

# **The Basic HTTP** **GET/response interaction**

Questions 1 to 7

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

Answer: Browser: HTTP 1.1

Wireshark packet capture showing an HTTP GET request from a browser to a server. The request is for `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html` and is version 1.1. A red box highlights `HTTP/1.1\r\n` in the request line, with a red arrow pointing to it.

No.	Time	Source	Destination	Protocol	Length	Info
591	4.341444	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
618	4.577545	128.119.245.12	40.40.9.226	HTTP	540	HTTP/1.1 200 OK (text/html)
650	4.781594	40.40.9.226	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
683	5.030151	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 591: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{D39F8ACF-4F74-4DBB-BB78-D636B11ACB0D}, id 0

Ethernet II, Src: Intel\_47:d5:29 (80:86:f2:47:d5:29), Dst: Routerboardc\_67:3d:40 (08:55:31:67:3d:40)

Internet Protocol Version 4, Src: 40.40.9.226, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 63540, Dst Port: 80, Seq: 1, Ack: 1, Len: 486

Hypertext Transfer Protocol

- 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/135.0.0.0 Safari/537.36 Edg/135.0.0.0\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=0.7\r\n
- Accept-Encoding: gzip, deflate\r\n
- Accept-Language: en-US,en;q=0.9\r\n
- \r\n
- [Response in frame: 618]
- [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]

Destination Hardware Address (eth.dst), 6 bytes

Packets: 804 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%)

Profile: Default

Server: HTTP 1.1

Wireshark packet capture showing an HTTP 200 OK response from a server to a browser. The response is for `http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html` and is version 1.1. A red box highlights `HTTP/1.1 200 OK\r\n` in the status line, with a red arrow pointing to it.

No.	Time	Source	Destination	Protocol	Length	Info
591	4.341444	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
618	4.577545	128.119.245.12	40.40.9.226	HTTP	540	HTTP/1.1 200 OK (text/html)
650	4.781594	40.40.9.226	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
683	5.030151	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 618: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{D39F8ACF-4F74-4DBB-BB78-D636B11ACB0D}, id 0

Ethernet II, Src: Routerboardc\_67:3d:40 (08:55:31:67:3d:40), Dst: Intel\_47:d5:29 (80:86:f2:47:d5:29)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 40.40.9.226

Transmission Control Protocol, Src Port: 80, Dst Port: 63540, Seq: 1, Ack: 487, Len: 486

Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
- Response Version: HTTP/1.1
- Status Code: 200
- [Status Code Description: OK]
- Response Phrase: OK
- Date: Sun, 04 May 2025 03:41:43 GMT\r\n
- Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n
- Last-Modified: Sat, 03 May 2025 05:59:02 GMT\r\n
- ETag: "80-63434f6b5b677"\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
- [Request in frame: 591]
- [Time since request: 0.236101000 seconds]
- [Request URI: /wireshark-labs/HTTP-wireshark-file1.html]
- [Full 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)

Destination Hardware Address (eth.dst), 6 bytes

Packets: 804 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%)

Profile: Default

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

Answer: English

Wireshark packet capture showing an HTTP GET request. The packet details pane highlights the 'Accept-Language' header, which is set to 'en-US,en;q=0.9'. A red box and arrow point to this header.

Destination Hardware Address (eth.dst), 6 bytes | Packets: 804 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%) | Profile: Default

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

Answer: My PC: 40.40.9.226 & Server: 128.119.245.12

Wireshark packet capture showing an HTTP GET request. The packet details pane highlights the 'Source Address' (40.40.9.226) and the 'Destination Address' (128.119.245.12). Red boxes and arrows point to these addresses.

