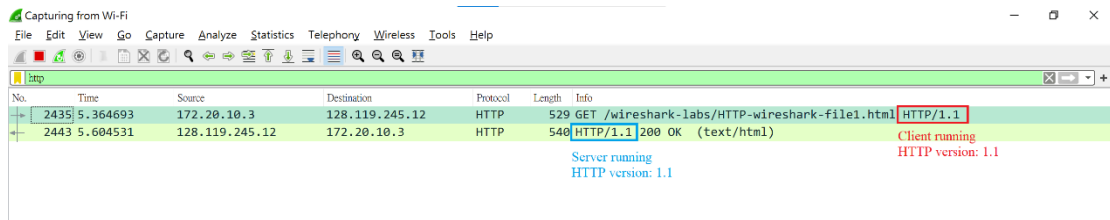


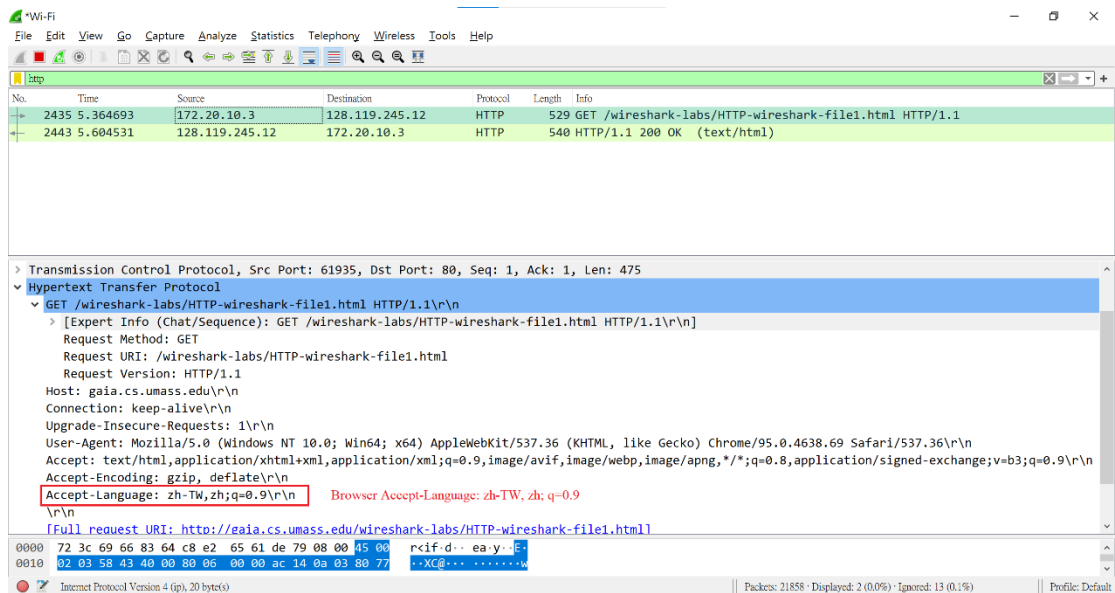
1. Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Ans : Browser running HTTP version: 1.1, Server too.



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

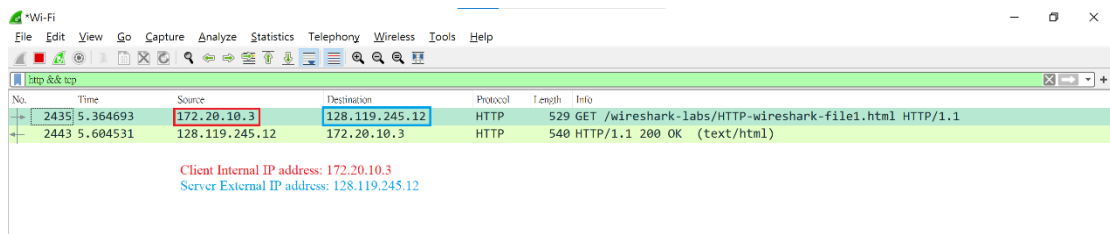
Ans : zh-TW, zh; q=0.9.



