

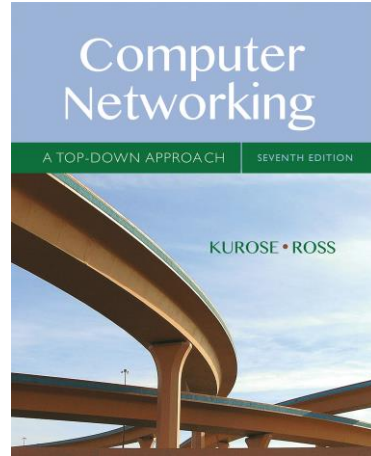
Name: Katie Schaumleffle

## Wireshark Lab: HTTP v7.0

Supplement to *Computer Networking: A Top-Down Approach*, 7<sup>th</sup> ed., J.F. Kurose and K.W. Ross

*"Tell me and I forget. Show me and I remember. Involve me and I understand."* Chinese proverb

© 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved



### 1. The Basic HTTP GET/response interaction

#### 1. Is your browser running HTTP version 1.0 or 1.1?

My browser is running HTTP version 1.1

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list pane shows two packets: a GET request (No. 260) and its response (No. 263). The packet details pane for packet 260 shows the structure of the HTTP request, including the request line, headers, and body. The 'Request Version: HTTP/1.1' field is highlighted with a red box. The packet bytes pane shows the raw data of the request, including the request line and headers.

```
> Frame 260: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF_{CCDC22D-0101}
> Ethernet II, Src: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e), Dst: Ubiquiti_50:af:2b (68:d7:9a:50:af:2b)
> Internet Protocol Version 4, Src: 172.16.1.114, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51949, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
< 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
        Connection: keep-alive\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/106.0.0.0
        Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
        \r\n
        [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
        [HTTP request 1/1]
        [Response in frame: 263]
```

## What version of HTTP is the server running?

The server is running HTTP version 1.1

The image shows a Wireshark packet capture window titled '\*Wi-Fi'. The packet list pane at the top shows two packets. Packet 260 is a GET request for '/wireshark-labs/HTTP-wireshark-file1.html' from 172.16.1.114 to 128.119.245.12. Packet 263 is the corresponding HTTP 1.1 200 OK response from 128.119.245.12 to 172.16.1.114.

The packet details pane for packet 263 is expanded, showing the following information:

- Frame 263: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{CCCC22D-01...}
- Ethernet II, Src: Ubiquiti\_50:af:2b (68:d7:9a:50:af:2b), Dst: IntelCor\_ec:1f:4e (68:3e:26:ec:1f:4e)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.1.114
- Transmission Control Protocol, Src Port: 80, Dst Port: 51949, Seq: 1, Ack: 473, 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: Sat, 15 Oct 2022 20:16:30 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Sat, 15 Oct 2022 05:59:01 GMT\r\n
  - Etag: "80-5eb0c706c0ea4"\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 1/1]
  - [Time since request: 0.095316000 seconds]
  - [\[Request in frame: 260\]](#)
  - [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)

The packet bytes pane on the right shows the raw data of the packet, including the HTTP response structure and the HTML content.

## 2. What languages (if any) does your browser indicate that it can accept to the server?

My browser accepts en-US (US English) and en (English).

The image shows a Wireshark packet capture of an HTTP GET request. The packet list at the top shows two frames: Frame 260 (HTTP GET) and Frame 263 (HTTP 200 OK). The packet details pane for Frame 260 is expanded, showing the Hypertext Transfer Protocol section. The 'Accept-Language' header is highlighted with a red box, indicating the browser's preferred languages: en-US and en.

No.	Time	Source	Destination	Protocol	Length	Info
260	13:16:29.633841	172.16.1.114	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
263	13:16:29.729157	128.119.245.12	172.16.1.114	HTTP	540	HTTP/1.1 200 OK (text/html)

Frame 260: 526 bytes on wire (4208 bits), 526 bytes captured (4208 bits) on interface \Device\NPF\_{CCDC22D-0101-8000-0000-0000-000000000000}

Ethernet II, Src: IntelCor\_ec:1f:4e (68:3e:26:ec:1f:4e), Dst: Ubiquiti\_50:af:2b (68:d7:9a:50:af:2b)

Internet Protocol Version 4, Src: 172.16.1.114, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 51949, Dst Port: 80, Seq: 1, Ack: 1, Len: 472

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

Connection: keep-alive\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/106.0.0.0 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/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

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

[HTTP request 1/1]

[Response in frame: 263]

3. What is the IP address of your computer? 172.16.1.114  
Of the gaia.cs.umass.edu server? 128.119.245.12

The image shows a Wireshark network traffic capture window titled "\*Wi-Fi". The main display area shows a list of captured packets. Two packets are highlighted in green:

No.	Time	Source	Destination	Protocol	Length	Info
260	13:16:29.633841	172.16.1.114	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file1.html HT
263	13:16:29.729157	128.119.245.12	172.16.1.114	HTTP	540	HTTP/1.1 200 OK (text/html)