Destination Hardware Address (eth.dst), 6 bytes | Packets: 804 · Displayed: 4 (0.5%) · Dropped: 0 (0.0%) | Profile: Default

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

Answer: Status Code: 200

The image shows a Wireshark packet capture of an HTTP transaction. The packet list pane at the top shows four packets. Packet 618 is the HTTP response, which is expanded in the packet details pane. A red arrow points to the '200 OK' status code in the 'Hypertext Transfer Protocol' section. The packet bytes pane on the right shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
591	4.341444	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
618	4.577545	128.119.245.12	40.40.9.226	HTTP	540	HTTP/1.1 200 OK (text/html)
650	4.781594	40.40.9.226	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
683	5.030151	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 618: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{D39F8ACF-4F74-40BB-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Routerboardc\_67:3d:40 (08:55:31:67:3d:40), Dst: Intel\_47:d5:29 (80:86:f2:47:d5:29)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 40.40.9.226  
> Transmission Control Protocol, Src Port: 80, Dst Port: 63540, Seq: 1, Ack: 487, Len: 486  
Hypertext Transfer Protocol  
 HTTP/1.1 200 OK\r\n  
 Response Version: HTTP/1.1  
 Status Code: 200  
 [Status Code Description: OK]  
 Response Phrase: OK  
 Date: Sun, 04 May 2025 03:41:43 GMT\r\n Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n Last-Modified: Sat, 03 May 2025 05:59:02 GMT\r\n ETag: "80-63434f6b5b677"\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 [Request in frame: 591]  
 [Time since request: 0.236101000 seconds]  
 [Request URI: /wireshark-labs/HTTP-wireshark-file1.html]  
 [Full 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)

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

Answer: Last Modified: Sat, 03 May 2025 05:59:02 GMT

The image shows the same Wireshark packet capture as above, but with the 'Last-Modified' header in the 'Hypertext Transfer Protocol' section highlighted with a red box and a red arrow. The header indicates the file was last modified on Saturday, May 3, 2025, at 05:59:02 GMT.

No.	Time	Source	Destination	Protocol	Length	Info
591	4.341444	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
618	4.577545	128.119.245.12	40.40.9.226	HTTP	540	HTTP/1.1 200 OK (text/html)
650	4.781594	40.40.9.226	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
683	5.030151	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 618: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{D39F8ACF-4F74-40BB-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Routerboardc\_67:3d:40 (08:55:31:67:3d:40), Dst: Intel\_47:d5:29 (80:86:f2:47:d5:29)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 40.40.9.226  
> Transmission Control Protocol, Src Port: 80, Dst Port: 63540, Seq: 1, Ack: 487, Len: 486  
Hypertext Transfer Protocol  
 HTTP/1.1 200 OK\r\n  
 Response Version: HTTP/1.1  
 Status Code: 200  
 [Status Code Description: OK]  
 Response Phrase: OK  
 Date: Sun, 04 May 2025 03:41:43 GMT\r\n Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n Last-Modified: Sat, 03 May 2025 05:59:02 GMT\r\n ETag: "80-63434f6b5b677"\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 [Request in frame: 591]  
 [Time since request: 0.236101000 seconds]  
 [Request URI: /wireshark-labs/HTTP-wireshark-file1.html]  
 [Full 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)

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

Answer: Bytes: 128

Wireshark packet capture showing an HTTP 200 OK response. The packet listing window shows packet 618 as an HTTP GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details window shows the response structure, including the Content-Length: 128 header, which is highlighted with a red box and an arrow. The packet bytes window shows the raw data in hexadecimal and ASCII.

## 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.

Answer: Content-Type: text/html; charset=UTF-8\r\n

Wireshark packet capture showing an HTTP 200 OK response. The packet listing window shows packet 618 as an HTTP GET request for /wireshark-labs/HTTP-wireshark-file1.html. The packet details window shows the response structure, including the Content-Type: text/html; charset=UTF-8\r\n header, which is highlighted with a red box and an arrow. The packet bytes window shows the raw data in hexadecimal and ASCII.

## **The HTTP CONDITIONAL GET/response interaction**

Questions 8 to 11

## 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?

Answer: No, “IF-MODIFIED-SINCE” line.

