

Melissa Jost  
915842777  
Section A03

Roberto Lozano  
914294300  
Section A01

# Wireshark Lab: HTTP

## 1. The Basic HTTP GET/response interaction

Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	Time	Source	Destination	Protocol	Length	Info
380	7.066249	192.168.1.69	128.119.245.12	HTTP	517	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
382	7.164547	128.119.245.12	192.168.1.69	HTTP	540	HTTP/1.1 200 OK (text/html)
396	7.192160	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
425	7.287757	128.119.245.12	192.168.1.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)

> Frame 380: 517 bytes on wire (4136 bits), 517 bytes captured (4136 bits) on interface \Device\NPF\_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0  
 > Ethernet II, Src: Apple\_ca:30:19 (c4:b3:01:ca:30:19), Dst: ARRISGro\_7f:d6:c0 (88:96:4e:7f:d6:c0)  
 > Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12  
 > Transmission Control Protocol, Src Port: 50861, Dst Port: 80, Seq: 1, Ack: 1, Len: 463  
 > Hypertext Transfer Protocol

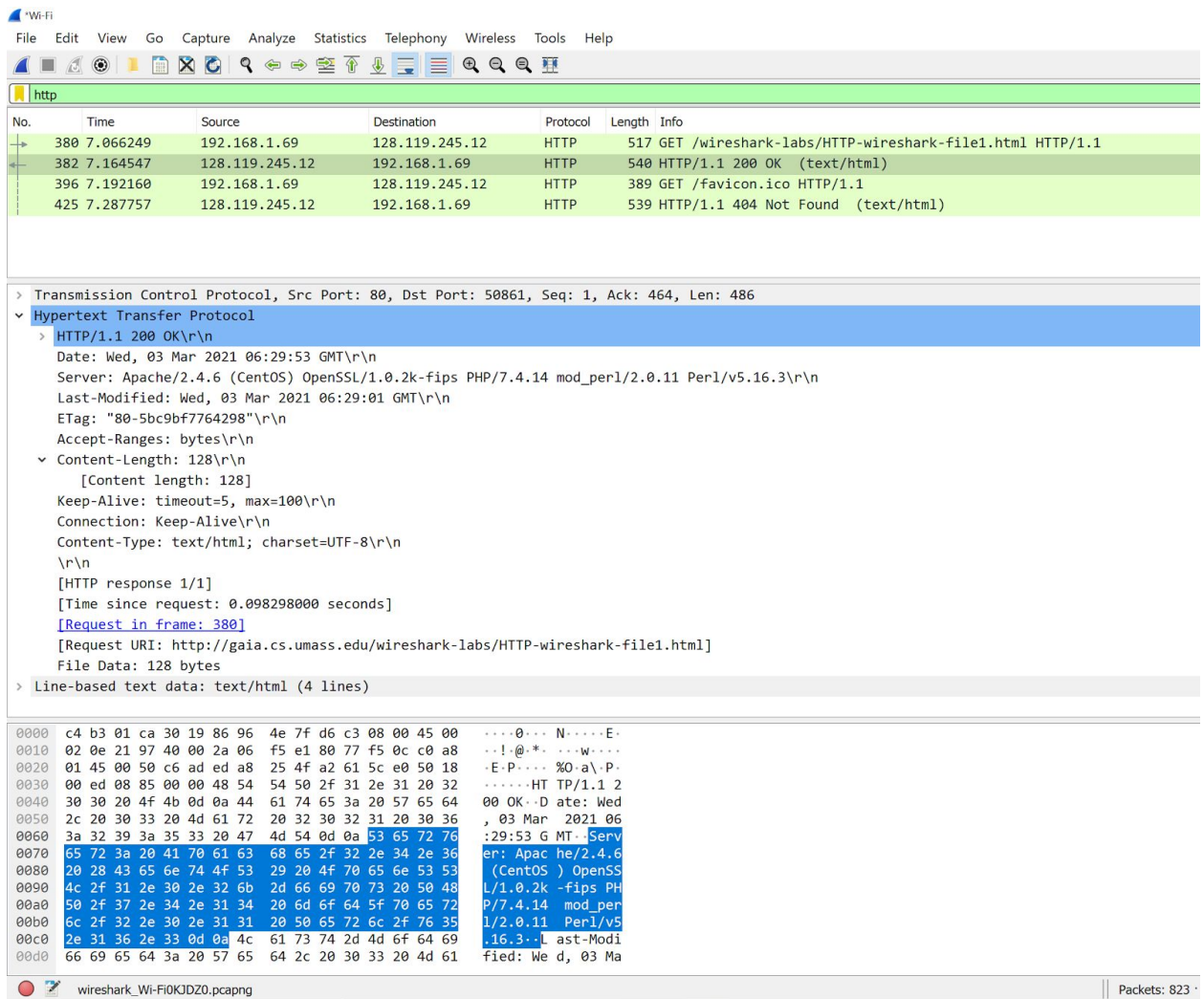
```

    > GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    If-Modified-Since: Wed, 03 Mar 2021 06:28:02 GMT\r\n
    If-None-Match: "80-5bc9bf3efa9bb"\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 382]
  
