

Fundamental of Networking Assignment



Amanuel Legesse

ATE/3628/11

DEPARTMENT : SOFTWARE ENGINEERING
EXTENSION



SUBMITTED TO: - ABRAHAM ARSESA

Chapter 2: Wire Shark HTTP Lab Report

What to hand in:

By looking at the information in the HTTP GET and response messages, answer the following questions. When answering the following questions, you should print out the GET and response messages (see the introductory Wireshark lab for an explanation of how to do this) and indicate where in the message you've found the information that answers the following questions. When you hand in your assignment, annotate the output so that it's clear where in the output you're getting the information for your answer (e.g., for our classes, we ask that students markup paper copies with a pen, or annotate electronic copies with text in a colored font).

1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

✓ The browser is running on HTTP version 1.1

Wireshark network traffic capture showing an HTTP GET request. The packet list pane displays the following information:

No.	Time	Source	Destination	Protocol	Length	Info
2476	8.081208	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2480	8.276117	128.119.245.12	192.168.1.12	HTTP	540	HTTP/1.1 200 OK (text/html)
2482	8.424755	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
2483	8.624807	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)
5407	23.119379	192.168.1.12	93.184.220.29	OCSP	435	Request
5411	23.242372	93.184.220.29	192.168.1.12	OCSP	853	Response
5432	24.250089	192.168.1.12	192.168.1.1	HTTP	254	GET /igdeviceidesc.xml HTTP/1.1
5436	24.260096	192.168.1.1	192.168.1.12	HTTP/X...	642	HTTP/1.1 200 OK

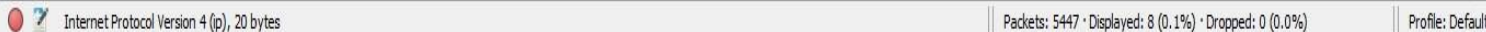
The packet details pane shows the following information for the selected packet (No. 2476):

- Transmission Control Protocol, Src Port: 50316, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
- 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: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

The packet bytes pane shows the raw data of the request:

```
0000 f0 b4 d2 d6 e7 15 28 e3 47 a0 18 af 08 00 45 00 .....( G .....E
0010 01 a2 42 13 40 00 80 06 80 0a c0 a8 01 0c 80 77 ..B.@... .....w
0020 f5 0c c4 8c 00 50 8c 35 8b 90 84 a7 f4 03 50 18 ....P.5 .....P
0030 02 01 d9 fe 00 00 47 45 54 20 2f 77 69 72 65 73 .....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 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;
```

- ✓ The language the browser is using is en-US.



3. What is the IP address of your computer? Of the gaia.cs.umass.edu server?

✓ The Internet address of the
gaia.cs.umass.edu is:
128.119.245.12

✓ The Computer Address used for this Assignment is:
192.168.1.12

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. The selected packet (No. 2476) is an HTTP GET request from 192.168.1.12 to 128.119.245.12. The middle pane shows the details of this packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol section. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2476	8.081208	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2480	8.276117	128.119.245.12	192.168.1.12	HTTP	540	HTTP/1.1 200 OK (text/html)
2482	8.424755	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
2483	8.624807	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)
5407	23.119379	192.168.1.12	93.184.220.29	OCSP	435	Request
5411	23.242372	93.184.220.29	192.168.1.12	OCSP	853	Response
5432	24.250089	192.168.1.12	192.168.1.1	HTTP	254	GET /igdevice-desc.xml HTTP/1.1
5436	24.260096	192.168.1.1	192.168.1.12	HTTP/Xm	642	HTTP/1.1 200 OK

Frame 2476: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits) on interface \Device\NPF_{AC6B9D89-A567-4392-BB1F-F6888E163DC7}, id 0
> Ethernet II, Src: LiteonTe_a0:18:af (28:e3:47:a0:18:af), Dst: D-LinkIn_d6:e7:15 (f0:b4:d2:d6:e7:15)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50316, Dst Port: 80, Seq: 1, Ack: 1, Len: 378
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\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n

Internet Protocol Version 4 (p), 20 bytes | Packets: 5447 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

4. What is the status code returned from the server to your browser?

✓ The status code returned is 200.