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

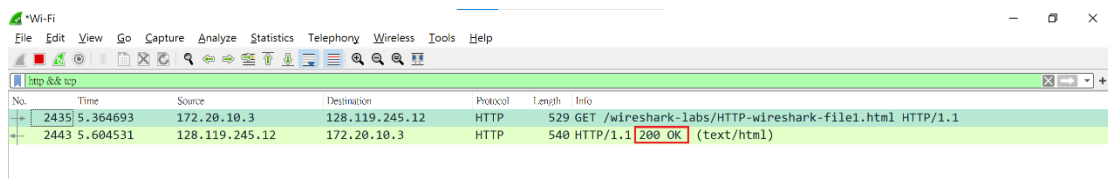
Ans : My computer Internal IP address: 172.20.10.3.

Server External IP address: 128.119.245.12.



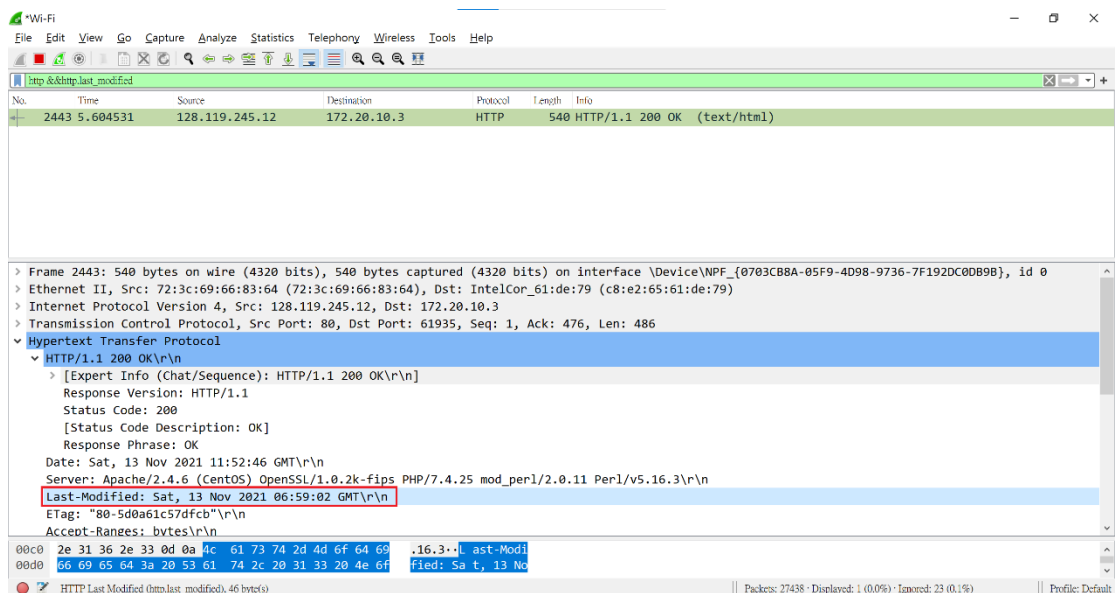
4. What is the status code returned from the server to your browser?

Ans : 200 OK



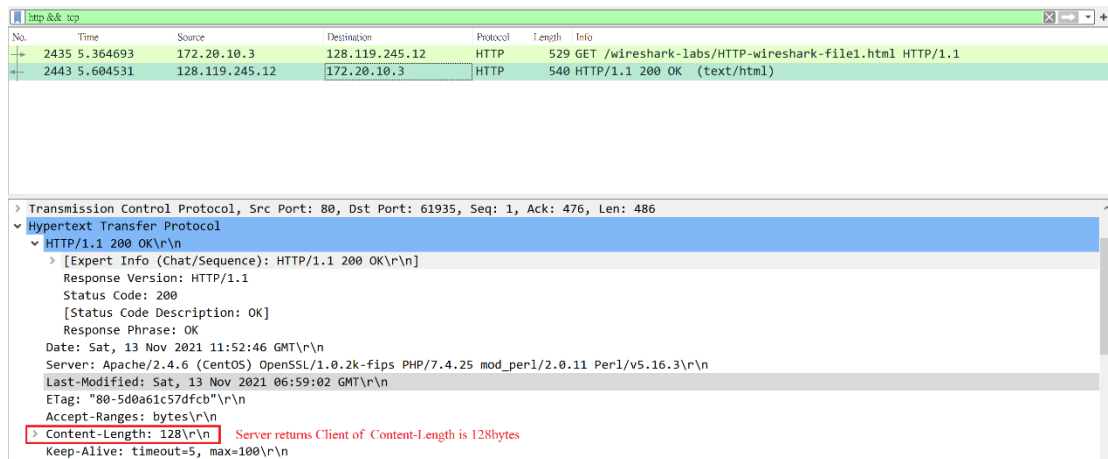
5. When was the HTML file that you are retrieving last modified at the server?