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list on the left shows packet 114 as the first GET request. The packet details pane on the right shows the structure of the request, including the method (GET), URI, version, host, and various headers. The packet bytes pane on the far right shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
114	3.437094	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
124	3.746194	128.119.245.12	40.40.9.226	HTTP	784	HTTP/1.1 200 OK (text/html)
194	6.691408	40.40.9.226	128.119.245.12	HTTP	583	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
200	6.936056	128.119.245.12	40.40.9.226	HTTP	783	HTTP/1.1 200 OK (text/html)
202	7.020253	40.40.9.226	128.119.245.12	HTTP	529	GET /favicon.ico HTTP/1.1
203	7.274836	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)
217	9.648311	40.40.9.226	128.119.245.12	HTTP	583	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
224	9.896568	128.119.245.12	40.40.9.226	HTTP	783	HTTP/1.1 200 OK (text/html)
226	9.954808	40.40.9.226	128.119.245.12	HTTP	529	GET /favicon.ico HTTP/1.1
229	10.197482	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 114: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{D39F8ACF-4F74-4DBB-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Intel\_47:d5:29 (80:86:f2:47:d5:29), Dst: Routerboardc\_67:3d:40 (08:55:31:67:3d:40)  
> Internet Protocol Version 4, Src: 40.40.9.226, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 51972, Dst Port: 80, Seq: 1, Ack: 1, Len: 486  
> Hypertext Transfer Protocol  
GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\nRequest Method: GET\r\nRequest URI: /wireshark-labs/HTTP-wireshark-file2.html\r\nRequest Version: HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0\r\nAccept: 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=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Response in frame: 124]  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

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

Answer: Text return in response.

The screenshot shows the Wireshark interface with a packet capture of an HTTP 200 OK response. The packet list on the left shows packet 124 as the first response. The packet details pane on the right shows the structure of the response, including the status line, headers, and the body. The packet bytes pane on the far right shows the raw data in hexadecimal and ASCII. A red box highlights the body of the response, which contains the text of the file.

No.	Time	Source	Destination	Protocol	Length	Info
114	3.437094	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
124	3.746194	128.119.245.12	40.40.9.226	HTTP	784	HTTP/1.1 200 OK (text/html)
194	6.691408	40.40.9.226	128.119.245.12	HTTP	583	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
200	6.936056	128.119.245.12	40.40.9.226	HTTP	783	HTTP/1.1 200 OK (text/html)
202	7.020253	40.40.9.226	128.119.245.12	HTTP	529	GET /favicon.ico HTTP/1.1
203	7.274836	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)
217	9.648311	40.40.9.226	128.119.245.12	HTTP	583	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
224	9.896568	128.119.245.12	40.40.9.226	HTTP	783	HTTP/1.1 200 OK (text/html)
226	9.954808	40.40.9.226	128.119.245.12	HTTP	529	GET /favicon.ico HTTP/1.1
229	10.197482	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Accept-Ranges: bytes\r\nContent-Length: 371\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[Request in frame: 114]  
[Time since request: 0.309100000 seconds]  
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]  
File Data: 271 bytes  
Line-based text data: text/html (10 lines)  
\n<html>\n\n\nCongratulations again! Now you've downloaded the file lab2-2.html. <br>\nThis file's last modification date will not change. <p>\nThus if you download this multiple times on your browser, a complete copy <br>\nwill only be sent once by the server due to the inclusion of the IF-MODIFIED-SINCE field in your browser's HTTP GET request to the server.\n\n</html>\n



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?

