQAFwMjGjGCI]
> HTTP chunked response
File Data: 3353 bytes
> Data (3353 bytes)
```

```
Wireshark - Paket 19152 - Wi-Fi
> Transmission Control Protocol, Src Port: 52980, Dst Port: 80, Seq: 1, Ack: 1, Len: 463
Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
Request Method: GET
Request URI: /wireshark-labs/HTTP-wireshark-file1.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-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3\r\n
Accept-Encoding: gzip, deflate\r\n
\r\n
Connection: keep-alive\r\n
0000 68 15 90 e2 e6 10 5c 87 9c d7 85 ac 08 00 45 00 h... \r\n .....E-
0010 01 f7 fc 5e 40 00 80 06 00 00 c0 a8 01 0a 80 77 ...@... ..w
0020 f5 0c ce f4 00 50 5b 54 67 bf f6 17 c4 10 50 18 ....P[T g...P
0030 02 04 39 20 00 00 47 45 54 20 2f 77 69 72 65 73 ...-9--GE T/wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-u
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 ireshark -file1.h
0060 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1.Ho
0070 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas
0080 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e s.edu-U ser-Agen
0090 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
00a0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
00b0 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a Win64; x64; rv:
00c0 31 30 39 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 109.0) G ecko/201
00d0 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 31 31 00101 Fi refox/11
00e0 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 1.0 .Acc ept: tex
00f0 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 t/html,a pplicati
0100 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 on/xhtml+xml,app
0110 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 lication /xml;q=0
```

3.1.2 Languages

3.1.3 IP addresses

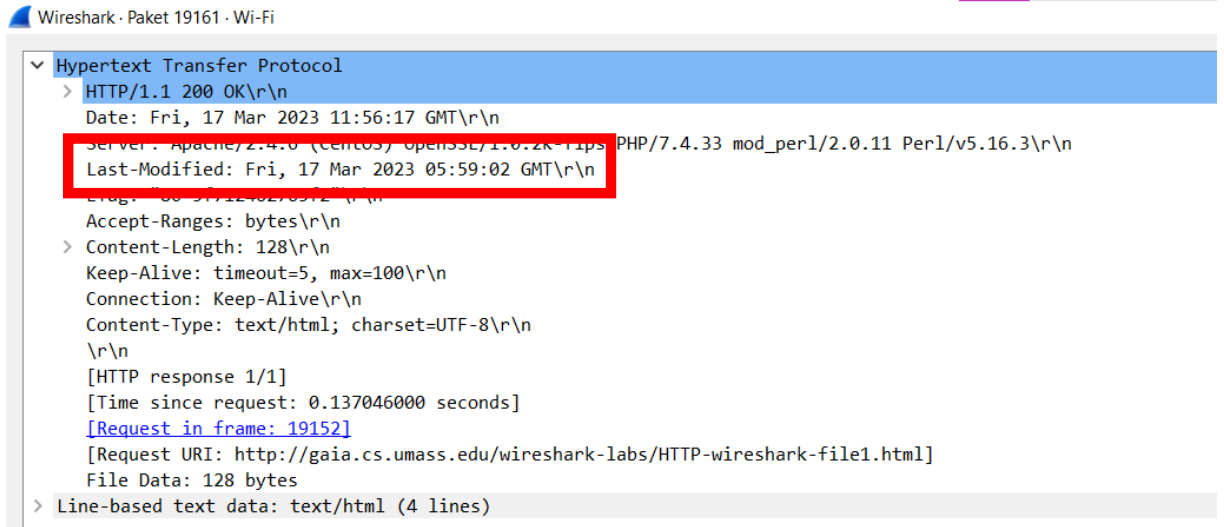
No.	Time	Source	Destination
44789	20:54:18,440969	192.168.1.10	128.119.245.12
1.1			

Bilgisayarımın IP adresi: 192.168.1.10 ve server'ın IP adresi 128.119.245.12 şeklindedir.

3.1.4 Return status code

200 OK, http başarı kodu görülmüştür.

3.1.5 Last modified



3.1.6 Bytes of content

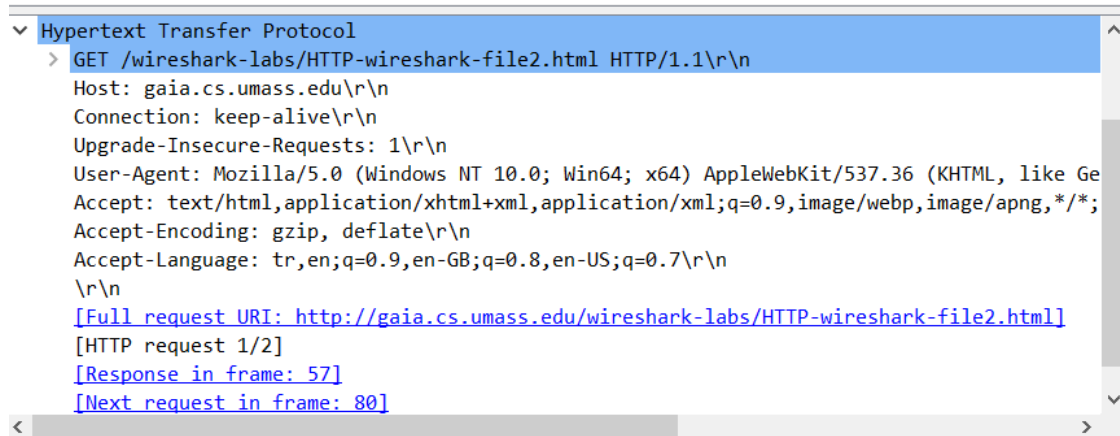


3.1.7 Headers

Veriler içerisinde paket listeleme penceresinin dışında görünen herhangi bir header görülmemiştir.

3.2 The HTTP CONDITIONAL GET/response interaction

3.2.1 First GET



Last modified değerine rastlanılmamıştır.

3.2.2 HTML content

