Laboratuvar Raporu 1

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Özlem Kayıkcı

152120191043

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İçindekiler

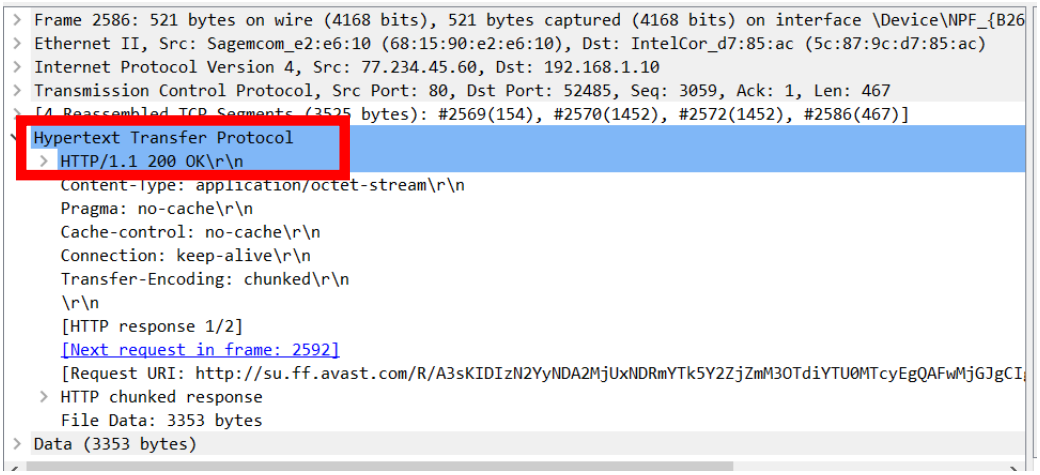
2 Giriş

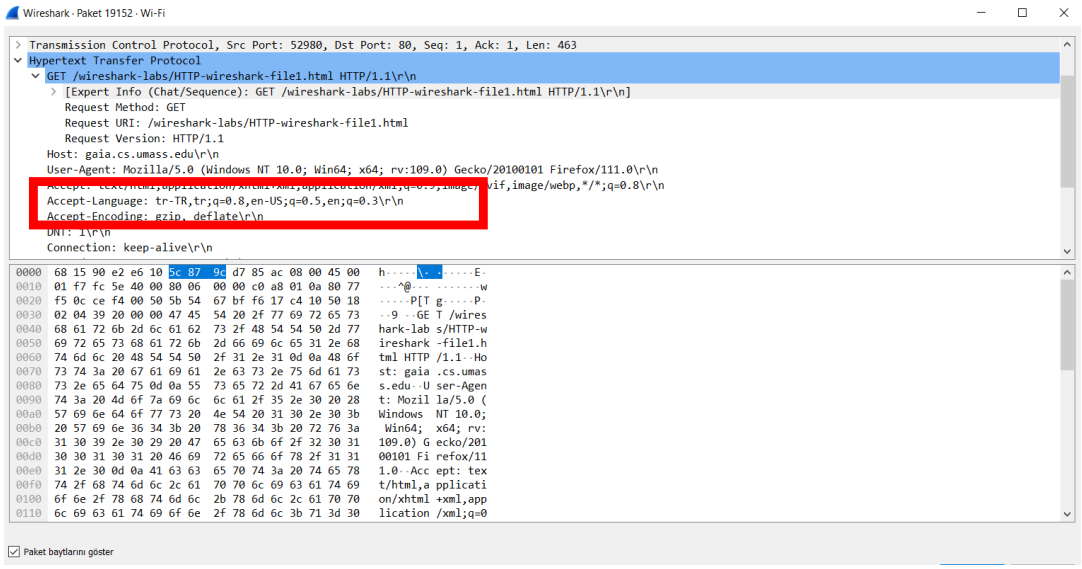
HTTP (Hyper Text Transfer Protocol), ağ üzerinde kullanılan bir iletişim protokolüdür. HTTP sayesinde ağı üzerindeki web sayfaları görüntülenir. İstemci ile sunucu-server arasındaki iletişim kuralları HTTP protokolü ile belirlenir ve bu ikili arasındaki alışveriş trafiğine bu protokol sayesinde ulaşabiliriz. HTTP protokolu 80 portunu kullanır ve tarayıcı farketmeksizin aranılan 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