Ans : We can filter messages by http.last\_modified and we see that the HTTP response I received for the html file doesn't show this field. but we do have a http.last\_modified field in the favicon response, however, we could found the last modified on "Sat, 13 Nov 2021 06:59:02 GMT".



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

Ans : 128 bytes

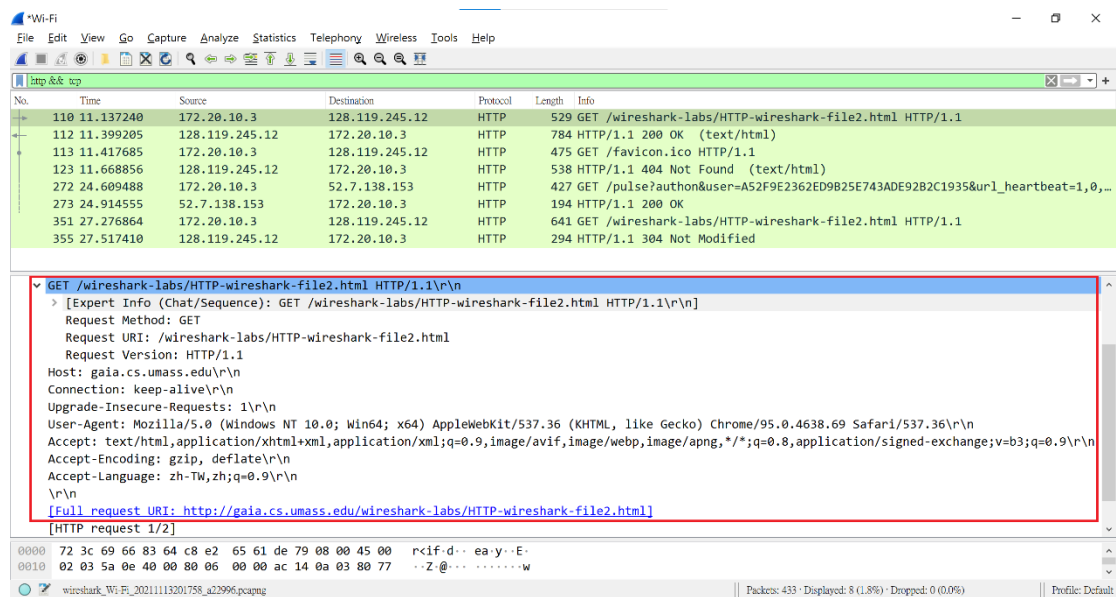


7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.

Ans : No, all of the headers can be found in the raw data.

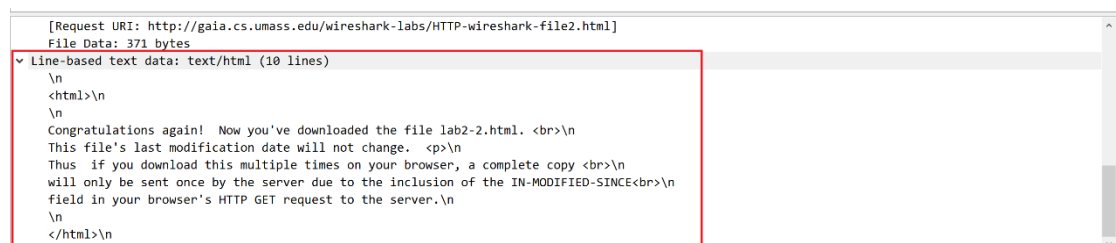
8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

Ans : No, I can't see “IF-MODIFIED-SINCE” in the HTTP GET.