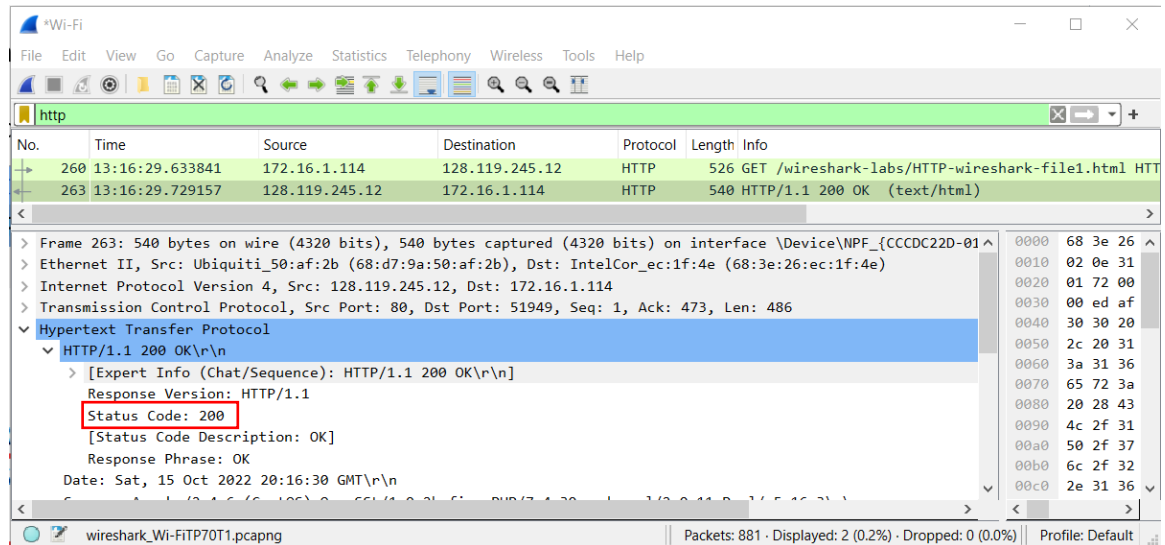
The packet details pane for packet 263 is expanded, showing the following information:

- Frame 263: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{CCDC22D-0101}
- Ethernet II, Src: Ubiquiti\_50:af:2b (68:d7:9a:50:af:2b), Dst: IntelCor\_ec:1f:4e (68:3e:26:ec:1f:4e)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.1.114
- Transmission Control Protocol, Src Port: 80, Dst Port: 51949, Seq: 1, Ack: 473, Len: 486
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
  - Date: Sat, 15 Oct 2022 20:16:30 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod\_perl/2.0.11 Perl/v5.16.3\r\n
  - Last-Modified: Sat, 15 Oct 2022 05:59:01 GMT\r\n
  - Etag: "80-5eb0c706c0ea4"\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 1/1]
  - [Time since request: 0.095316000 seconds]
  - [Request in frame: 260]
  - [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)

The packet bytes pane on the right shows the raw data in hexadecimal and ASCII format.

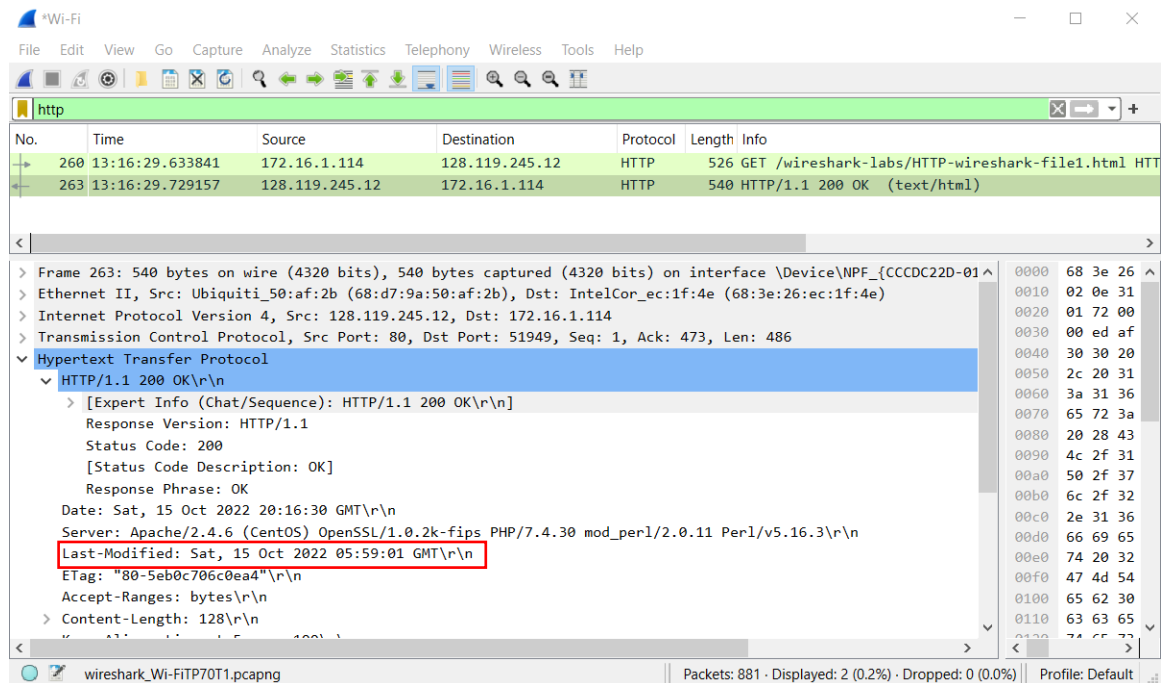
#### 4. What is the status code returned from the server to your browser?

