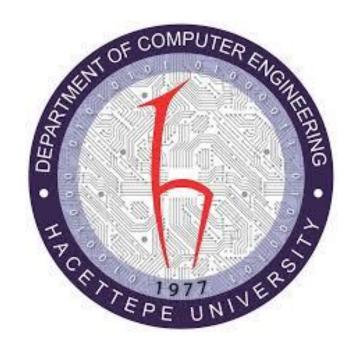
# HACETTEPE UNIVERSITY COMPUTER ENGINEERING DEPARTMENT COMPUTER NETWORKS LABORATORY



**EXPERIMENT: HTTP** 

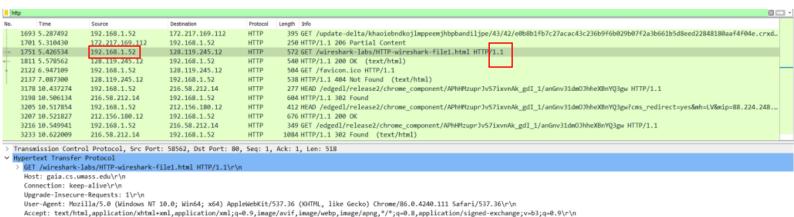
Deniz Ece AKTAŞ 21626901

Ece OMURTAY 21627543

**GROUP NUMBER: 12** 

# 1. The Basic HTTP GET/response interaction

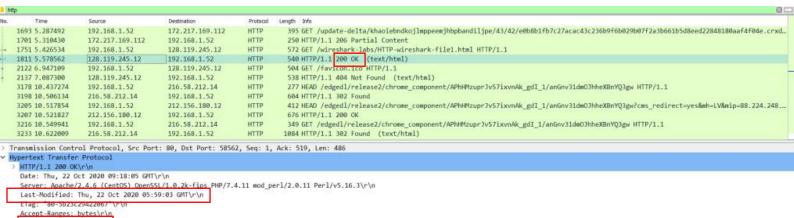
1. Our browser is running on HTTP version of 1.1



- Accept-Encoding: gzip, deflate\r\n
  Accept-Language: tr-TR,tr;q=0.9,pl-PL;q=0.8,pl;q=0.7,en-US;q=0.6,en;q=0.5\r\n
  \r\n

  [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

  [HTTP request 1/2]
  - 2. Our browser indicates tr-TR, pl-PL and en-US as languages
  - 3. IP address of our source(our) computer is 192.168.1.52.
  - 4. 200 is returned as status code from server to our browser.



- 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
  - - 6. 128 bytes of content are being returned from gaia.cs.umass.edu server to our browser.
    - 7. We do not see any other HTTP message in the packet-listing window.