The image shows a Wireshark network traffic capture. The top pane displays a list of captured packets. Packet 2480 is highlighted, showing an HTTP 1.1 200 OK response from 128.119.245.12 to 192.168.1.12. The middle pane shows the details of the selected packet, including the Ethernet II header, Internet Protocol Version 4 header, and the Hypertext Transfer Protocol section. The Hypertext Transfer Protocol section shows the response version as HTTP/1.1, the status code as 200, and the response phrase as OK. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2476	8.081208	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2480	8.276117	128.119.245.12	192.168.1.12	HTTP	540	HTTP/1.1 200 OK (text/html)
2482	8.424755	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
2483	8.624807	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)
5407	23.119379	192.168.1.12	93.184.220.29	OCSP	435	Request
5411	23.242372	93.184.220.29	192.168.1.12	OCSP	853	Response
5432	24.250089	192.168.1.12	192.168.1.1	HTTP	254	GET /igdeviceDesc.xml HTTP/1.1
5436	24.260096	192.168.1.1	192.168.1.12	HTTP/X...	642	HTTP/1.1 200 OK

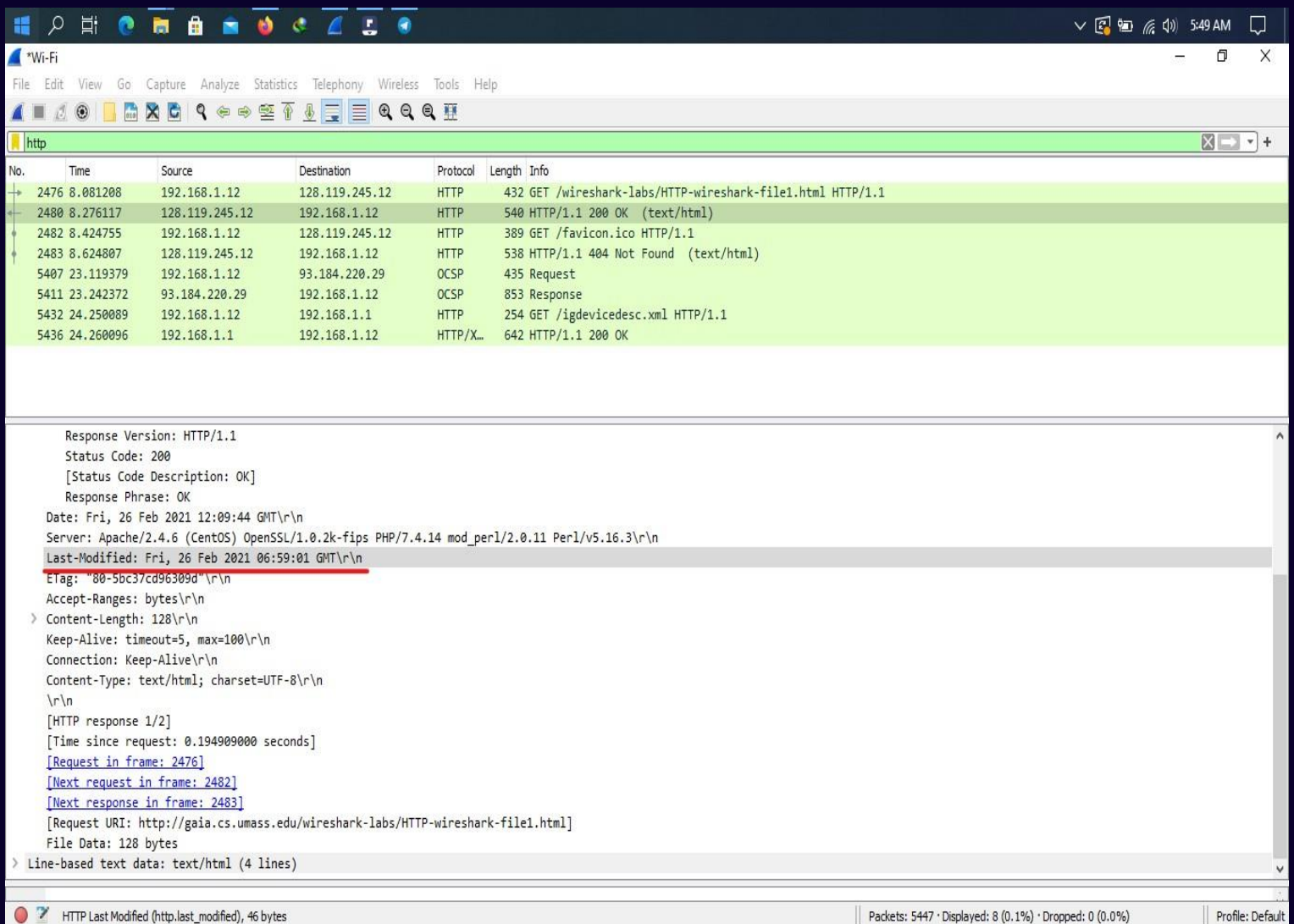
Frame 2480: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{AC6B9D89-A567-4392-BB1F-F688BE163DC7}, id 0
Ethernet II, Src: D-LinkIn_d6:e7:15 (f0:b4:d2:d6:e7:15), Dst: LiteonTe_a0:18:af (28:e3:47:a0:18:af)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
Transmission Control Protocol, Src Port: 80, Dst Port: 50316, Seq: 1, Ack: 379, Len: 486
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 26 Feb 2021 12:09:44 GMT\r\nServer: 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