The status code returned was 200.

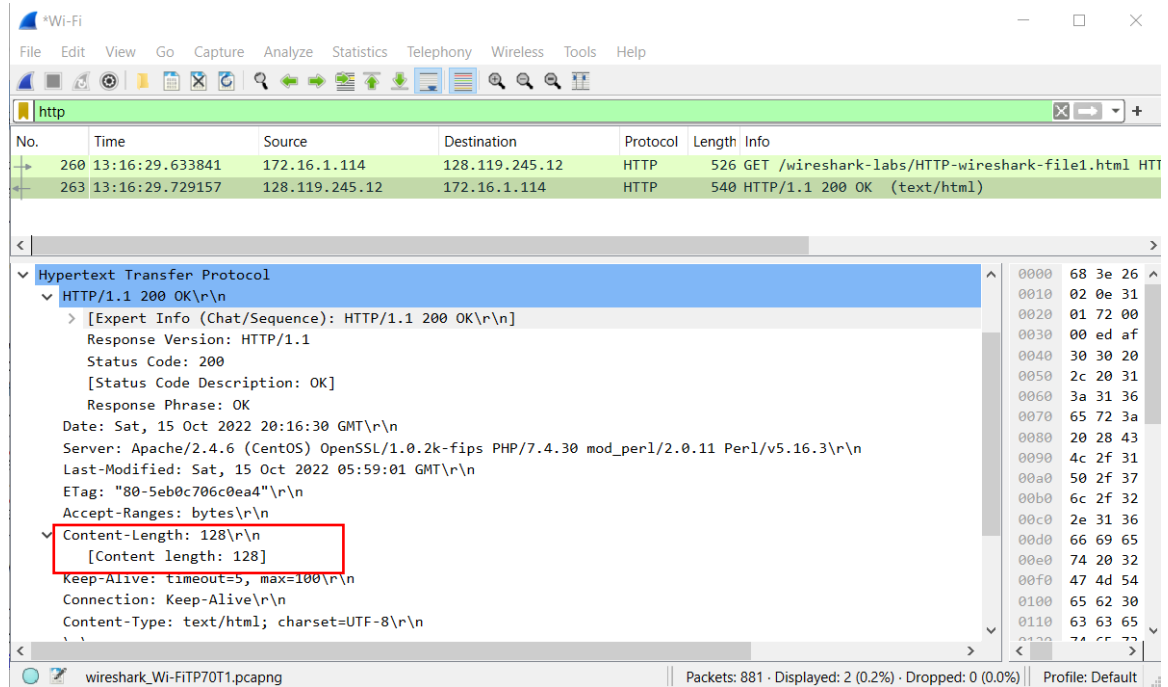


#### 5. When was the HTML file that you are retrieving last modified at the server?

This was last modified 10/15/2022 at 5:59:01 GMT



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



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, I don't see any headers that aren't displayed in the packet-listing window.

## 2. The HTTP CONDITIONAL GET/response interaction

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, the first GET request does not have an “If-Modified-Since” line.

The image shows a Wireshark network traffic capture window. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane on the left shows four packets, with packet 517 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP GET request. The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
497	16:11:03.672725	172.16.101.34	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.h
517	16:11:03.783329	128.119.245.12	172.16.101.34	HTTP	784	HTTP/1.1 200 OK (text/html)
661	16:11:15.848626	172.16.101.34	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.h
665	16:11:15.948888	128.119.245.12	172.16.101.34	HTTP	294	HTTP/1.1 304 Not Modified