Answer: If-Modified-Since: Sat, 03 2025 05:59:02 GMT\r\n

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. The second packet (No. 1367) is selected, showing it is an HTTP GET request from 40.40.9.226 to 128.119.245.12. The bottom pane shows the details of this packet, specifically the Hypertext Transfer Protocol section. The request line is 'GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n'. The 'Host' is 'gaia.cs.umass.edu\r\n'. The 'Accept' header is '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=0.7\r\n'. The 'Accept-Encoding' is 'gzip, deflate\r\n'. The 'Accept-Language' is 'en-US,en;q=0.9\r\n'. The 'If-None-Match' header is '173-63434f6b5aea7"\r\n'. The 'If-Modified-Since' header is 'Sat, 03 May 2025 05:59:02 GMT\r\n\r\n'. A red box highlights the 'If-Modified-Since' header, and a red arrow points to it from the right. The bottom status bar shows 'Packets: 1389 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
1331	3.778598	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1342	4.026881	128.119.245.12	40.40.9.226	HTTP	784	HTTP/1.1 200 OK (text/html)
1367	6.950125	40.40.9.226	128.119.245.12	HTTP	652	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1372	7.183584	128.119.245.12	40.40.9.226	HTTP	293	HTTP/1.1 304 Not Modified

```
> Frame 1367: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits) on interface \Device\NPF_{D39F8ACF-4F74-40B8-BB78-D636B11ACB0D}, id 0
> Ethernet II, Src: Intel_47:d5:29 (88:86:f2:47:d5:29), Dst: Routerboardc_67:3d:40 (08:55:31:67:3d:40)
> Internet Protocol Version 4, Src: 40.40.9.226, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 52832, Dst Port: 80, Seq: 487, Ack: 731, Len: 598
v Hypertext Transfer Protocol
  > GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36 Edg/135.0.0.0\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=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
    If-None-Match: "173-63434f6b5aea7"\r\n
    If-Modified-Since: Sat, 03 May 2025 05:59:02 GMT\r\n\r\n
    [response in frame: 1372]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```



**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.**

**Answer:** 304 Not Modified. The server did not explicitly return the contents.

The image shows a Wireshark packet capture window titled "Wi-Fi". The packet list pane displays four packets. Packet 1372 is an HTTP response with status code 304 (Not Modified). The packet details pane shows the structure of the HTTP response, with the status line "HTTP/1.1 304 Not Modified" highlighted by a red box and a red arrow. The status code 304 is also highlighted by a red box. The response phrase "Not Modified" is visible. The packet bytes pane shows the raw data of the response, which is empty except for the status line and headers.

No.	Time	Source	Destination	Protocol	Length	Info
1331	3.778598	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1342	4.026881	128.119.245.12	40.40.9.226	HTTP	784	HTTP/1.1 200 OK (text/html)
1367	6.950125	40.40.9.226	128.119.245.12	HTTP	652	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1372	7.183584	128.119.245.12	40.40.9.226	HTTP	293	HTTP/1.1 304 Not Modified

Frame 1372: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF\_{D39F8ACF-4F74-4DB8-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Routerboardc\_67:3d:40 (08:55:31:67:3d:40), Dst: Intel\_47:d5:29 (80:86:f2:47:d5:29)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 40.40.9.226  
> Transmission Control Protocol, Src Port: 80, Dst Port: 52832, Seq: 731, Ack: 1085, Len: 239  
Hypertext Transfer Protocol  
HTTP/1.1 304 Not Modified  
Response Version: HTTP/1.1  
Status Code: 304  
[Status Code Description: Not Modified]  
Response Phrase: Not Modified  
Date: Sun, 04 May 2025 04:41:41 GMT  
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3  
Connection: Keep-Alive  
Keep-Alive: timeout=5, max=99  
ETag: "173-63434f6b5aea7"  
\\r\\n  
[Request in frame: 1367]  
[Time since request: 0.233459000 seconds]  
[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

## **Retrieving Long Documents**

Questions 12 to 15

## 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?

**Answer:** 1 HTTP GET request send & Packet Number is 650.

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list pane shows four packets, with packet 650 highlighted. The packet details pane shows the structure of the HTTP GET request, including the host, connection, and user-agent. The packet bytes pane shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
650	3.726263	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