0000 28 e3 47 a0 18 af f0 b4 d2 d6 e7 15 08 00 45 00 (G.....E.
0010 02 0e a9 9a 40 00 30 06 68 17 80 77 f5 0c c0 a8@.h.w....
0020 01 0c 00 50 c4 8c 84 a7 f4 03 8c 35 8d 0a 50 18 ..P.....S..P.
0030 00 ed 9d 13 00 00 48 54 54 50 2f 31 2e 31 20 32HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 46 72 69 00 OK...D ate: Fri
0050 2c 20 32 36 20 46 65 62 20 32 30 32 31 20 31 32 , 26 Feb 2021 12
0060 3a 30 39 3a 34 34 20 47 4d 54 0d 0a 53 65 72 76 :09:44 GMT 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_perl

Internet Protocol Version 4 (IP), 20 bytes | Packets: 5447 · Displayed: 8 (0.1%) · Dropped: 0 (0.0%) | Profile: Default

5. When was the HTML file that you are retrieving last modified at the server?

✓ Last modified on Fri, 26 Feb 2021, 06:59:01 GMT



The image shows a Wireshark packet capture window. The top pane displays a list of network packets. The bottom pane shows the details of the selected packet (No. 2483), which is an HTTP 200 OK response. The response headers include the date, status code, and the 'Last-Modified' timestamp, which is highlighted in red. The status bar at the bottom indicates that the packet is an HTTP Last Modified response.

No.	Time	Source	Destination	Protocol	Length	Info
2476	8.081208	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2480	8.276117	128.119.245.12	192.168.1.12	HTTP	540	HTTP/1.1 200 OK (text/html)
2482	8.424755	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
2483	8.624807	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)
5407	23.119379	192.168.1.12	93.184.220.29	OCSP	435	Request
5411	23.242372	93.184.220.29	192.168.1.12	OCSP	853	Response
5432	24.250089	192.168.1.12	192.168.1.1	HTTP	254	GET /igdevicecdesc.xml HTTP/1.1
5436	24.260096	192.168.1.1	192.168.1.12	HTTP/X...	642	HTTP/1.1 200 OK

Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 26 Feb 2021 12:09:44 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: Fri, 26 Feb 2021 06:59:01 GMT\r\n
ETag: "80-5bc3/cd96309d"\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
\r\n
[HTTP response 1/2]
[Time since request: 0.194909000 seconds]
[Request in frame: 2476]
[Next request in frame: 2482]
[Next response in frame: 2483]
[Request URI: http://gala.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes
> Line-based text data: text/html (4 lines)

HTTP Last Modified (http.last_modified), 46 bytes

Packets: 5447 • Displayed: 8 (0.1%) • Dropped: 0 (0.0%)

Profile: Default

6. How many bytes of content are being returned to your browser?

✓ 128 bytes of content length are being returned.

The image shows a Wireshark network traffic capture window. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 2483), which is an HTTP 200 OK response. The details pane shows the response structure, including the status code, response phrase, date, server information, last-modified date, ETag, accept-ranges, content-length, keep-alive, connection, content-type, and file data. The content-length is highlighted as 128 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
2476	8.081208	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2480	8.276117	128.119.245.12	192.168.1.12	HTTP	540	HTTP/1.1 200 OK (text/html)
2482	8.424755	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
2483	8.624807	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)
5407	23.119379	192.168.1.12	93.184.220.29	OCSF	435	Request
5411	23.242372	93.184.220.29	192.168.1.12	OCSF	853	Response
5432	24.250089	192.168.1.12	192.168.1.1	HTTP	254	GET /igdeviceidesc.xml HTTP/1.1
5436	24.260096	192.168.1.1	192.168.1.12	HTTP/X...	642	HTTP/1.1 200 OK