```
\r\n
[HTTP response 1/2]
[Time since request: 0.146341000 seconds]
[Request in frame: 42]
[Next request in frame: 80]
[Next response in frame: 120]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
File Data: 371 bytes
▼ Line-based text data: text/html (10 lines)
  \n
  <html>\n
  \n
  Congratulations again! Now you've downloaded the file lab2-2.html. <br>\n
  This file's last modification date will not change. <p>\n
  Thus if you download this multiple times on your browser, a complete copy <br>\n
  will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE<br>\n
  field in your browser's HTTP GET request to the server.\n
  \n
  </html>\n
```

3.2.3 IF-MODIFIED-SINCE

```
▼ Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\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)
    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,en;q=0.9,en-GB;q=0.8,en-US;q=0.7\r\n
    If-None-Match: "173-5f71246275a3a"\r\n
    If-Modified-Since: Fri, 17 Mar 2023 05:59:02 GMT\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
    [HTTP request 1/1]
```

3.2.4 Second GET response

```
> Frame 213: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{B2607407-1B85-4DD5-BC71-915DC00AF9A8},
> Ethernet II, Src: Sagemcom_e2:e6:10 (68:15:90:e2:e6:10), Dst: IntelCor_d7:85:ac (5c:87:9c:d7:85:ac)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.10
> Transmission Control Protocol, Src Port: 80, Dst Port: 49367, Seq: 1, Ack: 613, Len: 240
▼ Hypertext Transfer Protocol
  > HTTP/1.1 304 Not Modified\r\n
    Date: Fri, 17 Mar 2023 19:23:10 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "173-5f71246275a3a"\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.150538000 seconds]
    [Request in frame: 206]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

304 Not Modified cevabını aldıktan sonra herhangi bir html/text 'e ulaşılmamıştır.

3.3 Retrieving Long Documents

3.3.1 Number of Request

Yalnızca 1 tane http GET istek mesajı gönderilmiştir ve 87. satırda bulunmaktadır.