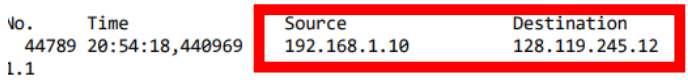
3.1.1 Version





3.1.2 Languages

3.1.3 IP addresses

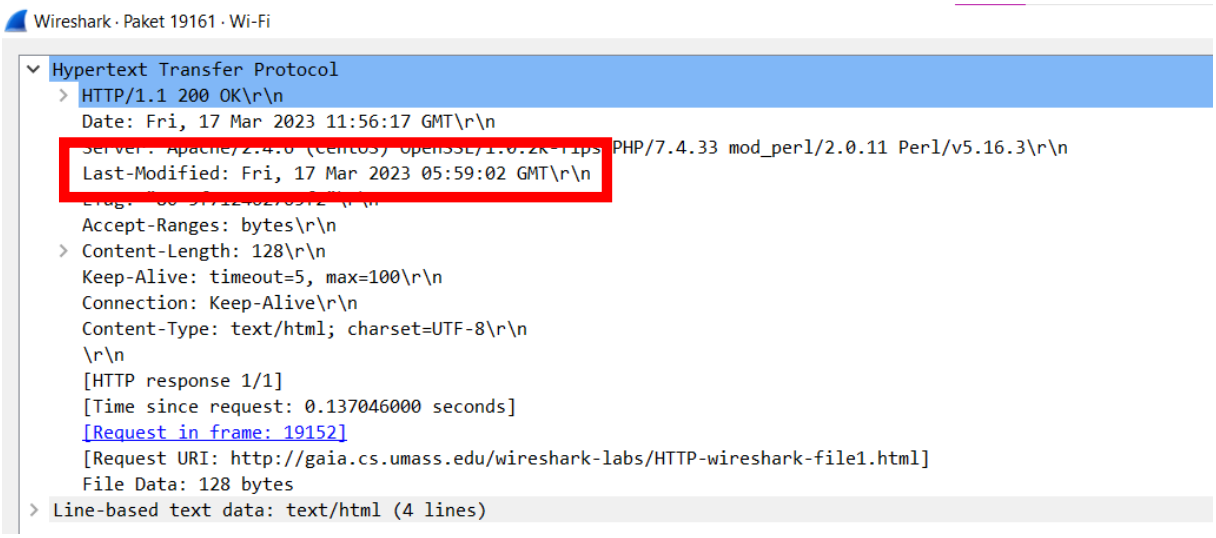


Bilgisayarımın IP adresi: 192.168.1.10 ve server'in IP adresi 128.119.245.12 şeklindedir.