Response Version: HTTP/1.1
Status Code: 200
[Status Code Description: OK]
Response Phrase: OK
Date: Fri, 26 Feb 2021 12:09:44 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: Fri, 26 Feb 2021 06:59:01 GMT\r\n
ETag: "80-5bc37cd96309d"\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 1/2]
[Time since request: 0.194909000 seconds]
[Request in frame: 2476]
[Next request in frame: 2482]
[Next response in frame: 2483]
[Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
File Data: 128 bytes

HTTP Last Modified (http.last_modified), 46 bytes

Packets: 5447 • Displayed: 8 (0.1%) • Dropped: 0 (0.0%)

Profile: Default

7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

✓ No. The raw data appears to match up exactly with what is shown in the packet-listing window.

8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

✓ No.

9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

✓ Yes it did, we can tell by the line-based data: text/html which is 10 lines of contents.

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet listing pane at the top shows four packets. The third packet (No. 126) is an HTTP 200 OK response from 192.168.1.12 to 128.119.245.12. The packet details pane shows the response structure, including the status line and the body content. The body content is displayed in the packet bytes pane, showing the HTML content of the file.

No.	Time	Source	Destination	Protocol	Length	Info
28	0.913559	192.168.1.12	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
37	1.110186	128.119.245.12	192.168.1.12	HTTP	784	HTTP/1.1 200 OK (text/html)
126	7.506730	192.168.1.12	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
129	7.707462	128.119.245.12	192.168.1.12	HTTP	294	HTTP/1.1 304 Not Modified