666	4.015041	128.119.245.12	40.40.9.226	HTTP	535	HTTP/1.1 200 OK (text/html)
679	4.214349	40.40.9.226	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
695	4.504012	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 650: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF\_{D39F8ACF-4F74-40BB-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Intel\_47:d5:29 (80:86:f2:d5:29), Dst: Routerboardc\_67:3d:40 (08:55:31:67:3d:40)  
> Internet Protocol Version 4, Src: 40.40.9.226, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 52334, Dst Port: 80, Seq: 1, Ack: 1, Len: 486  
> Hypertext Transfer Protocol  
GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Edg/136.0.0.0\r\nAccept: 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=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Response in frame: 666]  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

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

**Answer:** Packet 666

The screenshot shows the Wireshark interface with a packet capture of an HTTP 200 OK response. The packet list pane shows four packets, with packet 666 highlighted. The packet details pane shows the structure of the HTTP 200 OK response, including the status code, date, server, and content-type. The packet bytes pane shows the raw data of the response.

No.	Time	Source	Destination	Protocol	Length	Info
650	3.726263	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
666	4.015041	128.119.245.12	40.40.9.226	HTTP	535	HTTP/1.1 200 OK (text/html)
679	4.214349	40.40.9.226	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
695	4.504012	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 666: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF\_{D39F8ACF-4F74-40BB-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Routerboardc\_67:3d:40 (08:55:31:67:3d:40), Dst: Intel\_47:d5:29 (80:86:f2:d5:29)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 40.40.9.226  
> Transmission Control Protocol, Src Port: 80, Dst Port: 52334, Seq: 4381, Ack: 487, Len: 481  
> [4 Reassembled TCP Segments (4861 bytes): #663(1460), #664(1460), #665(1460), #666(481)]  
> Hypertext Transfer Protocol  
HTTP/1.1 200 OK\r\nDate: Sun, 04 May 2025 07:07:14 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\nLast-Modified: Sun, 04 May 2025 05:59:02 GMT\r\nETag: "1194-63449148aba13"\r\nAccept-Ranges: bytes\r\nContent-Length: 4500\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=UTF-8\r\n\r\n[Request in frame: 650]  
[Time since request: 0.288778000 seconds]  
[Request URI: /wireshark-labs/HTTP-wireshark-file3.html]  
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]  
File Data: 4500 bytes

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

Answer: Status Code: 200

The image shows a Wireshark packet capture of an HTTP response. The packet list pane shows several packets, with packet 666 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section shows the status code 200 OK. A red box highlights the status code and phrase, and a red arrow points to it from the text 'Answer: Status Code: 200'.

No.	Time	Source	Destination	Protocol	Length	Info
650	3.726263	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
666	4.015041	128.119.245.12	40.40.9.226	HTTP	535	HTTP/1.1 200 OK (text/html)
679	4.214349	40.40.9.226	128.119.245.12	HTTP	486	GET /favicon.ico HTTP/1.1
695	4.504012	128.119.245.12	40.40.9.226	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Frame 666: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF\_{D39F8ACF-4F74-40BB-BB78-D636B11AC800}, id 0

Ethernet II, Src: Routerboardc\_67:3d:40 (08:55:31:67:3d:40), Dst: Intel\_47:d5:29 (80:86:f2:47:d5:29)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 40.40.9.226

Transmission Control Protocol, Src Port: 80, Dst Port: 52334, Seq: 4381, Ack: 487, Len: 481

[4 Reassembled TCP Segments (4861 bytes): #663(1460), #664(1460), #665(1460), #666(481)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Sun, 04 May 2025 07:07:14 GMT\r\n

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\n

Last-Modified: Sun, 04 May 2025 05:59:02 GMT\r\n

ETag: "1194-63449148aba13"\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

[Request in frame: 650]

[Time since request: 0.288778000 seconds]

[Request URI: /wireshark-labs/HTTP-wireshark-file3.html]

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]

File Data: 4500 bytes

Line-based text data: text/html (08 lines)

Packets: 1304 · Displayed: 4 (0.3%) · 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?

Answer: 9 TCP segments.