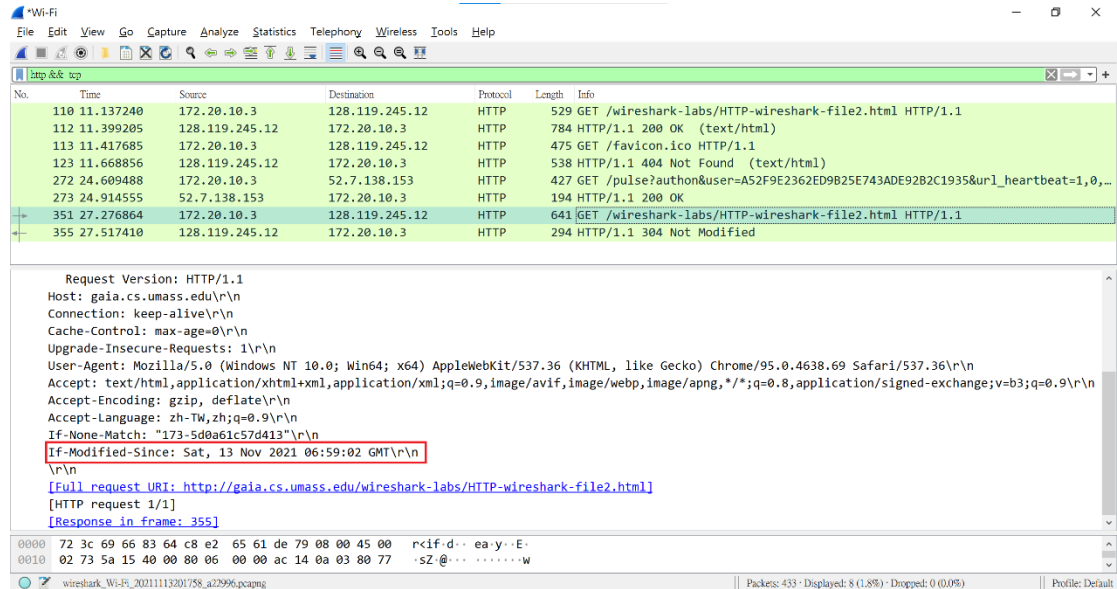
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

Ans : Yes, because I could see the content in the “Line-based text data” field and my Browser.



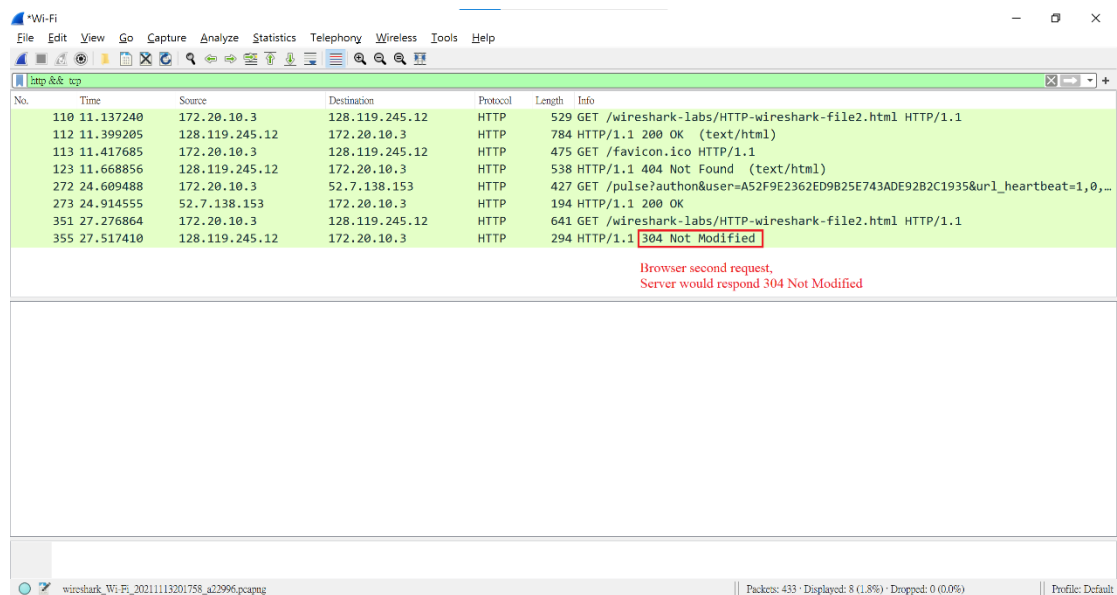
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE:” line in the HTTP GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