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
```

Response line (http.response.line), 32 bytes

Packets: 148 · Displayed: 4 (2.7%) · Dropped: 0 (0.0%)

Profile: Default

10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

✓ If-Modified-Since: Sat, 27 2021, 06:59:01 GMT

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list at the top shows four packets. The first two are GET requests, and the next two are 200 OK responses. The packet details pane for the first packet (No. 28) shows the request headers, including 'If-Modified-Since: Sat, 27 Feb 2021 06:59:01 GMT'.

No.	Time	Source	Destination	Protocol	Length	Info
28	0.913559	192.168.1.12	128.119.245.12	HTTP	535	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
37	1.110186	128.119.245.12	192.168.1.12	HTTP	784	HTTP/1.1 200 OK (text/html)
126	7.506730	192.168.1.12	128.119.245.12	HTTP	647	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
129	7.707462	128.119.245.12	192.168.1.12	HTTP	294	HTTP/1.1 304 Not Modified

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) Chrome/88.0.4324.182 Safari/537.36 Edg/88.0.705.74\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
If-None-Match: "173-5bc4beb6608cd"\r\n
If-Modified-Since: Sat, 27 Feb 2021 06:59:01 GMT\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: 129]

01e0 65 3b 76 3d 62 33 3b 71 3d 30 2e 39 0d 0a 41 63 e;v=b3;q=0.9...Ac
01f0 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67 cept-Enc oding: g
0200 7a 69 70 2c 20 64 65 66 6c 61 74 65 0d 0a 41 63 zip, def late...Ac
0210 63 65 70 74 2d 4c 61 6e 67 75 61 67 65 3a 20 65 cept-Lan guage: e
0220 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 49 n-US,en;q=0.9...I
0230 66 2d 4e 6f 6e 65 2d 4d 61 74 63 68 3a 20 22 31 f-None-M atch: "1
0240 37 33 2d 35 62 63 34 62 65 62 36 36 30 38 63 64 73-5bc4b eb6608cd
0250 22 0d 0a 49 66 2d 4d 6f 64 69 66 69 65 64 2d 53 "-If-Mo dified-S
0260 69 6e 63 65 3a 20 53 61 74 2c 20 32 37 20 46 65 ince: Sa t, 27 Fe
0270 62 20 32 30 32 31 20 30 36 3a 35 39 3a 30 31 20 b 2021 0 6:59:01
0280 47 4d 54 0d 0a 0d 0a GMT...

Request line (http.request.line), 50 bytes | Packets: 148 · Displayed: 4 (2.7%) · Dropped: 0 (0.0%) | Profile: Default

11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

- ✓
 - 304 not modified.
 - The server did not response because the content hasn't been updated recently.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list pane displays several packets, with packet 294 highlighted in green. This packet is an HTTP response with status code 304 and the phrase "Not Modified". The details pane for this packet shows the Hypertext Transfer Protocol section, which includes the request method (POST), host (ocsp.pki.goog), user-agent (Mozilla/5.0), and other headers. The packet bytes pane shows the raw data of the response, which is 83 bytes long.

No.	Time	Source	Destination	Protocol	Length	Info
56	6.423060	192.168.1.12	216.58.209.131	OCSP	441	Request
68	6.637643	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
72	6.792389	216.58.209.131	192.168.1.12	OCSP	755	Response
75	6.849464	128.119.245.12	192.168.1.12	HTTP	784	HTTP/1.1 200 OK (text/html)
77	7.031763	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
78	7.227569	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)
198	29.807482	192.168.1.12	128.119.245.12	HTTP	544	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
202	30.007946	128.119.245.12	192.168.1.12	HTTP	294	HTTP/1.1 304 Not Modified

Frame 56: 441 bytes on wire (3528 bits), 441 bytes captured (3528 bits) on interface \Device\NPF_{AC6B9D89-A567-4392-BB1F-F6B8BE163DC7}, id 0
> Ethernet II, Src: LiteonTe_a0:18:af (28:e3:47:a0:18:af), Dst: D-LinkIn_d6:e7:15 (f0:b4:d2:d6:e7:15)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 216.58.209.131
> Transmission Control Protocol, Src Port: 53190, Dst Port: 80, Seq: 1, Ack: 1, Len: 387
> Hypertext Transfer Protocol
> POST /gtsolcore HTTP/1.1\r\nHost: ocsp.pki.goog\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0\r\nAccept: */*\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nContent-Type: application/ocsp-request\r\nContent-Length: 83\r\nConnection: keep-alive\r\n\r\n[Full request URI: http://ocsp.pki.goog/gtsolcore]
[HTTP request 1/1]
[Response in frame: 72]
File Data: 83 bytes

0050 0a 48 6f 73 74 3a 20 6f 63 73 70 2e 70 6b 69 2e ·Host: o csp.pki.
0060 67 6f 6f 67 0d 0a 55 73 65 72 2d 41 67 65 6e 74 goog·Us er-Agent
0070 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 : Mozill a/5.0 (W
0080 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 indows N T 10.0;

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?

- ✓ Just one Get request messages except favicon.ico
Packet number 14 contains the Bill of rights.

The image shows a Wireshark network traffic capture. The top pane displays a list of packets. Packet 14 is highlighted, showing an HTTP GET request for /wireshark-labs/HTTP-wireshark-file3.html. Packet 21 shows the response (200 OK). Packet 23 shows a GET request for /favicon.ico, and packet 24 shows the response (404 Not Found).

No.	Time	Source	Destination	Protocol	Length	Info
14	0.491715	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
21	0.742685	128.119.245.12	192.168.1.12	HTTP	535	HTTP/1.1 200 OK (text/html)
23	0.801675	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
24	1.083784	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The bottom pane shows the expanded content of packet 14, which is an HTML document titled "Historical Documents: THE BILL OF RIGHTS". The HTML content includes a title, a body with a link to the Bill of Rights, and a paragraph about the Bill of Rights.

```
<html><head> \n
<title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
\n
\n
<body bgcolor="#ffffff" link="#330000" vlink="#666633">\n
<p><br>\n
</p>\n
<p></p><center><b>THE BILL OF RIGHTS</b><br>\n
  <em>Amendments 1-10 of the Constitution</em>\n
</center>\n
\n
<p>The Conventions of a number of the States having, at the time of adopting\n
the Constitution, expressed a desire, in order to prevent misconstruction\n
or abuse of its powers, that further declaratory and restrictive clauses\n
should be added, and as extending the ground of public confidence in the\n
Government will best insure the beneficent ends of its institution; </p><p> Resolved, by the Senate and House of Representatives of the United\n
States of America, in Congress assembled, two-thirds of both Houses concurring,\n
that the following articles be proposed to the Legislatures of the several\n
\n
0160 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d 6c 3e 3c UTF-8... <html><
0170 68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3e 48 69 head> < title>Hi
0180 73 74 6f 72 69 63 61 6c 20 44 6f 63 75 6d 65 6e storical Documen
```


13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

✓ As seen in the screen shot below packet number 21.

The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets, with packet 21 highlighted. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
14	0.491715	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
21	0.742685	128.119.245.12	192.168.1.12	HTTP	535	HTTP/1.1 200 OK (text/html)
23	0.801675	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
24	1.083784	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Details of packet 21 (Hypertext Transfer Protocol):

- HTTP/1.1 200 OK\r\n
- Date: Sun, 28 Feb 2021 09:16:10 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: Sun, 28 Feb 2021 06:59:01 GMT\r\n
- ETag: "1194-5bc60093a7fae"\r\n
- Accept-Ranges: bytes\r\n
- Content-Length: 4500\r\n
- 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 1/2]
- [Time since request: 0.250970000 seconds]

Raw packet data (hex):