**Hypertext Transfer Protocol**

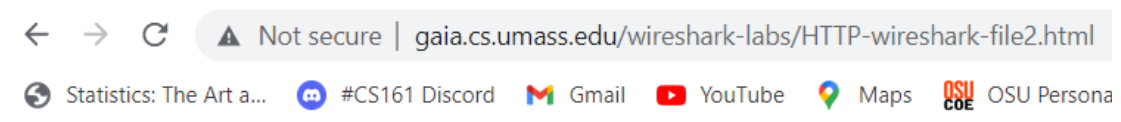
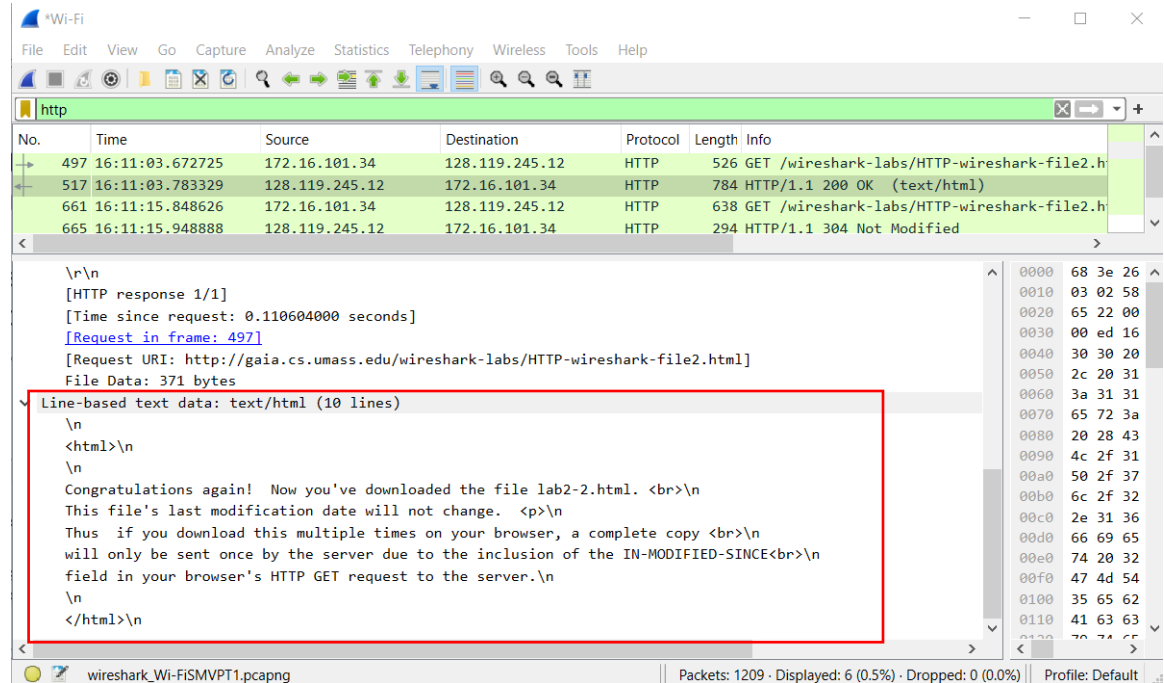
- GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
  - [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
  - Request Method: GET
  - Request URI: /wireshark-labs/HTTP-wireshark-file2.html
  - Request Version: HTTP/1.1
  - Host: gaia.cs.umass.edu\r\n
  - Connection: keep-alive\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/106.0.0
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,ap
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: en-US,en;q=0.9\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: 517]

0000 88 b1 e1  
0010 02 00 bb  
0020 f5 0c f9  
0030 01 00 88  
0040 68 61 72  
0050 69 72 65  
0060 74 6d 6c  
0070 73 74 3a  
0080 73 2e 65  
0090 6e 3a 20  
00a0 70 67 72  
00b0 52 65 71  
00c0 72 2d 41  
00d0 2f 35 2e  
00e0 20 31 30  
00f0 34 29 20  
0100 33 37 2e  
0110 6b 65 20  
0120 76 71 70

wireshark\_Wi-FISMVPT1.pcapng | Packets: 1209 · Displayed: 6 (0.5%) · Dropped: 0 (0.0%) | Profile: Default

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

Yes, the server returned the contents of the file. We can tell because the Line-based text data of the HTTP OK reply to the HTTP GET request in WireShark matches the data in the web browser.



Congratulations again! Now you've downloaded the file lab2-2.html.  
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy  
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE  
field in your browser's HTTP GET request to the server.



**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?**

Yes, the second HTTP GET request has an “If-Modified-Since” line. The information that follows it: Sat, 15 Oct 2022 05:59:01 GMT

The image shows a Wireshark packet capture window. The top pane displays a list of packets. Packet 661 is selected, showing an HTTP GET request from 172.16.101.34 to 128.119.245.12. The bottom pane shows the details of this packet, including the request URI, version, host, connection, cache-control, upgrade-insecure-requests, user-agent, accept, accept-encoding, accept-language, if-none-match, and if-modified-since. The if-modified-since header is highlighted with a red box, showing the value "Sat, 15 Oct 2022 05:59:01 GMT".

No.	Time	Source	Destination	Protocol	Length	Info
497	16:11:03.672725	172.16.101.34	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.h
517	16:11:03.783329	128.119.245.12	172.16.101.34	HTTP	784	HTTP/1.1 200 OK (text/html)
661	16:11:15.848626	172.16.101.34	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.h
665	16:11:15.948888	128.119.245.12	172.16.101.34	HTTP	294	HTTP/1.1 304 Not Modified

Request URI: /wireshark-labs/HTTP-wireshark-file2.html  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu\r\n\r\n  
Connection: keep-alive\r\n\r\n  
Cache-Control: max-age=0\r\n\r\n  
Upgrade-Insecure-Requests: 1\r\n\r\n  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,ap  
Accept-Encoding: gzip, deflate\r\n\r\n  
Accept-Language: en-US,en;q=0.9\r\n\r\n  
If-None-Match: "173-5eb0c706c02ec"\r\n\r\n  
**If-Modified-Since: Sat, 15 Oct 2022 05:59:01 GMT\r\n\r\n**  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
[HTTP request 1/2]  
[Response in frame: 665]  
[Next request in frame: 676]

**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.**

The HTTP status code and phrase is “304 Not Modified”. The server did not explicitly return the contents of the file because the file had not been modified. Since it wasn’t modified, the browser loaded the contents from its cache therefore no content length was specified.