Ans : Yes, If-Modified-since: Sat, 13 Nov 2021 06:59:02 GMT.



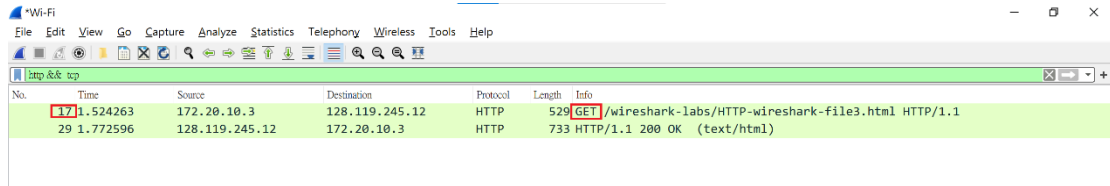
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.

Ans : The status code and phrase returned from the server is HTTP/1.1 304 Not Modified. The server didn't return the contents of the file since the browser loaded it from its cache.



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?

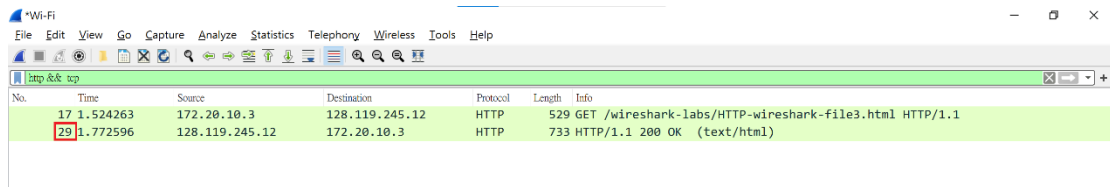
Ans : My browser sent only one HTTP GET request message. Packet number 17 contained the GET message for the Bill of Rights.



No.	Time	Source	Destination	Protocol	Length	Info
17	1.524263	172.20.10.3	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
29	1.772596	128.119.245.12	172.20.10.3	HTTP	733	HTTP/1.1 200 OK (text/html)

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

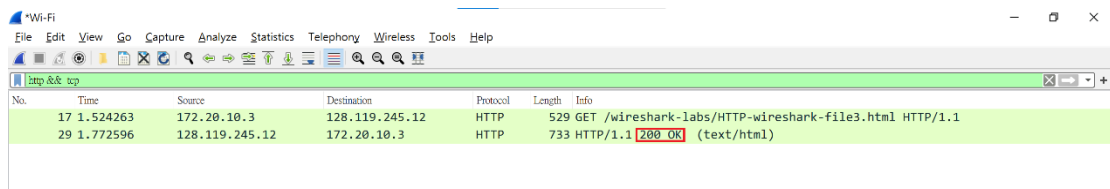
Ans : packet number: 29.