5. This HTML file was modified on 22 Oct 2020 at the server.

# 2. The HTTP CONDITIONAL GET/response interaction

8. There is no IF-MODIFIED-SINCE line in HTTP GET.

1396 6.223912

1441 6.368571

1888 8.431300

192.168.1.52

128.119.245.12

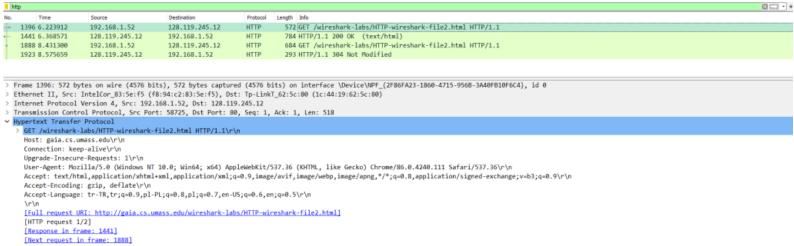
128.119.245.12

192.168.1.52

128.119.245.12

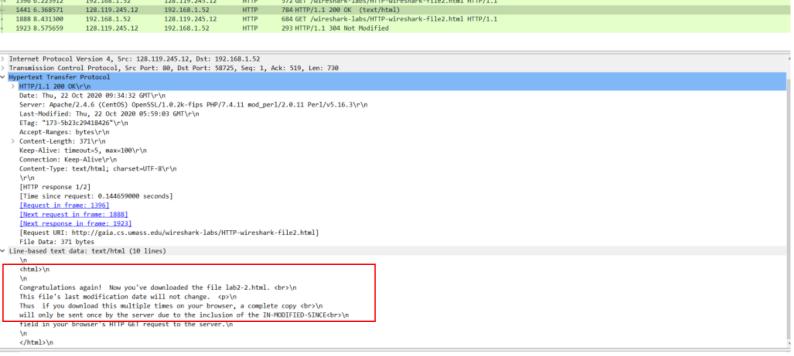
нттр

HTTP

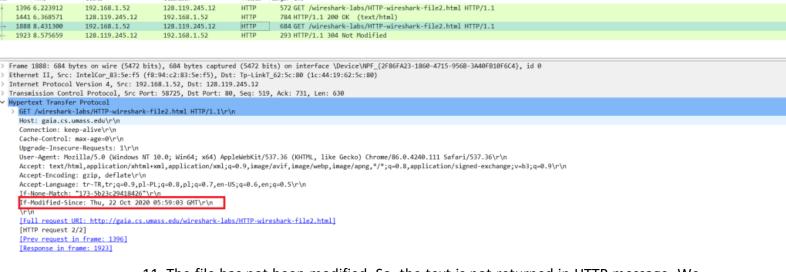


9. The server responded with the contents of the file to the first GET and we can tell this by the screenshot below

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



10. Second GET message has IF-MODIFIED-SINCE line. File is modified in 22 Oct 2020. It can be seen in screenshot below.



11. The file has not been modified. So, the text is not returned in HTTP message. We can tell this by the following screenshot.

```
1441 6.368571
                         128.119.245.12
                                                   192.168.1.52
                                                                             HTTP
                                                                                          784 HTTP/1.1 200 OK (text/html)
684 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
  1888 8,431306
                                                   128.119.245.12
                                                                             нттр
  1923 8.575659
                         128.119.245.12
                                                   192.168.1.52
                                                                             HTTP
                                                                                          293 HTTP/1.1 304 Not Modified
Frame 1923: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF (2F86FA23-1860-4715-956B-3A40FB10F6C4), id 0
                      Tp-LinkT_62:5c:80 (1c:44:19:62:5c:80), Dst: IntelCor_83:5e:f5 (f8:94:c2:83:5e:f5)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.52
Transmission Control Protocol, Src Port: 80, Dst Port: 58725, Seq: 731, Ack: 1149, Len: 239
Hypertext Transfer Protocol
> HTTP/1.1 384 Not Modified\r\n
Date: Thu, 22 Oct 2020 09:34:34 GMT\r\n
   Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\n
   Connection: Keep-Alive\r\n
```

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

```
Date: Inu, 22 Oct 2020 09:34:34 GMT\r\n
Server: Apache/2.4.6 ((ent05) OpenSSL/1.0.2k-fips PHP/7.4.11 mod_perl/2.0.11 Perl/v5.16.3\r\
Connection: Keep-Alive\r\n
Keep-Alive: timeout=5, max=99\r\n
ETag: "173-5b33c29418426"\r\n
Ir\n
Ir\n
IHITP response 2/2
[Time since request: 0.144359000 seconds]
IPrev request in frame: 13961
IPrev response in frame: 1441]
IRequest in frame: 1888]
[Request URI: http://geia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

128.119.245.12

1396 6.223912

192.168.1.52

### 3. Retrieving Long Documents

12. Since the document is so long, HTTP is divided into TCP packets. Only 1 GET request message is sent from our browser. GET message is on packet 1323. OK message is on packet 1364.

```
1273 4.665753
                         192.168.1.52
                                                   128.119.245.12
128.119.245.12
                                                                              TCP
                                                                                            66 58835 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1275 4.666086
                                                                                            66 58836 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
                         192,168,1,52
                                                                              TCP
                                                                                          141 Application Data
54 443 + 58809 [ACK] Seq-58 Ack-584 Win-68 Len-0
66 80 + 58836 [SYN, ACK] Seq-0 Ack-1 Win-29200 Len-0 MSS-1460 SACK_PERM-1 WS-128
54 58836 + 80 [ACK] Seq-1 Ack-1 Win-131328 Len-0
 1308 4.766336
                         192.168.1.52
                                                   162.159.138.234
 1313 4.778802
                         162.159.138.234
                                                   192.168.1.52
                                                                              TCP
 1321 4.804518
                         128.119.245.12
                                                   192.168.1.52
                                                   128.119.245.12
  1322 4.804609
                         192.168.1.52
                                                                              TCP
1323 4.805179
                         192,168.1.52
                                                   128.119.245.12
                                                                              нттр
                                                                                          572 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
                                                                                           66 80 + 58835 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 54 58835 + 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 54 80 + 58836 [ACK] Seq=1 Ack=519 Win=30336 Len=0
 1324 4.809437
                         128.119.245.12
                                                   192,168,1,52
                                                                              TCP
 1325 4.809495
1359 4.944795
                         192.168.1.52
                                                   128.119.245.12
                         128, 119, 245, 12
                                                   192,168,1,52
                                                                              TCP
  1363 4.954282
                         128.119.245.12
                                                   192.168.1.52
                                                                                         4410 80 + 58836 [ACK] Seq=1 Ack=519 Win=30336 Len=4356 [TCP segment of a reassembled PDU]
1364 4.954282
1365 4.954347
                         128,119,245,12
                                                   192.168.1.52
                                                                             HTTP
                                                                                          559 HTTP/1.1 200 OK (text/html)
                         192.168.1.52
                                                   128.119.245.12
                                                                                            54 58836 → 80 [ACK] Seq=519 Ack=4862 Win=131328 Len=0
 1487 5.299866
                         192.168.1.52
                                                   162.159.138.234
                                                                             TLSv1.2 141 Application Data
```

13. Packet 1363.