The image shows a Wireshark packet capture of an HTTP response. The packet list pane shows several packets, with packet 666 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section shows the status code 200 OK. A red box highlights the status code and phrase, and a red arrow points to it from the text 'Answer: Status Code: 200'.

No.	Time	Source	Destination	Protocol	Length	Info
649	3.725541	40.40.9.226	128.119.245.12	TCP	54	52334 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
650	3.726263	40.40.9.226	128.119.245.12	HTTP	540	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
651	3.735482	40.40.9.226	20.42.65.93	TCP	54	52273 → 443 [ACK] Seq=16694 Ack=387 Win=514 Len=0
652	3.740146	128.119.245.12	40.40.9.226	TCP	66	80 → 52333 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
653	3.740394	40.40.9.226	128.119.245.12	TCP	54	52333 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
654	3.742238	4.144.165.14	40.40.9.226	TCP	60	443 → 52335 [ACK] Seq=10035 Ack=4704 Win=64512 Len=0
655	3.887151	40.40.9.226	52.182.143.214	TLSv1.2	138	Application Data
656	3.887254	40.40.9.226	52.182.143.214	TLSv1.2	93	Application Data
657	3.887305	40.40.9.226	52.182.143.214	TLSv1.2	1145	Application Data
658	3.943012	20.42.65.93	40.40.9.226	TLSv1.2	365	Application Data
659	3.953116	128.119.245.12	40.40.9.226	TCP	66	80 → 52336 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
660	3.953387	40.40.9.226	128.119.245.12	TCP	54	52336 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
661	3.985272	40.40.9.226	20.42.65.93	TCP	54	52273 → 443 [ACK] Seq=16694 Ack=698 Win=513 Len=0
662	4.013994	128.119.245.12	40.40.9.226	TCP	60	80 → 52334 [ACK] Seq=1 Ack=487 Win=30336 Len=0
663	4.015041	128.119.245.12	40.40.9.226	TCP	1514	80 → 52334 [ACK] Seq=1 Ack=487 Win=30336 Len=1460 [TCP PDU reassembled in 666]
664	4.015041	128.119.245.12	40.40.9.226	TCP	1514	80 → 52334 [ACK] Seq=1461 Ack=487 Win=30336 Len=1460 [TCP PDU reassembled in 666]
665	4.015041	128.119.245.12	40.40.9.226	TCP	1514	80 → 52334 [ACK] Seq=2921 Ack=487 Win=30336 Len=1460 [TCP PDU reassembled in 666]
666	4.015041	128.119.245.12	40.40.9.226	HTTP	535	HTTP/1.1 200 OK (text/html)
667	4.015356	40.40.9.226	128.119.245.12	TCP	54	52334 → 80 [ACK] Seq=487 Ack=4862 Win=131328 Len=0
668	4.132292	52.182.143.214	40.40.9.226	TCP	60	443 → 52027 [ACK] Seq=1 Ack=1215 Win=16385 Len=0
669	4.132292	52.182.143.214	40.40.9.226	TLSv1.2	93	Application Data
670	4.138659	52.182.143.214	40.40.9.226	TLSv1.2	86	Application Data
671	4.138731	40.40.9.226	52.182.143.214	TCP	54	52027 → 443 [ACK] Seq=1215 Ack=72 Win=514 Len=0

Packets: 1304 · Displayed: 565 (43.3%) · Selected: 2 (0.2%) · Dropped: 0 (0.0%) Profile: Default

## **HTML Documents with Embedded Objects**

Questions 16 to 17

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

Answer: 3 HTTP GET request & 128.119.245.12 and 178.79.137.164 IP were sent GET request.

The screenshot shows a Wireshark packet capture of an HTTP session. The packet list pane displays several HTTP messages. Red boxes and arrows highlight the following:

- Packet 51: GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 from 40.40.9.226 to 128.119.245.12.
- Packet 128: 200 OK (text/html) from 128.119.245.12 to 40.40.9.226.
- Packet 137: GET /pearson.png HTTP/1.1 from 40.40.9.226 to 128.119.245.12.
- Packet 160: 200 OK (PNG) from 128.119.245.12 to 40.40.9.226.
- Packet 175: GET /8E\_cover\_small.jpg HTTP/1.1 from 40.40.9.226 to 178.79.137.164.
- Packet 183: 301 Moved Permanently from 178.79.137.164 to 40.40.9.226.

The packet details pane for packet 128 shows the full HTTP response, including headers like Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length, Keep-Alive, Connection, Content-Type, and the body content.

## 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.

Answer: Download in parallel & browser sent two GET requests to retrieve two images simultaneously.

The screenshot shows a Wireshark packet capture of an HTTP session. The packet list pane displays several HTTP messages. Red boxes and arrows highlight the following:

- Packet 51: GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1 from 40.40.9.226 to 128.119.245.12.
- Packet 128: 200 OK (text/html) from 128.119.245.12 to 40.40.9.226.
- Packet 137: GET /pearson.png HTTP/1.1 from 40.40.9.226 to 128.119.245.12.
- Packet 160: 200 OK (PNG) from 128.119.245.12 to 40.40.9.226.
- Packet 175: GET /8E\_cover\_small.jpg HTTP/1.1 from 40.40.9.226 to 178.79.137.164.
- Packet 183: 301 Moved Permanently from 178.79.137.164 to 40.40.9.226.