No.	Time	Source	Destination	Protocol	Length	Info
17	1.524263	172.20.10.3	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
29	1.772596	128.119.245.12	172.20.10.3	HTTP	733	HTTP/1.1 200 OK (text/html)

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

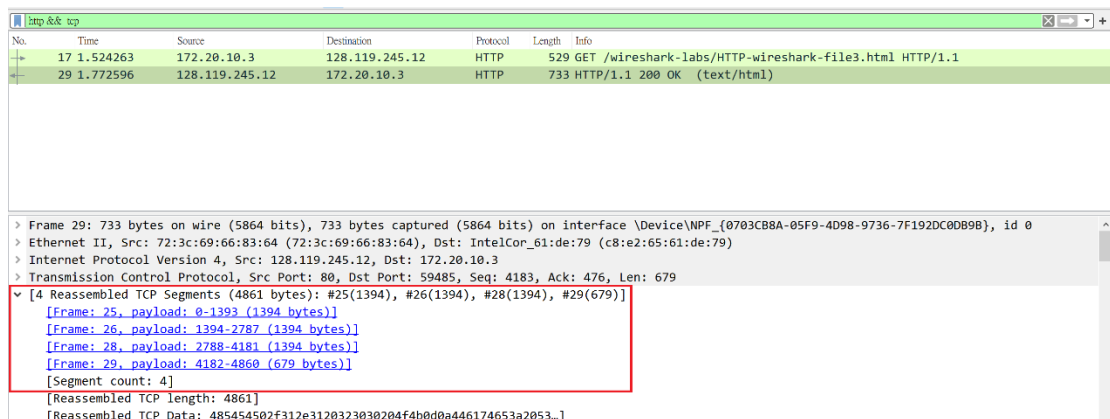
Ans : if click reboot browser the status is 304 Not Modified , that first clicked the status is 200 OK.



No.	Time	Source	Destination	Protocol	Length	Info
17	1.524263	172.20.10.3	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
29	1.772596	128.119.245.12	172.20.10.3	HTTP	733	HTTP/1.1 200 OK (text/html)

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

Ans : 4, Respectively are 1394, 1394, 1394 and 679 bytes, total length is 4861 bytes.



No.	Time	Source	Destination	Protocol	Length	Info
17	1.524263	172.20.10.3	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
29	1.772596	128.119.245.12	172.20.10.3	HTTP	733	HTTP/1.1 200 OK (text/html)

> Frame 29: 733 bytes on wire (5864 bits), 733 bytes captured (5864 bits) on interface \Device\NPF\_{0703CB8A-05F9-4D98-9736-7F192DC0B9B}, id 0

> Ethernet II, Src: 72:3c:69:66:83:64 (72:3c:69:66:83:64), Dst: IntelCor\_61:de:79 (c8:e2:65:61:de:79)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.20.10.3

> Transmission Control Protocol, Src Port: 80, Dst Port: 59485, Seq: 4183, Ack: 476, Len: 679

✓ [4 Reassembled TCP Segments (4861 bytes): #25(1394), #26(1394), #28(1394), #29(679)]

- [Frame: 25, payload: 0-1393 (1394 bytes)]
- [Frame: 26, payload: 1394-2787 (1394 bytes)]
- [Frame: 28, payload: 2788-4181 (1394 bytes)]
- [Frame: 29, payload: 4182-4860 (679 bytes)]

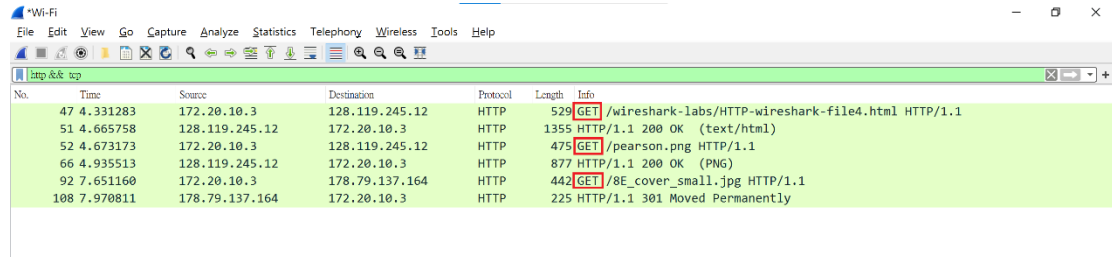
[Segment count: 4]

[Reassembled TCP length: 4861]

[Reassembled TCP Data: 485454502f312e3120323030204f4b0d0a446174653a2053...]