```

00e0	30 0d 0a 41 63 63 65 70	74 3a 20 74 65 78 74 2f	0·Accep t: text/
00f0	68 74 6d 6c 2c 61 70 70	6c 69 63 61 74 69 6f 6e	html,app lication
0100	2f 78 68 74 6d 6c 2b 78	6d 6c 2c 61 70 70 6c 69	/xhtml+x ml,appli
0110	63 61 74 69 6f 6e 2f 78	6d 6c 3b 71 3d 30 2e 39	cation/x ml;q=0.9
0120	2c 69 6d 61 67 65 2f 77	65 62 70 2c 2a 2f 2a 3b	,image/w ebp,*/*;
0130	71 3d 30 2e 38 0d 0a 41	63 63 65 70 74 2d 4c 61	q=0.8·A ccept-La
0140	6e 67 75 61 67 65 3a 20	65 6e 2d 55 53 2c 65 6e	nguage: en-US,en
0150	3b 71 3d 30 2e 35 0d 0a	41 63 63 65 70 74 2d 45	;q=0.5· Accept-E
0160	6e 63 6f 64 69 6e 67 3a	20 67 7a 69 70 2c 20 64	ncoding: gzip, d
0170	65 66 6c 61 74 65 0d 0a	43 6f 6e 6e 65 63 74 69	eflate· Connecti
0180	6f 6e 3a 20 6b 65 65 70	2d 61 6c 69 76 65 0d 0a	on: keep -alive·
0190	55 70 67 72 61 64 65 2d	49 6e 73 65 63 75 72 65	Upgrade- Insecure
01a0	2d 52 65 71 75 65 73 74	73 3a 20 31 0d 0a 49 6e	-Request s: 1·If
01b0	2d 4d 6f 64 69 6e 69 65	64 2d 53 69 6e 63 65 3a	-Modifie d-Since:

- My browser is running HTTP version 1.1
- The languages that the browser indicates that I can accept to the server is English US as seen by the text “en-US”
- The IP address of my computer is 192.168.1.69 and the IP address of the gaia.cs.umass.edu server is 128.119.245.12
- The status code returned from the server to my browser is 200 OK

- The HTML file was last modified on Wed, 03, Mar 2021 06:29:01 GMT



The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows four packets: a GET request (No. 380), an OK response (No. 382), a GET request for a favicon (No. 396), and a 404 Not Found response (No. 425). The packet details pane for packet 382 shows the HTTP response structure, including headers like Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length (128), Keep-Alive, Connection, and Content-Type. The packet bytes pane at the bottom shows the raw data of the response, which is the HTML content of the file.