```
0000 28 e3 47 a0 18 af f0 b4 d2 d6 e7 15 08 00 45 00  (..G.....E..
0010 02 09 4a d6 40 00 30 06 c6 e0 80 77 f5 0c c0 a8  ..J.@...w....
0020 01 0c 00 50 c0 96 63 c7 77 dc 25 58 08 b9 50 18  ...P..c..w.X..P..
```


14. What is the status code and phrase in the response?

✓ As seen in the above screen shot Http/1.1 200 OK.

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

✓ There are 4 TCP Segments.

The screenshot shows a Wireshark packet capture of an HTTP transaction. The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
14	0.491715	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
21	0.742685	128.119.245.12	192.168.1.12	HTTP	535	HTTP/1.1 200 OK (text/html)
23	0.801675	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
24	1.083784	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet details pane for packet 21 shows the reassembly of TCP segments:

- Frame 21: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{AC6B9D89-A567-4392-BB1F-F6B88E163DC7}, id 0
- Ethernet II, Src: D-LinkIn_d6:e7:15 (f0:b4:d2:d6:e7:15), Dst: LiteonTe_a0:18:af (28:e3:47:a0:18:af)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
- Transmission Control Protocol, Src Port: 80, Dst Port: 49302, Seq: 4381, Ack: 379, Len: 481
- 4 Reassembled TCP Segments (4861 bytes): #17(1460), #18(1460), #20(1460), #21(481)
- [Frame: 17, payload: 0-1459 (1460 bytes)]
- [Frame: 18, payload: 1460-2919 (1460 bytes)]
- [Frame: 20, payload: 2920-4379 (1460 bytes)]
- [Frame: 21, payload: 4380-4860 (481 bytes)]
- [Segment count: 4]
- [Reassembled TCP length: 4861]
- [Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a4461746553a2053756e2c203238204665622032...]

The packet details pane for packet 21 also shows the Hypertext Transfer Protocol section:

- Line-based text data: text/html (98 lines)
- <html><head> \n
- <title>Historical Documents:THE BILL OF RIGHTS</title></head>\n
- \n
- \n
- <body bgcolor="#ffffff" link="#330000" vlink="#666633">\n

The packet bytes pane shows the raw data of the reassembled TCP segment:

```
0000 28 e3 47 a0 18 af f0 b4 d2 d6 e7 15 08 00 45 00  (-G.....E..
0010 02 09 4a d6 40 00 30 06 c6 e0 80 77 f5 0c c0 a8  .J.@. ...W....
0020 01 0c 00 50 c0 96 63 c7 77 dc 25 58 08 b9 50 18  ..P..c. w.%X..P..
```

The status bar at the bottom indicates: Frame (535 bytes) Reassembled TCP (4861 bytes) | Packets: 44 · Displayed: 4 (9.1%) | Profile: Default

16. How many HTTP GET request messages did your browser send? To which internet addresses were these GET requests sent?

✓ The browser sent 3 HTTP GET request messages.
The GET request was sent to:

- 128.119.245.12 – wireshark-labs
- 128.119.245.12 – pearson.png
- 178.79.137.164 – 8E_cover_small.jpg

The image shows a Wireshark packet capture of an HTTP session. The packet list on the left shows several packets, with packet 237 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP GET request for /8E_cover_small.jpg. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
192	19.715321	192.168.1.12	216.58.209.131	OCSP	441	Request
204	19.861568	192.168.1.12	128.119.245.12	HTTP	432	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
211	20.060236	128.119.245.12	192.168.1.12	HTTP	1355	HTTP/1.1 200 OK (text/html)
212	20.076383	216.58.209.131	192.168.1.12	OCSP	755	Response
216	20.131805	192.168.1.12	128.119.245.12	HTTP	389	GET /pearson.png HTTP/1.1
226	20.532344	192.168.1.12	128.119.245.12	HTTP	389	GET /favicon.ico HTTP/1.1
228	20.728279	128.119.245.12	192.168.1.12	HTTP	539	HTTP/1.1 404 Not Found (text/html)
237	20.879441	192.168.1.12	178.79.137.164	HTTP	396	GET /8E_cover_small.jpg HTTP/1.1
240	20.999743	178.79.137.164	192.168.1.12	HTTP	225	HTTP/1.1 301 Moved Permanently
267	21.582761	192.168.1.12	2.23.159.161	OCSP	434	Request
269	21.951317	2.23.159.161	192.168.1.12	OCSP	943	Response

Frame 237: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface \Device\NPF_{AC6B9D89-A567-4392-8B1F-F6B88E163DC7}, id 0
> Ethernet II, Src: LiteonTe_a0:18:af (28:e3:47:a0:18:af), Dst: D-LinkIn_d6:e7:15 (f0:b4:d2:d6:e7:15)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 178.79.137.164
> Transmission Control Protocol, Src Port: 53082, Dst Port: 80, Seq: 1, Ack: 1, Len: 342
v Hypertext Transfer Protocol
GET /8E_cover_small.jpg HTTP/1.1\r\nHost: kurose.cslash.net\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:86.0) Gecko/20100101 Firefox/86.0\r\nAccept: image/webp,*/*\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nReferer: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html\r\n\r\n[Full request URI: http://kurose.cslash.net/8E_cover_small.jpg]
[HTTP request 1/1]
[Response in frame: 240]

0050 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 6b 75 TP/1.1.. Host: ku
0060 72 6f 73 65 2e 63 73 6c 61 73 68 2e 6e 65 74 0d rose.csl ash.net.
0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a -User-Ag ent: Moz
0080 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window

HTTP Host (http.host), 25 bytes

Packets: 867 • Displayed: 11 (1.3%) • Dropped: 0 (0.0%)

Profile: Default

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two web sites in parallel? Explain.

- ✓ Based on the timestamps, it appears the images were downloaded serially. The first image was requested and sent before the second image was requested by the browser.

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

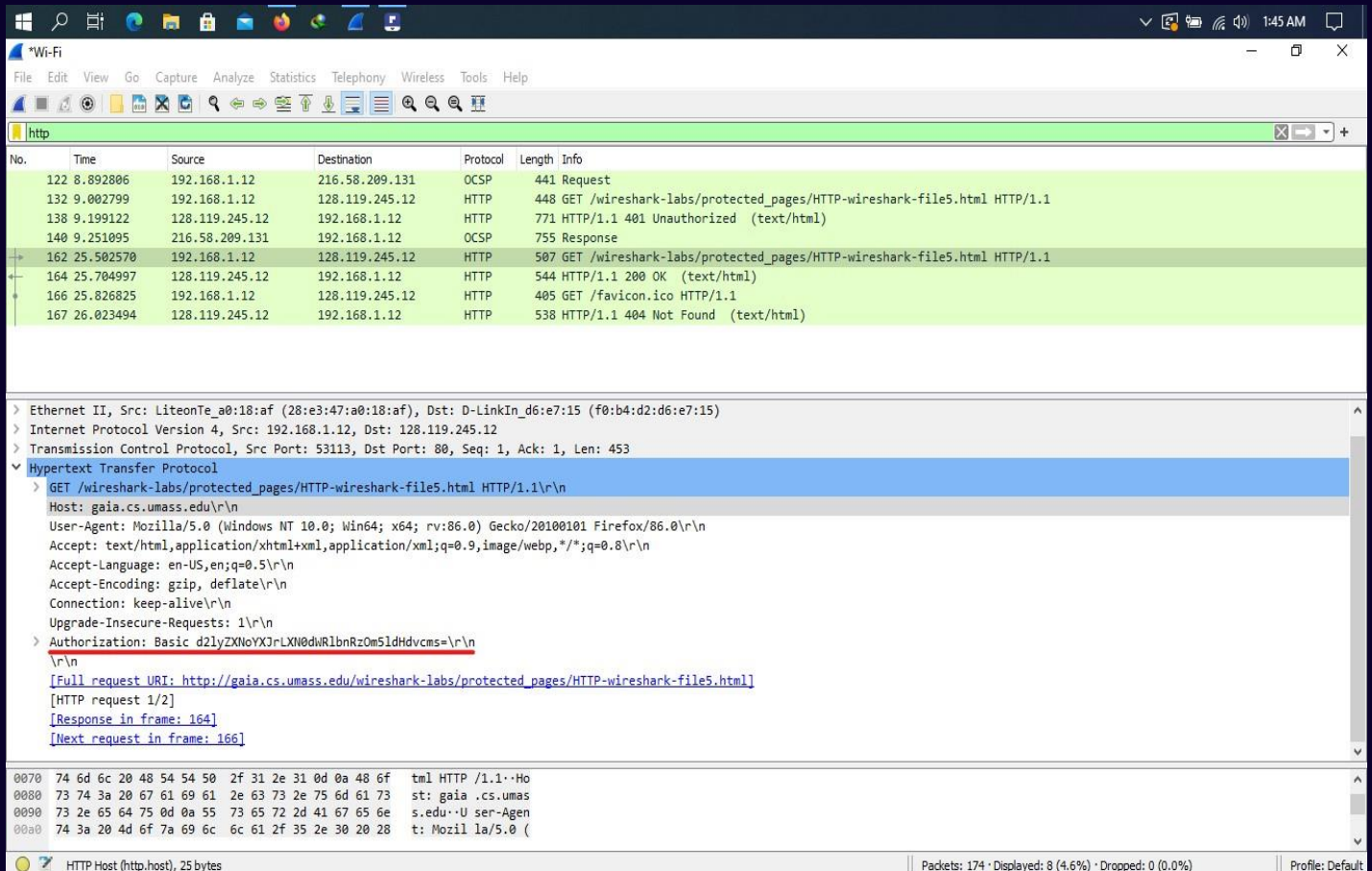
The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 138 is selected, showing an HTTP 401 Unauthorized response from 192.168.1.12 to 128.119.245.12. The bottom pane shows the details of this packet, including the Hypertext Transfer Protocol section. The status code is 401 and the phrase is Unauthorized. The response body contains an HTML error message.

No.	Time	Source	Destination	Protocol	Length	Info
122	8.892806	192.168.1.12	216.58.209.131	OCSP	441	Request
132	9.002799	192.168.1.12	128.119.245.12	HTTP	448	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
138	9.199122	128.119.245.12	192.168.1.12	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
140	9.251095	216.58.209.131	192.168.1.12	OCSP	755	Response
162	25.502570	192.168.1.12	128.119.245.12	HTTP	507	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
164	25.704997	128.119.245.12	192.168.1.12	HTTP	544	HTTP/1.1 200 OK (text/html)
166	25.826825	192.168.1.12	128.119.245.12	HTTP	405	GET /favicon.ico HTTP/1.1
167	26.023494	128.119.245.12	192.168.1.12	HTTP	538	HTTP/1.1 404 Not Found (text/html)