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

Ans : 3, Respectively are 128.119.245.12 and 128.119.245.12 and 178.79.137.164.

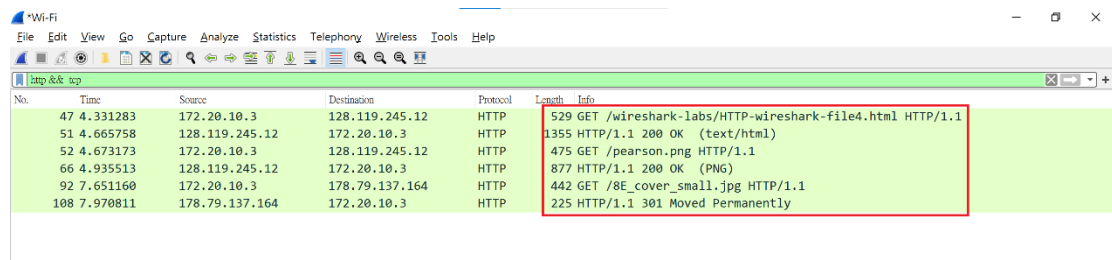


A screenshot of the Wireshark network protocol analyzer. The 'Packet List' pane shows a list of captured packets. The first three packets are HTTP GET requests. The first packet (No. 47) is a GET request for '/wireshark-labs/HTTP-wireshark-file4.html' from source 172.20.10.3 to destination 128.119.245.12. The second packet (No. 51) is a GET request for '/pearson.png' from source 128.119.245.12 to destination 172.20.10.3. The third packet (No. 52) is a GET request for '/8E\_cover\_small.jpg' from source 172.20.10.3 to destination 178.79.137.164. The 'Packet Details' pane shows the details of the selected packet (No. 47), which is an HTTP/1.1 GET request.

No.	Time	Source	Destination	Protocol	Length	Info
47	4.331283	172.20.10.3	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
51	4.665758	128.119.245.12	172.20.10.3	HTTP	1355	HTTP/1.1 200 OK (text/html)
52	4.673173	172.20.10.3	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
66	4.935513	128.119.245.12	172.20.10.3	HTTP	877	HTTP/1.1 200 OK (PNG)
92	7.651160	172.20.10.3	178.79.137.164	HTTP	442	GET /8E_cover_small.jpg HTTP/1.1
108	7.970811	178.79.137.164	172.20.10.3	HTTP	225	HTTP/1.1 301 Moved Permanently

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.

Ans : The two pictures downloaded by the browser are downloaded serially. For example, when we download two larger programs, the system sources are shared and exchanged. Because the download speed is fast, the difference may not be visible to the naked eye, but the more works downloaded, the less system resources are allocated, and the easier it is to see that it is a serial download, However, 8E\_cover\_small.jpg be rewrite his position, so respond 301 Move Permanently.

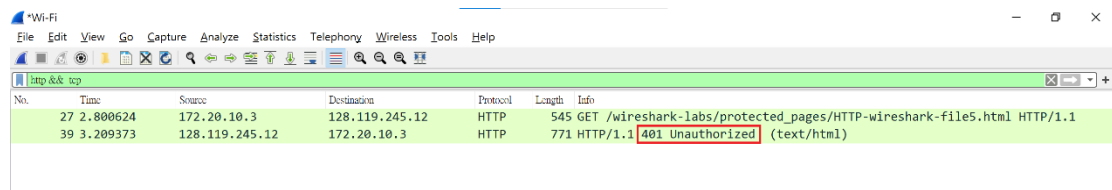


A screenshot of the Wireshark network protocol analyzer. The 'Packet List' pane shows a list of captured packets. The first three packets are HTTP GET requests. The first packet (No. 47) is a GET request for '/wireshark-labs/HTTP-wireshark-file4.html' from source 172.20.10.3 to destination 128.119.245.12. The second packet (No. 51) is a GET request for '/pearson.png' from source 128.119.245.12 to destination 172.20.10.3. The third packet (No. 52) is a GET request for '/8E\_cover\_small.jpg' from source 172.20.10.3 to destination 178.79.137.164. The 'Packet Details' pane shows the details of the selected packet (No. 47), which is an HTTP/1.1 GET request.