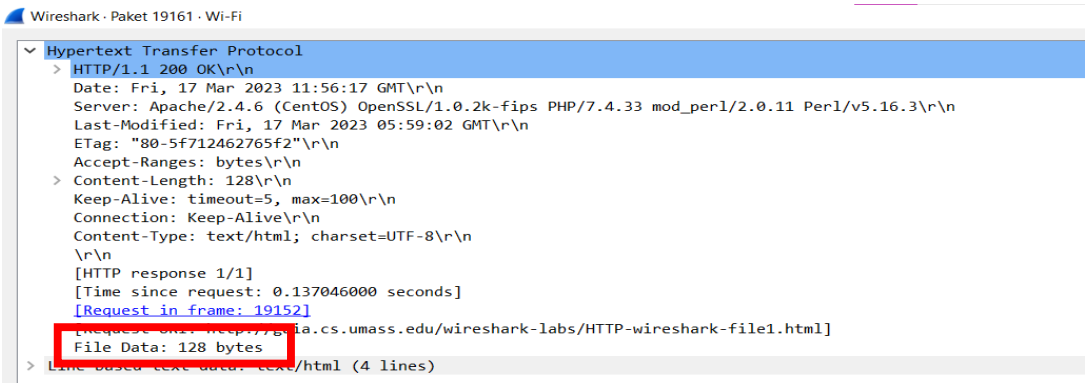
3.1.4 Return status code

200 OK, http başarı kodu görülmüştür.

3.1.5 Last modified



3.1.6 Bytes of content

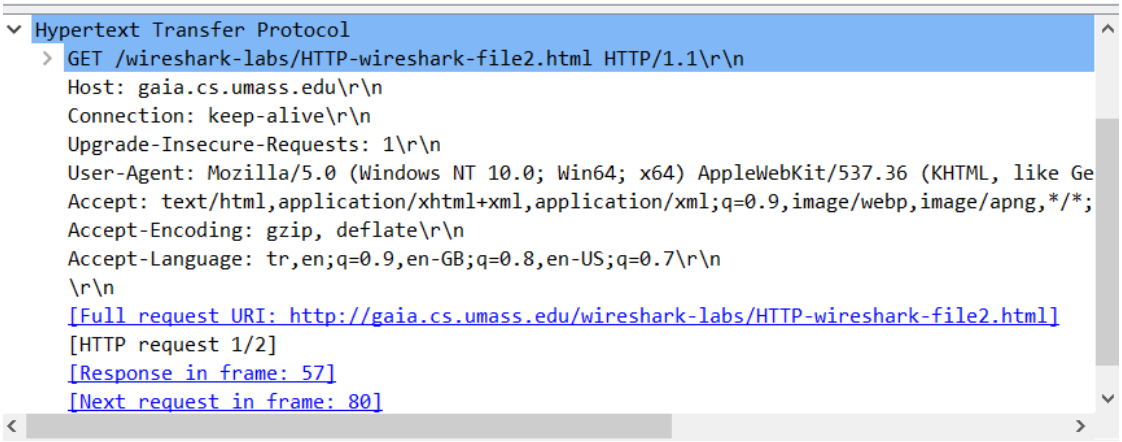


3.1.7 Headers

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

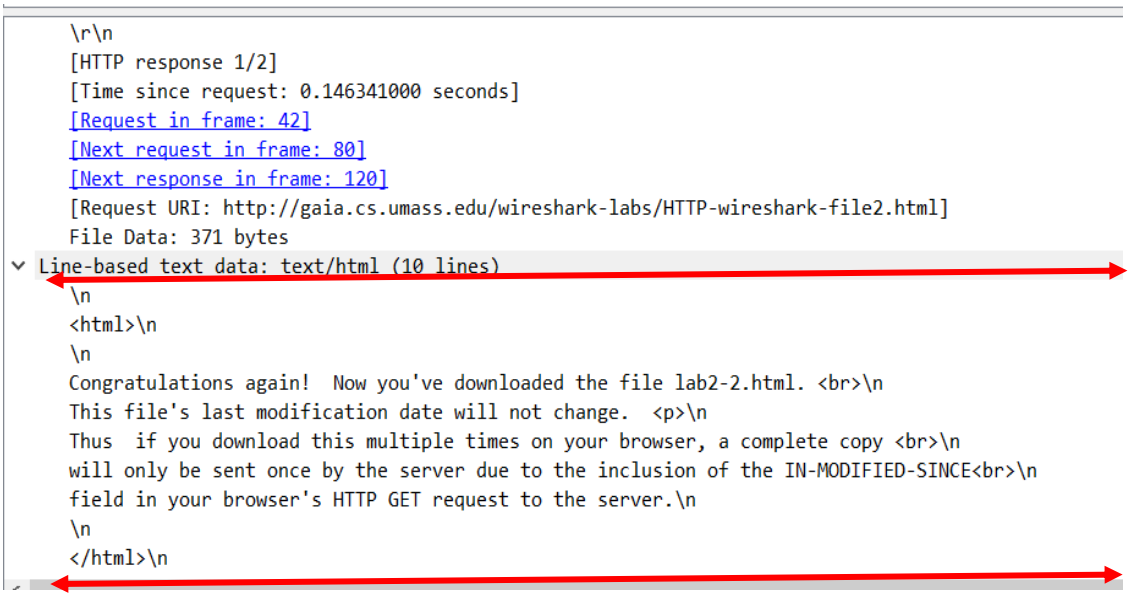
3.2 The HTTP CONDITIONAL GET/response interaction