```
> Frame 138: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{AC6B9D89-A567-4392-BB1F-F6B88E163DC7}, id 0
> Ethernet II, Src: D-LinkIn_d6:e7:15 (f0:b4:d2:d6:e7:15), Dst: LiteonTe_a0:18:af (28:e3:47:a0:18:af)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.12
> Transmission Control Protocol, Src Port: 80, Dst Port: 53109, Seq: 1, Ack: 395, Len: 717
> Hypertext Transfer Protocol
  > HTTP/1.1 401 Unauthorized\r\n
    Date: Sun, 28 Feb 2021 09:39:36 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
    WWW-Authenticate: Basic realm="wireshark-students only"\r\n
    Content-Length: 381\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=iso-8859-1\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.196323000 seconds]
    [Request in frame: 132]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
    File Data: 381 bytes
0000 28 e3 47 a0 18 af f0 b4 d2 d6 e7 15 00 00 45 00 ( .G.....E.
0010 02 f5 10 a5 40 00 2f 06 01 26 80 77 f5 0c c0 a8 ...@./.&w...
0020 01 0c 00 50 cf 75 e8 38 8e 6e 95 59 5d 46 50 18 ...P.u:8.n-Y]FP
0030 00 ed 96 0f 00 00 48 54 54 50 2f 31 2e 31 20 34 .....HT TP/1.1 4
```

- ✓ Status code - 401
Phrase – Unauthorized.

19. When your browser's sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?



✓ Authorization:
Basic d2lyZXNoYXJrLXN0dWRIbnRzOm5ldHdvcm5=