No.	Time	Source	Destination	Protocol	Length	Info
74	22:40:18,810416	192.168.1.10	20.189.173.3	TCP	1494	49400 → 443 [ACK] Seq=21728 Ack=1801 Win=517 Len=1440 [TCP segment of a reassembled PDU]
75	22:40:18,810416	192.168.1.10	20.189.173.3	TCP	1494	49400 → 443 [ACK] Seq=23168 Ack=1801 Win=517 Len=1440 [TCP segment of a reassembled PDU]
76	22:40:18,810416	192.168.1.10	20.189.173.3	TCP	1494	49400 → 443 [ACK] Seq=24608 Ack=1801 Win=517 Len=1440 [TCP segment of a reassembled PDU]
77	22:40:18,810416	192.168.1.10	20.189.173.3	TLSv1.2	1400	Application Data
78	22:40:18,830412	192.168.1.10	128.119.245.12	TCP	66	49416 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
84	22:40:18,882350	192.168.1.10	20.86.249.62	TCP	66	49417 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
85	22:40:18,911050	128.119.245.12	192.168.1.10	TCP	66	80 → 49415 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
86	22:40:18,911757	192.168.1.10	128.119.245.12	TCP	54	49415 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
87	22:40:18,914949	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
88	22:40:18,951436	20.86.249.62	192.168.1.10	TCP	66	443 → 49417 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM
89	22:40:18,951743	192.168.1.10	20.86.249.62	TCP	54	49417 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
90	22:40:18,954128	192.168.1.10	20.86.249.62	TLSv1.2	571	Client Hello
91	22:40:19,011143	128.119.245.12	192.168.1.10	TCP	66	80 → 49416 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1452 SACK_PERM WS=128
92	22:40:19,011732	192.168.1.10	128.119.245.12	TCP	54	49416 → 80 [ACK] Seq=1 Ack=1 Win=132096 Len=0
93	22:40:19,060403	20.86.249.62	192.168.1.10	TCP	1506	443 → 49417 [ACK] Seq=1 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
94	22:40:19,061595	20.86.249.62	192.168.1.10	TCP	1506	443 → 49417 [ACK] Seq=1453 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
95	22:40:19,061595	20.86.249.62	192.168.1.10	TCP	1506	443 → 49417 [ACK] Seq=2905 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
96	22:40:19,061595	20.86.249.62	192.168.1.10	TCP	1506	443 → 49417 [ACK] Seq=4357 Ack=518 Win=525056 Len=1452 [TCP segment of a reassembled PDU]
97	22:40:19,061595	20.86.249.62	192.168.1.10	TLSv1.2	1387	Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hello Done

3.3.2 Packet with phrase

106.satırdaki paket istenilen özellikleri karşılayan pakettir.

105	22:40:19,114659	192.168.1.10	20.189.173.3	TCP	54	49400 → 443 [ACK] Seq=27394 Ack=2701 Win=513 Len=0
106	22:40:19,117286	128.119.245.12	192.168.1.10	TCP	1506	80 → 49415 [ACK] Seq=1 Ack=501 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
107	22:40:19,117286	128.119.245.12	192.168.1.10	TCP	1506	80 → 49415 [ACK] Seq=1453 Ack=501 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
108	22:40:19,117286	128.119.245.12	192.168.1.10	TCP	1506	80 → 49415 [ACK] Seq=2905 Ack=501 Win=30336 Len=1452 [TCP segment of a reassembled PDU]
109	22:40:19,117286	128.119.245.12	192.168.1.10	HTTP	559	HTTP/1.1 200 OK (text/html)
110	22:40:19,117879	192.168.1.10	128.119.245.12	TCP	54	49415 → 80 [ACK] Seq=501 Ack=4862 Win=132096 Len=0
111	22:40:19,134622	20.86.249.62	192.168.1.10	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
112	22:40:19,136629	192.168.1.10	20.86.249.62	TLSv1.2	1494	Application Data

3.3.3 Status code question

200 OK http durum koduna rastlanılmıştır.

3.3.4 Data-containing TCP segments

3 paket (106,107 ve 108.numaralı paketler) verileri taşıyan TCP segmentleridir.

3.4 HTML Documents with Embedded Objects

3.4.1 Number of get request messages in the list

3 adet http GET istek mesajı gönderilmiştir (307,323,393). Sayfa ve logo 128.119.245.12 adresine gönderilirken, jpg dosyası 178.79.137.164 adresine gönderilmiştir.