3.2.1 First GET

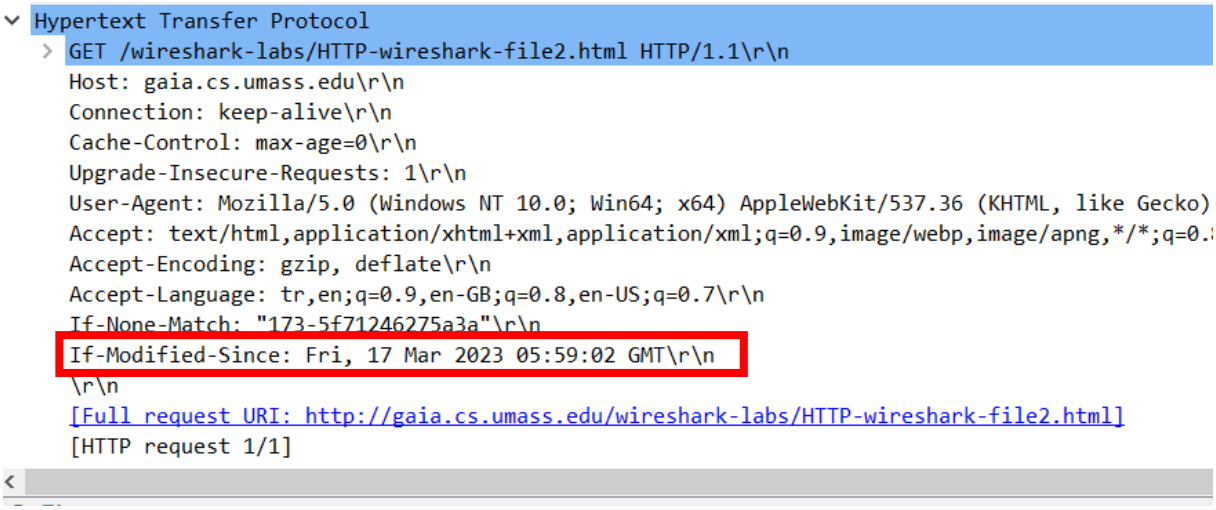


Last modified değerine rastlanılmamıştır.