The image shows a Wireshark packet capture window titled "\*Wi-Fi". The packet list on the left shows four packets. The fourth packet, at time 16:11:15.948888, is an HTTP 304 Not Modified response from 128.119.245.12 to 172.16.101.34. The packet details pane on the right shows the expanded view of this packet. The "Hypertext Transfer Protocol" section is expanded, showing the "HTTP/1.1 304 Not Modified\r\n" status line. The "Status Code: 304" and "[Status Code Description: Not Modified]" are highlighted with a red box. The "Response Phrase: Not Modified" is also visible. The packet bytes pane on the far right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
497	16:11:03.672725	172.16.101.34	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file2.h
517	16:11:03.783329	128.119.245.12	172.16.101.34	HTTP	784	HTTP/1.1 200 OK (text/html)
661	16:11:15.848626	172.16.101.34	128.119.245.12	HTTP	638	GET /wireshark-labs/HTTP-wireshark-file2.h
665	16:11:15.948888	128.119.245.12	172.16.101.34	HTTP	294	HTTP/1.1 304 Not Modified

▼ Hypertext Transfer Protocol  
    ▼ HTTP/1.1 304 Not Modified\r\n  
        > [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]  
            Response Version: HTTP/1.1  
            Status Code: 304  
            [Status Code Description: Not Modified]  
            Response Phrase: Not Modified  
            Date: Sat, 15 Oct 2022 23:11:16 GMT\r\n            Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod\_perl/2.0.11 Perl/v5.16.3\r\n            Connection: Keep-Alive\r\n            Keep-Alive: timeout=5, max=100\r\n            ETag: "173-5eb0c706c02ec"\r\n            \r\n            [HTTP response 1/2]  
            [Time since request: 0.100262000 seconds]  
            [Request in frame: 661]  
            [Next request in frame: 676]

### 3. Retrieving Long Documents

#### 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?

There is only one HTTP GET request message. The packet number is 171.

The image shows a Wireshark packet capture of an HTTP transaction. The packet list pane at the top shows four packets. Packet 171 is highlighted with a red box, showing it is an HTTP GET request for '/wireshark-labs/HTTP-wireshark-file3.html' from source 172.16.227.23 to destination 128.119.245.12. The packet details pane below shows the full structure of the TCP segment, including source and destination ports, sequence and acknowledgment numbers, and flags. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
171	09:22:49.372847	172.16.227.23	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
173	09:22:49.455619	128.119.245.12	172.16.227.23	HTTP	1514	HTTP/1.1 200 OK (text/html)
174	09:22:49.456468	128.119.245.12	172.16.227.23	HTTP	2974	Continuation
175	09:22:49.456468	128.119.245.12	172.16.227.23	HTTP	535	Continuation

Transmission Control Protocol, Src Port: 62053, Dst Port: 80, Seq: 1, Ack: 1, Len: 472

- Source Port: 62053
- Destination Port: 80
- [Stream index: 9]
- [Conversation completeness: Complete, WITH\_DATA (31)]
- [TCP Segment Len: 472]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 2660467672
- [Next Sequence Number: 473 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 856650705
- 0101 .... = Header Length: 20 bytes (5)
- > Flags: 0x018 (PSH, ACK)
- Window: 513
- [Calculated window size: 131328]
- [Window size scaling factor: 256]
- Checksum: 0x069f [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0

0020 f5 0c f2 65 ^  
0030 02 01 06 9f  
0040 68 61 72 6t  
0050 69 72 65 73  
0060 74 6d 6c 2e  
0070 73 74 3a 2e  
0080 73 2e 65 64  
0090 6e 3a 20 6t  
00a0 70 67 72 61  
00b0 52 65 71 75  
00c0 72 2d 41 67  
00d0 2f 35 2e 3e  
00e0 20 31 30 2e  
00f0 34 29 20 41  
0100 33 37 2e 33  
0110 6b 65 20 47  
0120 2f 31 30 3e  
0130 69 2f 35 33  
0140 3a 20 74 65  
0150 69 63 61 74

Transmission Control Protocol (tcp), 20 bytes | Packets: 240 · Displayed: 4 (1.7%) · Dropped: 0 (0.0%) | Profile: Default

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

The packet number in the trace that contains the status code and phrase is packet number 173.

The image shows a Wireshark packet capture of an HTTP GET request and its response. The packet list at the top shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
171	09:22:49.372847	172.16.227.23	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
173	09:22:49.455619	128.119.245.12	172.16.227.23	HTTP	1514	HTTP/1.1 200 OK (text/html)
174	09:22:49.456468	128.119.245.12	172.16.227.23	HTTP	2974	Continuation
175	09:22:49.456468	128.119.245.12	172.16.227.23	HTTP	535	Continuation

Packet 173 is highlighted with a red box. The packet details pane shows the following information:

- Transmission Control Protocol, Src Port: 62053, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
- Source Port: 62053
- Destination Port: 80
- [Stream index: 9]
- [Conversation completeness: Complete, WITH\_DATA (31)]
- [TCP Segment Len: 472]
- Sequence Number: 1 (relative sequence number)
- Sequence Number (raw): 2660467672
- [Next Sequence Number: 473 (relative sequence number)]
- Acknowledgment Number: 1 (relative ack number)
- Acknowledgment number (raw): 856650705
- 0101 .... = Header Length: 20 bytes (5)
- > Flags: 0x018 (PSH, ACK)
- Window: 513
- [Calculated window size: 131328]
- [Window size scaling factor: 256]
- Checksum: 0x069f [unverified]
- [Checksum Status: Unverified]
- Urgent Pointer: 0

The packet bytes pane shows the raw data of the packet, starting with 0020 f5 0c f2 65.