```
66 58836 + 80 [SYN] Seq=0 Win-64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
66 58836 + 80 [SYN] Seq=0 Win-64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 1273 4.665753
                         192.168.1.52
                                                    128.119.245.12
 1275 4.666086
                         192,168,1,52
                                                    128, 119, 245, 12
                                                                               TCP
                                                                                            54 443 + 58809 [ACK] Seq=58 Ack=584 Win=68 Len=0
66 80 + 58836 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len
 1313 4.778802
                         162,159,138,234
                                                    192,168,1,52
                                                                               TCP
                         128.119.245.12
 1321 4.804518
                                                    192.168.1.52
                                                                              TCP
                                                                                                                                                              -0 MSS=1460 SACK PERM=1 WS=128
                                                                              TCP 54 58836 + 80 [ACK] Seq-1 Ack=1 Win=131328 Len=0
HTTP 572 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
 1322 4.804609
                         192,168,1,52
                                                    128, 119, 245, 12
 1323 4.805179
                         192,168.1.52
                                                   128.119.245.12
                                                                                            66 80 + 58835 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128 54 58835 + 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 1324 4.809437
                         128.119.245.12
                                                    192.168.1.52
                                                    128,119,245,12
                                                                              TCP
 1325 4,809495
                         192,168,1,52
                                                                                          54 80 + 58836 [ACK] Seq=1 Ack=519 Win=30336 Len=0
4410 80 + 58836 [ACK] Seq=1 Ack=519 Win=30336 Len=4356 [TCP segment of a reassembled PDU]
                         128.119.245.12
                                                                               TEP
1363 4.954282
                         128, 119, 245, 12
                                                    192,168,1,52
                                                                               TCP
                         128.119.245.12
                                                    192.168.1.52
                                                                              HTTP
                                                                                           559 HTTP/1.1 200 OK (text/html)
                                                                                             54 58836 → 80 [ACK] Seq=519 Ack=4862 Win=131328 Len
 1365 4.954347
                         192,168,1,52
                                                    128.119.245.12
                                                                               TCP
 1487 5.299066
                         192.168.1.52
                                                    162.159.138.234
                                                                              TLSv1.2 141 Application Data
```

14. 200-OK.