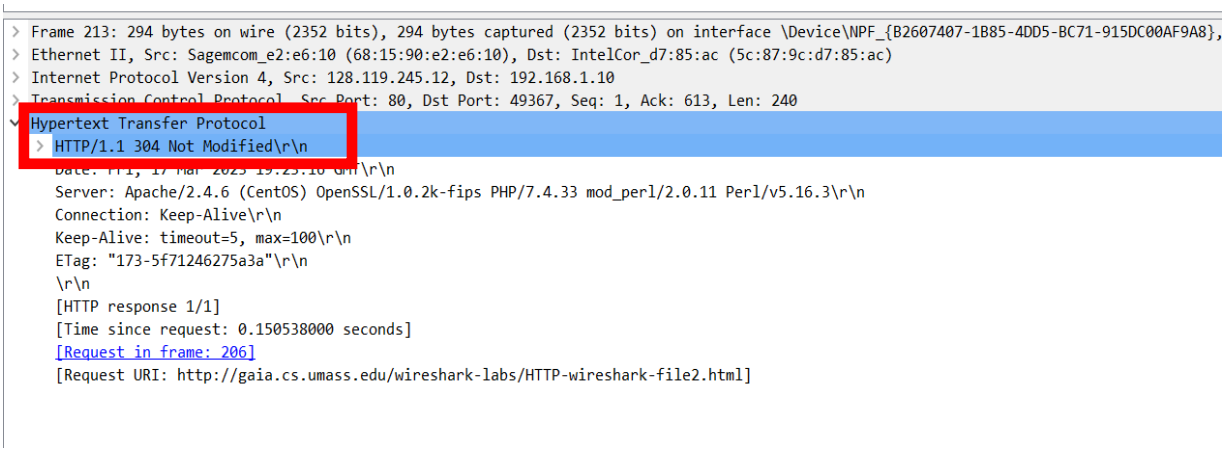
3.2.2 HTML content



3.2.3 IF-MODIFIED-SINCE



3.2.4 Second GET response

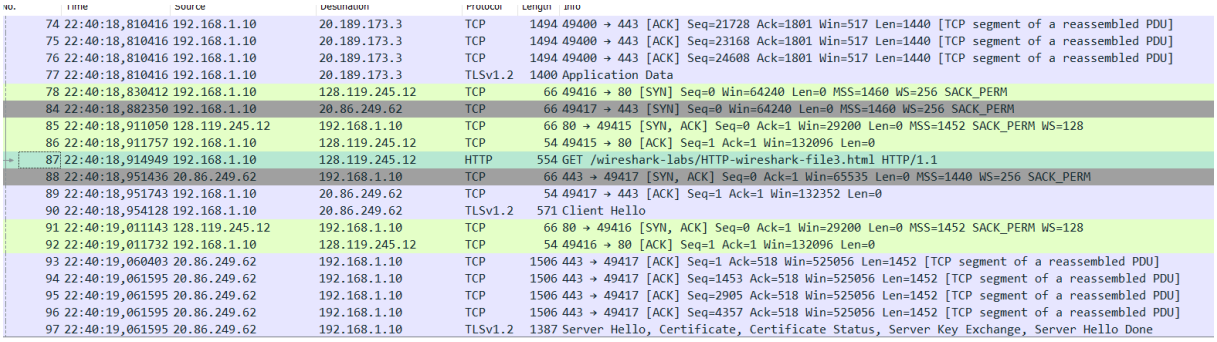


304 Not Modified cevabını aldıktan sonra herhangi bir html/text ‘e ulaşılmamıştır.

3.3 Retrieving Long Documents

3.3.1 Number of Request

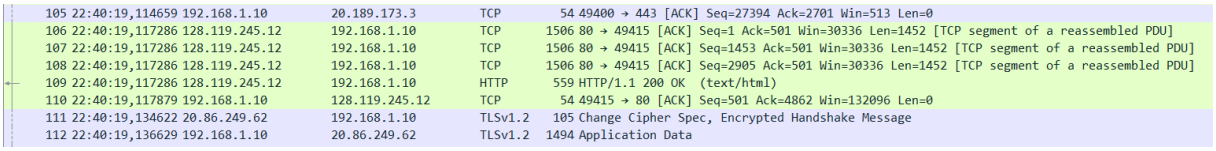
Yalnızca 1 tane http GET istek mesajı gönderilmiştir ve 87. satırda bulunmaktadır.



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.



No.	Time	Source	Destination	Protocol	Length	Info
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.

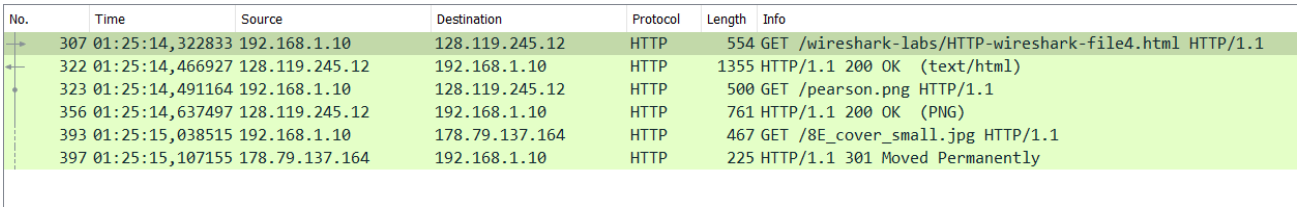
3.3.4 Data-containing TCP segments

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

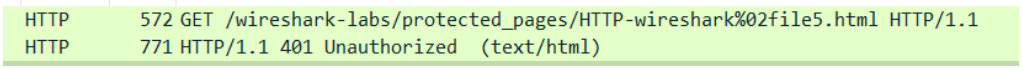
3.4.2 Serial or parallel

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.

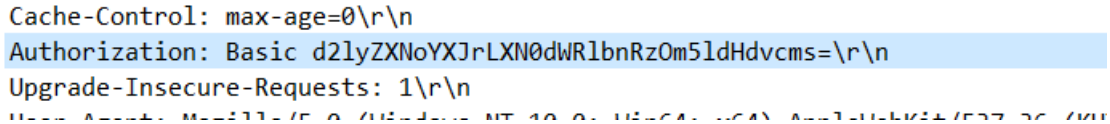
3.5 HTTP Authentication

3.5.1 Server's response

401 Unauthorized dönütü alındı.



3.5.2 HTTP GET message for the second time



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 ulaşılabileceği gözlemlenmiştir.

2.bölüm ,The http condıtıonal 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.