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

The status code is 200 and the phrase is OK.

The image shows a Wireshark network traffic analysis. The top pane displays a list of captured packets. The bottom pane shows the detailed view of the selected packet (No. 173).

**Packets List:**

No.	Time	Source	Destination	Protocol	Length	Info
171	09:22:49.372847	172.16.227.23	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
173	09:22:49.455619	128.119.245.12	172.16.227.23	HTTP	1514	HTTP/1.1 200 OK (text/html)
174	09:22:49.456468	128.119.245.12	172.16.227.23	HTTP	2974	Continuation
175	09:22:49.456468	128.119.245.12	172.16.227.23	HTTP	535	Continuation

**Packet 173 Details:**

- Transmission Control Protocol, Src Port: 62053, Dst Port: 80, Seq: 1, Ack: 1, Len: 472
  - Source Port: 62053
  - Destination Port: 80
  - [Stream index: 9]
  - [Conversation completeness: Complete, WITH\_DATA (31)]
  - [TCP Segment Len: 472]
  - Sequence Number: 1 (relative sequence number)
  - Sequence Number (raw): 2660467672
  - [Next Sequence Number: 473 (relative sequence number)]
  - Acknowledgment Number: 1 (relative ack number)
  - Acknowledgment number (raw): 856650705
  - 0101 .... = Header Length: 20 bytes (5)
  - Flags: 0x018 (PSH, ACK)
  - Window: 513
  - [Calculated window size: 131328]
  - [Window size scaling factor: 256]
  - Checksum: 0x069f [unverified]
  - [Checksum Status: Unverified]
  - Urgent Pointer: 0

**Packet 173 Hex Data:**

Offset	Hex	ASCII
0020	f5 0c f2 65	^
0030	02 01 06 9f	
0040	68 61 72 6f	
0050	69 72 65 73	
0060	74 6d 6c 2e	
0070	73 74 3a 2e	
0080	73 2e 65 64	
0090	6e 3a 20 6f	
00a0	70 67 72 61	
00b0	52 65 71 75	
00c0	72 2d 41 67	
00d0	2f 35 2e 3e	
00e0	20 31 30 2e	
00f0	34 29 20 41	
0100	33 37 2e 33	
0110	6b 65 20 47	
0120	2f 31 30 3e	
0130	69 2f 35 3e	
0140	3a 20 74 65	
0150	69 63 61 74	

**Status Bar:** Transmission Control Protocol (tcp), 20 bytes | Packets: 240 - Displayed: 4 (1.7%) - Dropped: 0 (0.0%) | Profile: Default

## 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 three data-containing TCP segments needed to carry the HTTP response.

Wireshark packet capture showing an HTTP response. The packet list shows three TCP segments (101, 175, 193) carrying the HTTP response. The packet details pane shows the reassembled TCP segments (4821 bytes) and the HTTP response (535 bytes). The packet bytes pane shows the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
24	09:22:48.244083	146.112.41.2	172.16.227.23	TLSv1.3	1293	Application Data, Application Data, Application Data
43	09:22:48.334062	172.217.14.196	172.16.227.23	TLSv1.3	218	Application Data
91	09:22:48.956051	146.112.41.2	172.16.227.23	TLSv1.3	157	Application Data
101	09:22:48.967302	146.112.41.2	172.16.227.23	TLSv1.3	1009	Application Data, Application Data, Application Data
175	09:22:49.456468	128.119.245.12	172.16.227.23	HTTP	535	HTTP/1.1 200 OK (text/html)
193	09:22:49.575584	204.79.197.200	172.16.227.23	TLSv1.2	1251	Server Hello, Certificate, Certificate Status, Server Key Exchange,
197	09:22:49.582926	172.16.227.23	204.79.197.200	TLSv1.2	775	Application Data

Frame 101: 1009 bytes on wire (8072 bits), 1009 bytes captured (8072 bits) on interface \Device\NPF\_{CCDC22D-0101-426D-BAD9-134DD9F42989}

Ethernet II, Src: CiscoMer\_20:33:22 (68:3a:1e:20:33:22), Dst: IntelCor\_ec:1f:4e (68:3e:26:ec:1f:4e)

Internet Protocol Version 4, Src: 146.112.41.2, Dst: 172.16.227.23

Transmission Control Protocol, Src Port: 443, Dst Port: 62051, Seq: 4381, Ack: 518, Len: 955

[3 Reassembled TCP Segments (4821 bytes): #97(2750), #100(1460), #101(611)]

Transport Layer Security

Transport Layer Security

Segment count: Unsigned integer (4 bytes)

Packets: 240 · Displayed: 7 (2.9%) · Dropped: 0 (0.0%)

Profile: Default

#### 4. HTML Documents with Embedded Objects

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

There were three HTTP GET requests sent. The first two were sent to 128.119.245.12 and the last one was sent to 178.79.137.164.