No.	Time	Source	Destination	Protocol	Length	Info
380	7.066249	192.168.1.69	128.119.245.12	HTTP	517	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
382	7.164547	128.119.245.12	192.168.1.69	HTTP	540	HTTP/1.1 200 OK (text/html)
396	7.192160	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
425	7.287757	128.119.245.12	192.168.1.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Transmission Control Protocol, Src Port: 80, Dst Port: 50861, Seq: 1, Ack: 464, Len: 486

**Hypertext Transfer Protocol**

- HTTP/1.1 200 OK\r\n
  - Date: Wed, 03 Mar 2021 06:29:53 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Wed, 03 Mar 2021 06:29:01 GMT\r\n
  - ETag: "80-5bc9bf7764298"\r\n
  - Accept-Ranges: bytes\r\n
  - Content-Length: 128\r\n
    - [Content length: 128]
  - Keep-Alive: timeout=5, max=100\r\n
  - Connection: Keep-Alive\r\n
  - Content-Type: text/html; charset=UTF-8\r\n
  - \r\n
  - [HTTP response 1/1]
  - [Time since request: 0.098298000 seconds]
  - [Request in frame: 380]
  - [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
  - File Data: 128 bytes

Line-based text data: text/html (4 lines)

```

0000  c4 b3 01 ca 30 19 86 96 4e 7f d6 c3 08 00 45 00  ....0... N....E-
0010  02 0e 21 97 40 00 2a 06 f5 e1 80 77 f5 0c c0 a8  ..!.@.*. ...w....
0020  01 45 00 50 c6 ad ed a8 25 4f a2 61 5c e0 50 18  .E.P.... %O.a.P-
0030  00 ed 08 85 00 00 48 54 54 50 2f 31 2e 31 20 32  .....HT TP/1.1 2
0040  30 20 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64  00 OK..D ate: Wed
0050  2c 20 30 33 20 4d 61 72 20 32 30 32 31 20 30 36  , 03 Mar 2021 06
0060  3a 32 39 3a 35 33 20 47 4d 54 0d 0a 53 65 72 76  :29:53 G MT..Serv
0070  65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36  er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53  ((CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48  L/1.0.2k -fips PH
00a0  50 2f 37 2e 34 2e 31 34 20 6d 6f 64 5f 70 65 72  P/7.4.14 mod_per
00b0  6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35  l/2.0.11 Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69  .16.3..L ast-Modi
00d0  66 69 65 64 3a 20 57 65 64 2c 20 30 33 20 4d 61  fied: We d, 03 Ma
  
```

Packets: 823

- There are 128 bytes of content being returned from the browser as seen in the Content-Length field.
- No, I don't see any headers within the data that are not displayed in the packet-listing window.

## 2. The HTTP CONDITIONAL GET/response interaction

The image shows a Wireshark packet capture of an HTTP interaction. The packet list pane at the top shows six packets. Packet 83 is a GET request for /wireshark-labs/HTTP-wireshark-file2.html. Packet 85 is the corresponding 200 OK response. Subsequent packets (103, 134, 146, 157) are requests for favicon.ico, which returns 404 Not Found, 304 Not Modified, and 304 Not Modified respectively.

No.	Time	Source	Destination	Protocol	Length	Info
83	2.682577	192.168.1.69	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
85	2.783475	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
103	2.851722	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
134	2.950915	128.119.245.12	192.168.1.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)
146	5.381343	192.168.1.69	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
157	5.480658	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

Frame 83: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF\_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0  
> Ethernet II, Src: Apple\_ca:30:19 (c4:b3:01:ca:30:19), Dst: ARRISGro\_7f:d6:c0 (88:96:4e:7f:d6:c0)  
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 50955, Dst Port: 80, Seq: 1, Ack: 1, Len: 378  
▼ Hypertext Transfer Protocol  
    > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n  
    Host: gaia.cs.umass.edu\r\n  
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n  
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n  
    Accept-Language: en-US,en;q=0.5\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-file2.html>]  
    [HTTP request 1/1]  
    [Response in frame: 85]

00d0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 38 35 2e 0101 Fir efox/85.  
00e0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 00..Accep t: text/  
00f0 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e html,app lication  
0100 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 /xhtml+x ml,appli  
0110 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 cation/x ml;q=0.9  
0120 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b ,image/w ebp,\*/\*;  
0130 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8..A ccept-La  
0140 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e nguage: en-US,en  
0150 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5.. Accept-E  
0160 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d  
0170 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 eflate.. Connecti  
0180 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..  
0190 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure  
01a0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 0d 0a -Request s: 1....