No.	Time	Source	Destination	Protocol	Length	Info
47	4.331283	172.20.10.3	128.119.245.12	HTTP	529	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
51	4.665758	128.119.245.12	172.20.10.3	HTTP	1355	HTTP/1.1 200 OK (text/html)
52	4.673173	172.20.10.3	128.119.245.12	HTTP	475	GET /pearson.png HTTP/1.1
66	4.935513	128.119.245.12	172.20.10.3	HTTP	877	HTTP/1.1 200 OK (PNG)
92	7.651160	172.20.10.3	178.79.137.164	HTTP	442	GET /8E_cover_small.jpg HTTP/1.1
108	7.970811	178.79.137.164	172.20.10.3	HTTP	225	HTTP/1.1 301 Moved Permanently

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

Ans : 401 Unauthorized.



A screenshot of the Wireshark network protocol analyzer. The 'Packet List' pane shows a list of captured packets. The first two packets are HTTP GET requests. The first packet (No. 27) is a GET request for '/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html' from source 172.20.10.3 to destination 128.119.245.12. The second packet (No. 39) is a GET request for '/wireshark-labs/protected\_pages/HTTP-wireshark-file5.html' from source 128.119.245.12 to destination 172.20.10.3. The 'Packet Details' pane shows the details of the selected packet (No. 39), which is an HTTP/1.1 401 Unauthorized response.

No.	Time	Source	Destination	Protocol	Length	Info
27	2.800624	172.20.10.3	128.119.245.12	HTTP	545	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
39	3.209373	128.119.245.12	172.20.10.3	HTTP	771	HTTP/1.1 401 Unauthorized (text/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?

Ans : Authorized field.

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 526 is selected, showing an HTTP GET request from 172.20.10.3 to 128.119.245.12. The bottom pane shows the details of this packet, specifically the Hypertext Transfer Protocol section. The request is for the URI /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html. The details pane highlights the 'Authorization' field, which has the value 'Basic MDow\r\n'. The packet bytes pane at the bottom shows the raw data of the packet, with the 'Authorization' field highlighted in blue.

No.	Time	Source	Destination	Protocol	Length	Info
479	28.724840	172.20.10.3	128.119.245.12	HTTP	571	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
494	28.976347	128.119.245.12	172.20.10.3	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
526	31.530934	172.20.10.3	128.119.245.12	HTTP	598	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
529	31.792440	128.119.245.12	172.20.10.3	HTTP	770	HTTP/1.1 401 Unauthorized (text/html)
1122	80.512751	172.20.10.3	217.11.235.45	HTTP	518	GET /util/base64-decoder-encoder.asp HTTP/1.1
1131	80.995242	217.11.235.45	172.20.10.3	HTTP	458	HTTP/1.1 301 Moved Permanently (text/html)

> Frame 526: 598 bytes on wire (4784 bits), 598 bytes captured (4784 bits) on interface \Device\NPF\_{0703CB8A-05F9-4D98-9736-7F192DC0DB9B}, id 0  
> Ethernet II, Src: IntelCor\_61:de:79 (c8:e2:65:61:de:79), Dst: 72:3c:69:66:83:64 (72:3c:69:66:83:64)  
> Internet Protocol Version 4, Src: 172.20.10.3, Dst: 128.119.245.12  
> Transmission Control Protocol, Src Port: 59613, Dst Port: 80, Seq: 518, Ack: 718, Len: 544  
v Hypertext Transfer Protocol  
v GET /wireshark-labs/protected\_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n  
v [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  
v Authorization: Basic MDow\r\n  
Upgrade-Insecure-Requests: 1\r\n

00c0 78 2d 61 67 65 3d 30 0d 0a 41 75 74 68 6f 72 69 x-age=0. .Authori  
00d0 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 20 4d 44 zation: Basic MD

HTTP Authorization header (http.authorization), 27 byte(s) | Packets: 2408 · Displayed: 6 (0.2%) · Dropped: 0 (0.0%) | Profile: Default