The image shows a Wireshark packet capture of HTTP traffic. The packet list at the top shows several GET requests. The packet details pane at the bottom shows the expanded view of the selected packet (192), displaying the full request URI and other headers.

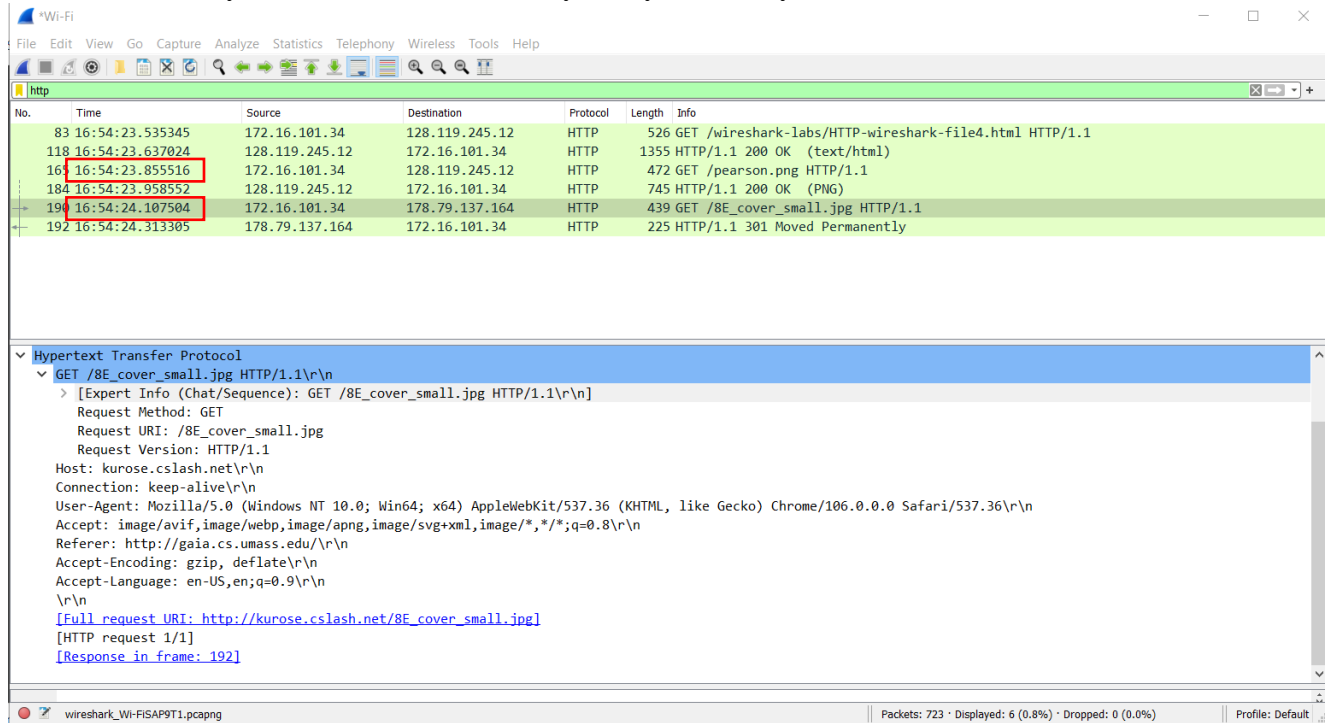
No.	Time	Source	Destination	Protocol	Length	Info
83	16:54:23.535345	172.16.101.34	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
118	16:54:23.637024	128.119.245.12	172.16.101.34	HTTP	1355	HTTP/1.1 200 OK (text/html)
165	16:54:23.855516	172.16.101.34	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
184	16:54:23.958552	128.119.245.12	172.16.101.34	HTTP	745	HTTP/1.1 200 OK (PNG)
198	16:54:24.107504	172.16.101.34	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
192	16:54:24.313305	178.79.137.164	172.16.101.34	HTTP	225	HTTP/1.1 301 Moved Permanently

**Hypertext Transfer Protocol**

- GET /8E\_cover\_small.jpg HTTP/1.1\r\n
  - [Expert Info (Chat/Sequence): GET /8E\_cover\_small.jpg HTTP/1.1\r\n]
  - Request Method: GET
  - Request URI: /8E\_cover\_small.jpg
  - Request Version: HTTP/1.1
  - Host: kurose.cslash.net\r\n
  - Connection: keep-alive\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n
  - Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8\r\n
  - Referer: http://gaia.cs.umass.edu\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: en-US,en;q=0.9\r\n
  - \r\n
  - [Full request URI: http://kurose.cslash.net/8E\_cover\_small.jpg]
  - [HTTP request 1/1]
  - [Response in frame: 192]

**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.**

When looking at the time stamp, these were sent about 1 second apart, which tells me they were downloaded serially. They were very close, but not simultaneous.



The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 192).