wireshark Wi-FiABYNZ0.pcapng Packets: 254 · Displayed: 6 (2.4%) Profile: Defi

- I do not see an “IF-MODIFIED-SINCE” line in the first HTTP GET

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
83	2.682577	192.168.1.69	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
85	2.783475	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
103	2.851722	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
134	2.950915	128.119.245.12	192.168.1.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)
146	5.381343	192.168.1.69	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
157	5.480658	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

Content-Type: text/html; charset=UTF-8\r\n  
\r\n  
[HTTP response 1/2]  
[Time since request: 0.100898000 seconds]  
[\[Request in frame: 83\]](#)  
[\[Next request in frame: 146\]](#)  
[\[Next response in frame: 157\]](#)  
[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)

```

\r\n
<html>\r\n
\r\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
\r\n
</html>\r\n

```

0000 c4 b3 01 ca 30 19 86 96 4e 7f d6 c3 08 00 45 00 ...0... N....E.  
0010 03 02 53 19 40 00 2b 06 c2 6b 80 77 f5 0c c0 a8 ..S.@.+ .k.w....  
0020 01 45 00 50 c7 0b d4 6b 09 ad fb 1f 0f 91 50 18 ..E.P...k .....P.  
0030 00 ed f3 8b 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2  
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 57 65 64 00 OK..D ate: Wed  
0050 2c 20 30 33 20 4d 61 72 20 32 30 32 31 20 30 36 , 03 Mar 2021 06  
0060 3a 34 37 3a 34 34 20 47 4d 54 0d 0a 53 65 72 76 :47:44 G MT..Serv  
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6  
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS  
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH  
00a0 50 2f 37 2e 34 2e 31 34 20 6d 6f 64 5f 70 65 72 P/7.4.14 mod\_per  
00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5  
00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..L ast-Modi  
00d0 66 69 65 64 3a 20 57 65 64 2c 20 30 33 20 4d 61 fied: We d, 03 Ma

wireshark Wi-FiABYNZ0.ocaona Packets: 254 · Displayed: 6 (2.4%) · Drooped: 0 (0.0%) Profile: Default

- Yes, the server did explicitly return the contents of the file. I can tell by seeing the text of the HTML file displayed in the “line based text data” field



Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
83	2.682577	192.168.1.69	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
85	2.783475	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
103	2.851722	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
134	2.950915	128.119.245.12	192.168.1.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)
146	5.381343	192.168.1.69	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
157	5.480658	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 146: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF\_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93}

> Ethernet II, Src: Apple\_ca:30:19 (c4:b3:01:ca:30:19), Dst: ARRISGro\_7f:d6:c0 (88:96:4e:7f:d6:c0)

> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 50955, Dst Port: 80, Seq: 379, Ack: 731, Len: 490

> Hypertext Transfer Protocol

> GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n

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

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

If-Modified-Since: Wed, 03 Mar 2021 06:47:01 GMT\r\n

If-None-Match: "173-5bc9c37d88c9f"\r\n

Cache-Control: max-age=0\r\n

\r\n

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

[HTTP request 2/2]

[Prev request in frame: 83]

00e0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 00..Accep t: text/  
00f0 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e html,app lication  
0100 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 /xhtml+x ml,appli  
0110 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 cation/x ml;q=0.9  
0120 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b ,image/w ebp,\*/\*;  
0130 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8..A ccept-La  
0140 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e nguage: en-US,en  
0150 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5.. Accept-E  
0160 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d  
0170 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 eflate.. Connecti  
0180 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..  
0190 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure  
01a0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 49 66 -Request s: 1..If  
01b0 2d 4d 6f 64 69 66 69 65 64 2d 53 69 6e 63 65 3a -Modifie d-Since:

HTTP Accept (http.accept), 84 bytes

Packets: 254 · Displayed: 6 (2.4%) · Dropped: 0 (0.0%) Profile: Defi

- Yes, I do see an “IF-MODIFIED-SINCE” line in the second HTTP GET. The information that follows is Wed, 03 Mar 2021 06:47:01 GMT

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
83	2.682577	192.168.1.69	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file
85	2.783475	128.119.245.12	192.168.1.69	HTTP	784	HTTP/1.1 200 OK (text/html)
103	2.851722	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
134	2.950915	128.119.245.12	192.168.1.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)
146	5.381343	192.168.1.69	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file
157	5.480658	128.119.245.12	192.168.1.69	HTTP	293	HTTP/1.1 304 Not Modified

> Frame 157: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF\_{65E4FA18-2BBE-45  
 > Ethernet II, Src: 86:96:4e:7f:d6:c3 (86:96:4e:7f:d6:c3), Dst: Apple\_ca:30:19 (c4:b3:01:ca:30:19)  
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.69  
 > Transmission Control Protocol, Src Port: 80, Dst Port: 50955, Seq: 731, Ack: 869, Len: 239  
 > Hypertext Transfer Protocol  
 > HTTP/1.1 304 Not Modified\r\n  
 Date: Wed, 03 Mar 2021 06:47:47 GMT\r\n  
 Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.14 mod\_perl/2.0.11 Perl/v5.16.3\r\n  
 Connection: Keep-Alive\r\n  
 Keep-Alive: timeout=5, max=99\r\n  
 ETag: "173-5bc9c37d88c9f"\r\n  
 \r\n  
 [HTTP response 2/2]  
 [Time since request: 0.099315000 seconds]  
[\[Prev request in frame: 83\]](#)  
[\[Prev response in frame: 85\]](#)  
[\[Request in frame: 146\]](#)  
 [Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

0000 c4 b3 01 ca 30 19 86 96 4e 7f d6 c3 08 00 45 00 ...0... N....E.  
 0010 01 17 53 1a 40 00 2b 06 c4 55 80 77 f5 0c c0 a8 ..S.@.+ .U.w....  
 0020 01 45 00 50 c7 0b d4 6b 0c 87 fb 1f 11 7b 50 18 .E.P...k .....{P.  
 0030 00 f5 fa 99 00 00 48 54 54 50 2f 31 2e 31 20 33 .....HT TP/1.1 3  
 0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not M odified.  
 0050 0a 44 61 74 65 3a 20 57 65 64 2c 20 30 33 20 4d .Date: W ed, 03 M  
 0060 61 72 20 32 30 32 31 20 30 36 3a 34 37 3a 34 37 ar 2021 06:47:47  
 0070 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap  
 0080 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6e 74 ache/2.4 .6 (Cent  
 0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2e 30 2e OS) Open SSL/1.0.  
 00a0 32 6b 2d 66 69 70 73 20 50 48 50 2f 37 2e 34 2e 2k-fips PHP/7.4.  
 00b0 31 34 20 6d 6f 64 5f 70 65 72 6c 2f 32 2e 30 2e 14 mod\_p erl/2.0.  
 00c0 31 31 20 50 65 72 6c 2f 76 35 2e 31 36 2e 33 0d 11 Perl/ v5.16.3.  
 00d0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 .Connect ion: Kee

wireshark Wi-Fi: RYNY70 ncano || Packets: 254 · Displayed: 6 (2.4%) · Dropped: 0 (0.0%) ||

- The HTTP status code and phrase returned from the server in response to the second HTTP GET are 304 Not Modified. The server did not explicitly return the contents of the file as it was not modified since the last response.