The packet details pane for packet 128 shows the full HTTP response, including headers like Date, Server, Last-Modified, ETag, Accept-Ranges, Content-Length, Keep-Alive, Connection, Content-Type, and the body content.

## **HTTP Authentication**

Questions 18 to 19



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

**Answer:** HTTP/1.1 401 Unauthorized \r\n

The screenshot shows a Wireshark capture of an HTTP transaction. The packet list on the left shows several packets, with packet 721 (HTTP/1.1 401 Unauthorized) highlighted. The packet details pane on the right shows the structure of the HTTP response, including the status line 'HTTP/1.1 401 Unauthorized\r\n', response version, status code, status code description, response phrase, date, server information, WWW-Authenticate header, content length, keep-alive, connection, content type, and request URI. A red arrow points to the status line in the details pane.

No.	Time	Source	Destination	Protocol	Length	Info
527	0.899230	40.40.9.226	128.119.245.12	HTTP	55	Continuation
644	3.229996	40.40.9.226	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
721	3.507493	128.119.245.12	40.40.9.226	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
864	13.773352	40.40.9.226	128.119.245.12	HTTP	640	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
868	14.057057	128.119.245.12	40.40.9.226	HTTP	583	HTTP/1.1 404 Not Found (text/html)

Frame 721: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF\_{D39F8ACF-4F74-4D8B-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Routerboardc\_67:3d:40 (08:55:31:67:3d:40), Dst: Intel\_47:d5:29 (08:86:f2:47:d5:29)  
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 40.40.9.226  
> Transmission Control Protocol, Src Port: 80, Dst Port: 53640, Seq: 1, Ack: 503, Len: 717  
Hypertext Transfer Protocol  
HTTP/1.1 401 Unauthorized\r\n  
Response Version: HTTP/1.1  
Status Code: 401  
[Status Code Description: Unauthorized]  
Response Phrase: Unauthorized  
Date: Sun, 04 May 2025 08:48:37 GMT\r\nServer: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod\_perl/2.0.11 Perl/v5.16.3\r\nWWW-Authenticate: Basic realm="wireshark-students only"\r\nContent-Length: 381\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: text/html; charset=iso-8859-1\r\n\r\n[Request in frame: 644]  
[Time since request: 0.277497000 seconds]  
[Request URI: /wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html]

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

**Answer:** Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs=\r\n

The screenshot shows a Wireshark capture of a second HTTP transaction. The packet list on the left shows several packets, with packet 864 (HTTP GET) highlighted. The packet details pane on the right shows the structure of the HTTP request, including the request method, request URI, request version, host, connection, cache-control, authorization, upgrade-insecure-requests, user-agent, accept, accept-encoding, accept-language, and request URI. A red arrow points to the Authorization header in the details pane.

No.	Time	Source	Destination	Protocol	Length	Info
527	0.899230	40.40.9.226	128.119.245.12	HTTP	55	Continuation
644	3.229996	40.40.9.226	128.119.245.12	HTTP	555	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
721	3.507493	128.119.245.12	40.40.9.226	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
864	13.773352	40.40.9.226	128.119.245.12	HTTP	640	GET /wireshark-labs/protected_pages/HTTP-wiresharkfile5.html HTTP/1.1
868	14.057057	128.119.245.12	40.40.9.226	HTTP	583	HTTP/1.1 404 Not Found (text/html)

Frame 864: 640 bytes on wire (5120 bits), 640 bytes captured (5120 bits) on interface \Device\NPF\_{D39F8ACF-4F74-4D8B-BB78-D636B11ACB0D}, id 0  
> Ethernet II, Src: Intel\_47:d5:29 (08:86:f2:47:d5:29), Dst: Routerboardc\_67:3d:40 (08:55:31:67:3d:40)  
> Internet Protocol Version 4, Src: 40.40.9.226, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 53704, Dst Port: 80, Seq: 1, Ack: 1, Len: 586  
Hypertext Transfer Protocol  
GET /wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html HTTP/1.1\r\nRequest Method: GET  
Request URI: /wireshark-labs/protected\_pages/HTTP-wiresharkfile5.html  
Request Version: HTTP/1.1  
Host: gaia.cs.umass.edu\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nAuthorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcmcs=\r\nCredentials: wireshark-students:network  
Upgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36 Edg/136.0.0.0\r\nAccept: 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=0.7\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9\r\n\r\n[Response in frame: 868]