No.	Time	Source	Destination	Protocol	Length	Info
83	16:54:23.535345	172.16.101.34	128.119.245.12	HTTP	526	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
118	16:54:23.637024	128.119.245.12	172.16.101.34	HTTP	1355	HTTP/1.1 200 OK (text/html)
164	16:54:23.855516	172.16.101.34	128.119.245.12	HTTP	472	GET /pearson.png HTTP/1.1
184	16:54:23.958552	128.119.245.12	172.16.101.34	HTTP	745	HTTP/1.1 200 OK (PNG)
192	16:54:24.107504	172.16.101.34	178.79.137.164	HTTP	439	GET /8E_cover_small.jpg HTTP/1.1
192	16:54:24.313305	178.79.137.164	172.16.101.34	HTTP	225	HTTP/1.1 301 Moved Permanently

**Hypertext Transfer Protocol**

- GET /8E\_cover\_small.jpg HTTP/1.1\r\n
  - [Expert Info (Chat/Sequence): GET /8E\_cover\_small.jpg HTTP/1.1\r\n]
  - Request Method: GET
  - Request URI: /8E\_cover\_small.jpg
  - Request Version: HTTP/1.1
  - Host: kurose.cslash.net\r\n
  - Connection: keep-alive\r\n
  - User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36\r\n
  - Accept: image/avif,image/webp,image/apng,image/svg+xml,image/\*,\*/\*;q=0.8\r\n
  - Referer: http://gaia.cs.umass.edu/\r\n
  - Accept-Encoding: gzip, deflate\r\n
  - Accept-Language: en-US,en;q=0.9\r\n
  - \r\n
  - [Full request URI: http://kurose.cslash.net/8E\_cover\_small.jpg]
  - [HTTP request 1/1]
  - [Response in frame: 192]

Wireshark - Wi-FiSAP9T1.pcapng | Packets: 723 · Displayed: 6 (0.8%) · Dropped: 0 (0.0%) | Profile: Default



## 5 HTTP Authentication

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

The server's response to the initial HTTP GET was 401 Unauthorized.

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The bottom pane shows the details of the selected packet (No. 61), which is an HTTP 401 Unauthorized response.

No.	Time	Source	Destination	Protocol	Length	Info
59	17:09:29.958113	172.16.101.34	128.119.245.12	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
61	17:09:30.062056	128.119.245.12	172.16.101.34	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
134	17:09:52.686692	172.16.101.34	128.119.245.12	HTTP	627	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
136	17:09:52.780572	128.119.245.12	172.16.101.34	HTTP	544	HTTP/1.1 200 OK (text/html)

**Hypertext Transfer Protocol**

- HTTP/1.1 401 Unauthorized\r\n
  - [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
  - Response Version: HTTP/1.1
  - Status Code: 401
  - [Status Code Description: Unauthorized]
  - Response Phrase: Unauthorized
  - Date: Sun, 16 Oct 2022 00:09:30 GMT\r\n
  - Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 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: 0.103943000 seconds]
  - [Request in frame: 59]

wireshark\_Wi-FiGBXT1.pcapng | Packets: 177 · Displayed: 4 (2.3%) · Dropped: 0 (0.0%) | Profile: Default

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

The second HTTP GET request includes the field “Authorization: Basic” with the username and password that I entered.

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list at the top shows four packets. The selected packet (No. 61) is an HTTP GET request from 172.16.101.34 to 128.119.245.12. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the request details.

No.	Time	Source	Destination	Protocol	Length	Info
59	17:09:29.958113	172.16.101.34	128.119.245.12	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
61	17:09:30.062056	128.119.245.12	172.16.101.34	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
134	17:09:52.686692	172.16.101.34	128.119.245.12	HTTP	627	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
136	17:09:52.780572	128.119.245.12	172.16.101.34	HTTP	544	HTTP/1.1 200 OK (text/html)

**Hypertext Transfer Protocol**

- GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
  - [Expert Info (Chat/Sequence): GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
  - Request Method: GET
  - Request URI: /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html
  - Request Version: HTTP/1.1
  - Host: gaia.cs.umass.edu\r\n
  - Connection: keep-alive\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/106.0.0.0 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/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
  - \r\n
  - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html]
  - [HTTP request 1/1]
  - [Response in frame: 61]

The screenshot shows the Wireshark interface with the same packet capture. The selected packet (No. 134) is the second HTTP GET request. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the request details. A red box highlights the new 'Authorization: Basic' header field.

No.	Time	Source	Destination	Protocol	Length	Info
59	17:09:29.958113	172.16.101.34	128.119.245.12	HTTP	542	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
61	17:09:30.062056	128.119.245.12	172.16.101.34	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
134	17:09:52.686692	172.16.101.34	128.119.245.12	HTTP	627	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
136	17:09:52.780572	128.119.245.12	172.16.101.34	HTTP	544	HTTP/1.1 200 OK (text/html)

**Hypertext Transfer Protocol**

- GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
  - [Expert Info (Chat/Sequence): GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
  - Request Method: GET
  - Request URI: /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html
  - Request Version: HTTP/1.1
  - Host: gaia.cs.umass.edu\r\n
  - Connection: keep-alive\r\n
  - Cache-Control: max-age=0\r\n
  - Authorization: Basic d2lyZXNoYXJrLXN0dWR1bnRzOm5ldHdvcm0=\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/106.0.0.0 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/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
  - \r\n
  - [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html]