### 3. Retrieving Long Documents

The image shows a Wireshark packet capture of an HTTP transaction. The top pane displays a list of packets. Packet 47 is a GET request for /wireshark-labs/HTTP-wireshark-file3.html. Packet 54 is the corresponding 200 OK response. The middle pane shows the details of the selected packet (47), including the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
47	2.675728	192.168.1.69	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
54	2.774039	128.119.245.12	192.168.1.69	HTTP	535	HTTP/1.1 200 OK (text/html)
79	2.904963	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
86	3.002691	128.119.245.12	192.168.1.69	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Frame 47: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF\_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}

Ethernet II, Src: Apple\_ca:30:19 (c4:b3:01:ca:30:19), Dst: ARRISGro\_7f:d6:c0 (88:96:4e:7f:d6:c0)

Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 54280, Dst Port: 80, Seq: 1, Ack: 1, Len: 378

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n

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

Accept-Language: en-US,en;q=0.5\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: 54]

00d0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 38 35 2e 0101 Fir efox/85.  
00e0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 00..Accep t: text/  
00f0 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e html,app lication  
0100 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c 69 /xhtml+x ml,appli  
0110 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e 39 cation/x ml;q=0.9  
0120 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f 2a 3b ,image/w ebp,\*/\*;  
0130 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d 4c 61 q=0.8..A ccept-La  
0140 6e 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e nguage: en-US,en  
0150 3b 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 ;q=0.5.. Accep t-E  
0160 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 ncoding: gzip, d  
0170 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 74 69 eflate.. Connecti  
0180 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep -alive..  
0190 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade- Insecure  
01a0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 0d 0a -Request s: 1....

wireshark Wi-FiYOHHAZO.pcapng | Packets: 97 · Displayed: 4 (4.1%) | Profile: Default

- The browser only sent 1 HTTP GET request message. The 47th packet contains the GET message for the Bill of Rights.
- The 54th packet contains the status code and the phrase associated with the response to the HTTP GET request.
- The status code and phrase in the response is 200 OK
- 5 TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights.



## 4. HTML Documents with Embedded Objects

The image shows a Wireshark capture of HTTP traffic. The top pane displays a list of packets, with packet 195 selected. The middle pane shows the details of the selected packet, which is an HTTP GET request for the file `/wireshark-labs/HTTP-wireshark-file4.html`. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
195	2.180468	192.168.1.69	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
218	2.279100	128.119.245.12	192.168.1.69	HTTP	1355	HTTP/1.1 200 OK (text/html)
292	2.331783	192.168.1.69	128.119.245.12	HTTP	389	GET /pearson.png HTTP/1.1
432	2.429673	128.119.245.12	192.168.1.69	HTTP	746	HTTP/1.1 200 OK (PNG)
439	2.491627	192.168.1.69	178.79.137.164	HTTP	396	GET /8E_cover_small.jpg HTTP/1.1
445	2.537013	192.168.1.69	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
448	2.634908	128.119.245.12	192.168.1.69	HTTP	538	HTTP/1.1 404 Not Found (text/html)
450	2.652207	178.79.137.164	192.168.1.69	HTTP	225	HTTP/1.1 301 Moved Permanently

Frame 195: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF\_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0  
> Ethernet II, Src: Apple\_ca:30:19 (c4:b3:01:ca:30:19), Dst: ARRISGro\_7f:d6:c0 (88:96:4e:7f:d6:c0)  
> Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 54510, Dst Port: 80, Seq: 1, Ack: 1, Len: 378  
▼ Hypertext Transfer Protocol  
 > GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1\r\n  
 Host: gaia.cs.umass.edu\r\n  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n  
 Accept-Language: en-US,en;q=0.5\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-file4.html]  
 [HTTP request 1/1]  
 [Response in frame: 218]

0020 f5 0c d4 ee 00 50 d1 39 7e 74 cd 3c 35 9b 50 18 ..P.9 ~t.<5.P.  
0030 04 02 05 4b 00 00 47 45 54 20 2f 77 69 72 65 73 ...K..GE T /wires  
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 hark-lab s/HTTP-w  
0050 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 34 2e 68 ireshark -file4.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 38 35 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 85.0) Ge cko/2010  
00d0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 38 35 2e 0101 Fir efox/85.  
00e0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 0 .Accep t: text/  
00f0 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f 6e html,app lication

wireshark\_Wi-Fi0PS6Y0.pcapng | Packets: 926 · Displayed: 8 (0.9%) | Profile: Defa

- The browser sent 3 HTTP GET requests and they were sent to the HTML page, to the Pearson image, and to the Pearson book image.
- The browser downloaded the two images serially instead of in parallel since the second image was not requested until the first image was received.