```
1273 4.665753
                       192.168.1.52
                                                                            TCP
                                                                                          66 58835 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1
                                                 128.119.245.12
                                                                                          66 58836 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1275 4.666086
                                                 128.119.245.12
                                                                           TL5v1.2
1308 4.766336
                       192,168,1,52
                                                 162, 159, 138, 234
                                                                                        141 Application Data
1313 4.778802
                                                                                          54 443 + 58809 [ACK] Seq=58 Ack=584 Win=68 Len=0
                                                                           TCP 66 80 + 58836 [SYN, ACK] Seq-0 Ack-1 Win-29200 Len-0 MSS-1460 SACK_PERM-1 WS-128
TCP 54 58836 + 80 [ACK] Seq-1 Ack-1 Win-131328 Len-0
HTTP 572 GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
1321 4.804518
                       128.119.245.12
                                                 192.168.1.52
                                                  128.119.245.12
1323 4.805179
                       192,168,1,52
                                                 128.119.245.12
                                                                                          66 80 + 58835 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M5S=1460 SACK_PERM=1 WS=128
1324 4.809437
                       128.119.245.12
                                                 192.168.1.52
                                                                                         54 58835 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
54 80 → 58836 [ACK] Seq=1 Ack=519 Win=30336 Len=0
1325 4.809495
                       192.168.1.52
                                                 128, 119, 245, 12
                                                                            TCP
                       128.119.245.12
1359 4.944795
                                                 192.168.1.52
                                                                                       4410 80 → 58836 [ACK] Seq=1 Ack=519 Win=30336 Len=4356 [TCP segment of a reassembled PDU]
559 HTTP/1.1 200 OK (text/html)
54 58836 → 80 [ACK] Seq=519 Ack=4862 Win=131328 Len=0
1363 4 954282
                       128,119,245,12
                                                 192,168,1,52
                                                                            TCP
                       128.119.245.12
1364 4.954282
                                                                           HTTP
                                                 192.168.1.52
1365 4.954347
                       192,168,1,52
                                                 128,119,245,12
                                                                            TCP
                                                                           TLSv1.2 141 Application Data
1487 5.299066
                                                 162.159.138.234
                       192.168.1.52
```

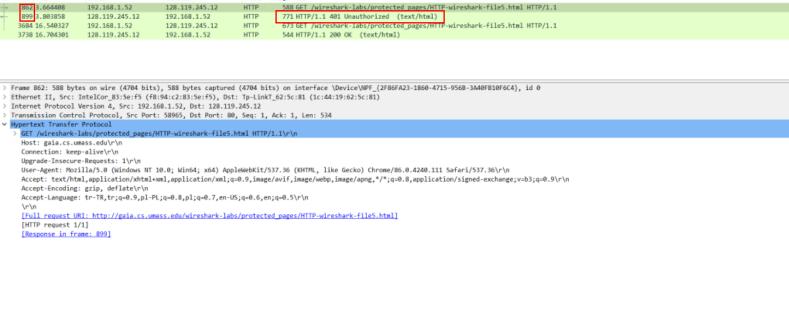
- 15. There is only one TCP segment. It is in packet 1363.
- 4. HTML Documents with Embedded Objects
  - 16. Our browser sent 3 HTTP GET messages: packet 1005 base file -, packet 1083 Pearson logo and packet 1188 textbook cover -. GET message is sent to the same IP addresses so the pictures come from the same server.

No.	Time	Source	Destination	Protocol	Length Info
- :	005 3.949691	192.168.1.52	128.119.245.12	HTTP	572 GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
. ;	053 4.101156	128.119.245.12	192.168.1.52	HTTP	1127 HTTP/1.1 200 OK (text/html)
+ :	083 4.223159	192.168.1.52	128.119.245.12	HTTP	504 GET /pearson.png HTTP/1.1
	124 4.372004	128.119.245.12	192.168.1.52	HTTP	761 HTTP/1.1 200 OK (PNG)
	188 4.544428	192.168.1.52	128.119.245.12	HTTP	478 GET /~kurose/cover_5th_ed.jpg HTTP/1.1
	314 4.980528	128.119.245.12	192.168.1.52	HTTP	1184 HTTP/1.1 200 OK (JPEG JFIF image)

17. The images are downloaded serially in our browser. HTTP messages are between the GET messages. First image was requested and sent before the second image, and so on. We can understand this from first images get packet is 1083 and its OK reply is sent on 1124 packet, the second images GET is sent on 1188 packet and it's reply is gotten on 1314 packet so they don't happen simultaneously.

### 5. HTML Authentication

18. Packet 862 is the GET message, packet 899 is the server's reply message which is Unauthorized. If authorization is needed on a page, 401 unauthorized message is returned after the first get and then after filling the necessary areas like passwords the get message is sent a second time and if the authorized is correct then OK message is displayed.



## 19. The new message is Authorization: Basic

No.		Time	Source	Destination	Protocol	Length Info						
	862	3.664408	192.168.1.52	128.119.245.12	HTTP	588 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1						
	899	3.803858	128.119.245.12	192.168.1.52	HTTP	771 HTTP/1.1 401 Unauthorized (text/html)						
-	3684	16.540327	192.168.1.52	128.119.245.12	HTTP	673 GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1						
+	3738	16.704301	128.119.245.12	192.168.1.52	HTTP	544 HTTP/1.1 200 OK (text/html)						
	[TCP Segment Len: 619]											
Sequence number: 1 (relative sequence number)												
	Sequence number (raw): 761427631											
	[Nex	t sequence nur										
Acknowledgment number: 1 (relative ack number) Acknowledgment number (raw): 2495211382												
											0101 = Header Length: 20 bytes (5)	

> Flags: 0x018 (PSH, ACK)
Window size value: 513
[Calculated window size: 131328]

[Calculated window size: 191328]
[Window size scaling factor: 256]
Checksum: 0x0e02 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]

TCP payload (619 bytes)

[Timestamps]

Time

Destination

Protocol

Length Info

Hypertext Transfer Protocol
> GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.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 Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\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/86.0.4240.111 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q-0.9,image/avif,image/webp,image/apng,\*/\*;q-0.8,application/xigned-exchange;v-b3;q-0.9\r\n

Accept-Encoding: gzip, deflate\r\n Accept-Language: tr-TR,tr;q=0.9,pl-PL;q=0.8,pl;q=0.7,en-US;q=0.6,en;q=0.5\r\n

\r\n