No.	Time	Source	Destination	Protocol	Length	Info
307	01:25:14,322833	192.168.1.10	128.119.245.12	HTTP	554	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
322	01:25:14,466927	128.119.245.12	192.168.1.10	HTTP	1355	HTTP/1.1 200 OK (text/html)
323	01:25:14,491164	192.168.1.10	128.119.245.12	HTTP	500	GET /pearson.png HTTP/1.1
356	01:25:14,637497	128.119.245.12	192.168.1.10	HTTP	761	HTTP/1.1 200 OK (PNG)
393	01:25:15,038515	192.168.1.10	178.79.137.164	HTTP	467	GET /8E_cover_small.jpg HTTP/1.1
397	01:25:15,107155	178.79.137.164	192.168.1.10	HTTP	225	HTTP/1.1 301 Moved Permanently

3.4.2 Serial or parallel

İndirmeler seri olarak gerçekleşmiştir ; 323 numaralı paketteki GET isteği 356 numaralı pakette OK cevabını almış, 393 numaralı GET isteği 397 numaralı pakette OK cevabını almıştır.

3.5 HTTP Authentication

3.5.1 Server's response

401 Unauthorized dönütü alındı.

```
HTTP 572 GET /wireshark-labs/protected_pages/HTTP-wireshark%02file5.html HTTP/1.1
HTTP 771 HTTP/1.1 401 Unauthorized (text/html)
```

3.5.2 HTTP GET message for the second time

```
Cache-Control: max-age=0\r\n
> Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzM5ldHdvcms=\r\n
Upgrade-Insecure-Requests: 1\r\n
Host: Assets: Main-111-15-0-4/Modified: NT 10 0: 15-04-2020 15:37:36 /101
```

Username ve password girildikten sonra Authorization :Basic görülmüştür.

4 LABORATUVAR UYGULAMASI SONUCU

1.bölüm, The basic http get başlığı altında yapılan uygulama sonucunda, browser'ın kullandığı HTTP versiyonunu, kabul edilen dilleri, source olarak isteği IP adresim üzerinden Server yani destination olarak isteğin server IP adresine yönlendiğini ve server'ın bu uygulama sonucu gidişatla ilgili response olarak 200 OK http durum kodunu gönderdiği başarı kodu sonucunda yüklenen dosyanın boyutuna da ulaşılabilceği gözlemlenmiştir.

2.bölüm, The http conditional get başlığı altında yapılan uygulama sonucunda, cache sunucusu get mesajını asıl sunucuya gönderir ve oradan bir response alır. Cache, response ile dönen nesnenin değiştirme tarihi ve ayrıca nesneyi yerelde tutar.Başka bir zaman diliminde nesnenin tekrar talep edilmesi halinde halihazırda cache'de tutulan bilgilerin güncelliğini, değiştirilip değiştirilmediğini anlamak için last-modified ve If-modified-since değerlerine bakılır. İki değer aynıysa değişim yoktur ve cache'in yerelinden nesnenin kopyası çekilir eğer iki değer birbirinden farklı ise yani nesne üzerinde değişim mevcutsa asıl sunucuya tekrar ulaşılır ve 200 OK http kodu döner.Herhangi bir değişim olmaması halinde 304 Not Modified http kodu döndürülecektir, bu durumda nesnenin wireshark ortamında tekrar gönderimi de görülmemiştir.

3. bölüm, Retrieving Long Documents başlığı altında yapılan uygulama sonucunda, belgelerin ve bilgilerin aktarımını sağlama inceleme fırsatı bulunmuştur, TCP segmentleri bu görevde görmekteyiz.

4.bölüm, HTML Documents with Embedded Objects başlığı altında yapılan uygulama sonucunda, gömülü objelerin iletimi sırasındaki iletişim incelenmiştir, bu sırada farklı objelerin farklı destinasyon adreslerine gönderimi olmuş, indirmelerin seri ya da paralel olarak gerçekleşmiş olması incelenmiştir.

5.bölüm, HTTP Authentication başlığı altında yapılan uygulama sonucunda, yetkilendirme olması dahilinde yetkili ve henüz yetkilendirilmemiş haldeki dönütler incelenmiştir.