## 5. HTTP Authentication

The image shows a Wireshark packet capture of an HTTP transaction. The packet list at the top shows several HTTP packets. Packet 207 is a GET request for a protected page, which results in a 401 Unauthorized response (packet 209). Packet 237 is a GET request for a favicon, which results in a 404 Not Found response (packet 254). The packet details pane for packet 209 shows the HTTP response structure, including the status line '401 Unauthorized' and the 'WWW-Authenticate: Basic' header. The packet bytes pane shows the raw data of the response, including the status code and headers.

No.	Time	Source	Destination	Protocol	Length	Info
103	13.138726	192.168.1.69	128.119.245.12	HTTP	448	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
106	13.240082	128.119.245.12	192.168.1.69	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
152	19.729246	2600:1700:e1c0:dc0...	2600:1406:cc00::173...	HTTP	361	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?a2c03...
154	19.760467	2600:1406:cc00::173...	2600:1700:e1c0:dc0...	HTTP	342	HTTP/1.1 304 Not Modified
207	34.091411	192.168.1.69	128.119.245.12	HTTP	507	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
209	34.191470	128.119.245.12	192.168.1.69	HTTP	544	HTTP/1.1 200 OK (text/html)
237	34.274431	192.168.1.69	128.119.245.12	HTTP	405	GET /favicon.ico HTTP/1.1
254	34.372099	128.119.245.12	192.168.1.69	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 207: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits) on interface \Device\NPF\_{65E4FA18-2BBE-459E-BA4D-2BD0A818A93A}, id 0  
 Ethernet II, Src: Apple\_ca:30:19 (c4:b3:01:ca:30:19), Dst: ARRISGro\_7f:d6:c0 (88:96:4e:7f:d6:c0)  
 Internet Protocol Version 4, Src: 192.168.1.69, Dst: 128.119.245.12  
 Transmission Control Protocol, Src Port: 55062, Dst Port: 80, Seq: 1, Ack: 1, Len: 453  
 Hypertext Transfer Protocol  
 GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n  
 Host: gaia.cs.umass.edu\r\n  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0\r\n  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8\r\n  
 Accept-Language: en-US,en;q=0.5\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Connection: keep-alive\r\n  
 Upgrade-Insecure-Requests: 1\r\n  
 Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\r\n  
 \r\n  
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html]  
 [HTTP request 1/2]  
 [Response in frame: 209]

0020 f5 0c d7 16 00 50 4e a2 50 25 22 a5 20 bf 50 18 ...PN. P%". .P.  
 0030 04 02 79 d2 00 00 47 45 54 20 2f 77 69 72 65 73 ...y...GE T /wires  
 0040 68 61 72 6b 2d 6c 61 62 73 2f 70 72 6f 74 65 63 hark-lab s/protec  
 0050 74 65 64 5f 70 61 67 65 73 2f 48 54 54 50 2d 77 ted\_page s/HTTP-w  
 0060 69 72 65 73 68 61 72 6b 2d 66 69 6c 65 35 2e 68 ireshark -file5.h  
 0070 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f tml HTTP /1.1 .Ho  
 0080 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 st: gaia .cs.umas  
 0090 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 65 6e s.edu .U ser-Agen  
 00a0 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (  
 00b0 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0,  
 00c0 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 72 76 3a Win64; x64; rv:  
 00d0 38 35 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31 30 85.0) Ge cko/2010  
 00e0 30 31 30 31 20 46 69 72 65 66 6f 78 2f 38 35 2e 0101 Fir efox/85.  
 00f0 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 0..Accep t: text/

Transmission Control Protocol (tcp), 20 bytes | Packets: 289 · Displayed: 8 (2.8%) · Dropped: 0 (0.0%) | Profile: Default

- The server's response in response to the initial HTTP GET message from the browser is 401 Unauthorized.
- The new field that is included in the HTTP GET message is the Authorization field.