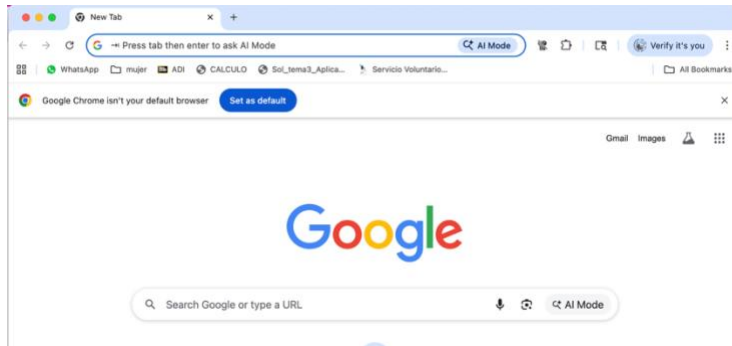


Catalina Cisneros

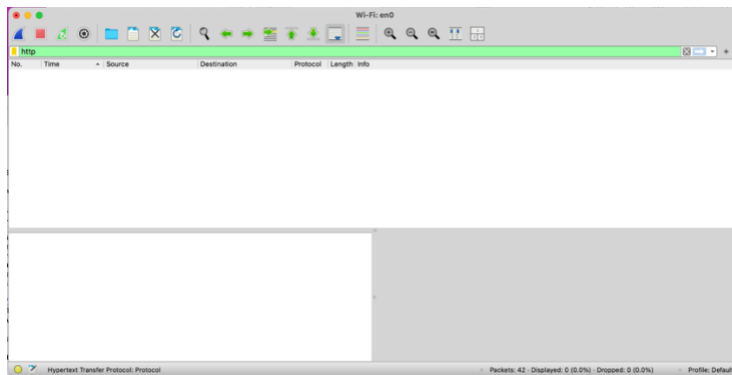
Lab: Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction

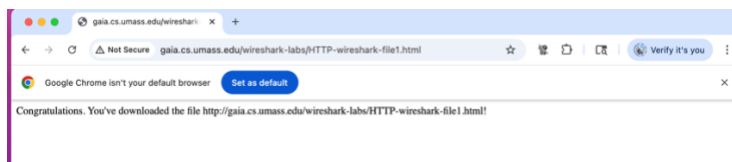
Start up your web browser.



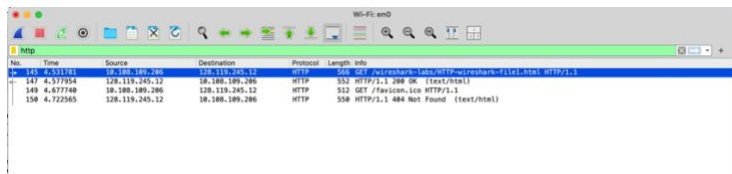
Start Wireshark and wait 2 minutes



Enter on my browser: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>



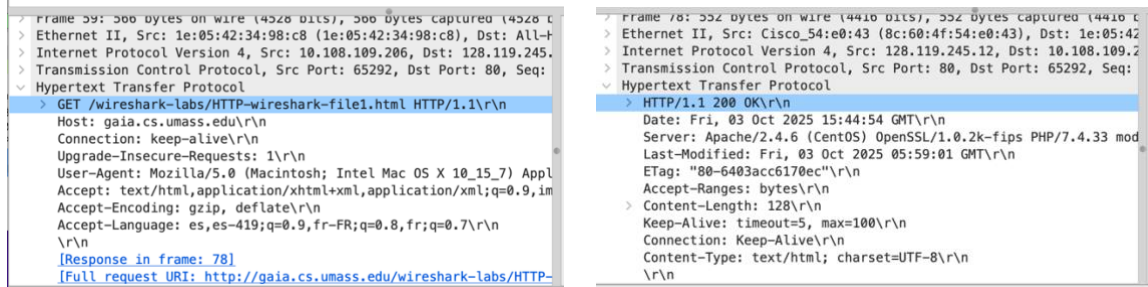
Stop packet capture



Questions

1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?

→ Both browser and server are running HTTP/1.1



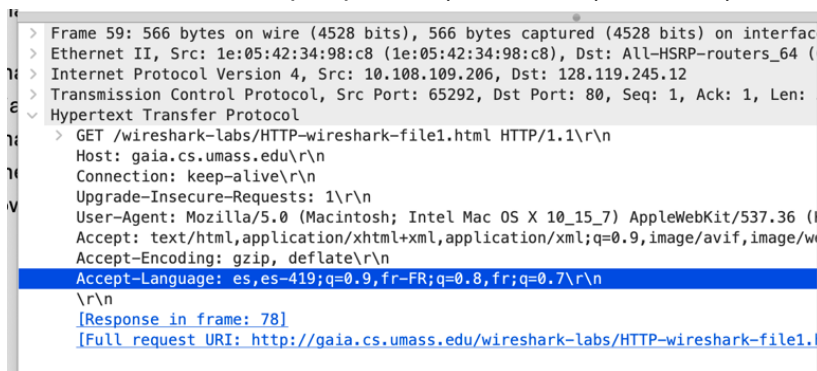
The first screenshot shows an HTTP GET request from the browser to the server. The second screenshot shows the corresponding HTTP 200 OK response from the server.

```
> GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) Appl
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
Accept-Encoding: gzip, deflate\r\n
Accept-Language: es,es-419;q=0.9,fr-FR;q=0.8,fr;q=0.7\r\n
\r\n
[Response in frame: 78]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-
```

```
> HTTP/1.1 200 OK\r\n
Date: Fri, 03 Oct 2025 15:44:54 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod
Last-Modified: Fri, 03 Oct 2025 05:59:01 GMT\r\n
ETag: "80-6403acc6170ec"\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
```

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

→ Browser can accept Spanish (es, es-419), French (fr-FR, fr)



The screenshot shows the 'Accept-Language' header in the browser's HTTP request, indicating support for Spanish (es, es-419), French (fr-FR, fr), and English (en).

```
Accept-Language: es,es-419;q=0.9,fr-FR;q=0.8,fr;q=0.7\r\n
\r\n
[Response in frame: 78]
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html]
```

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

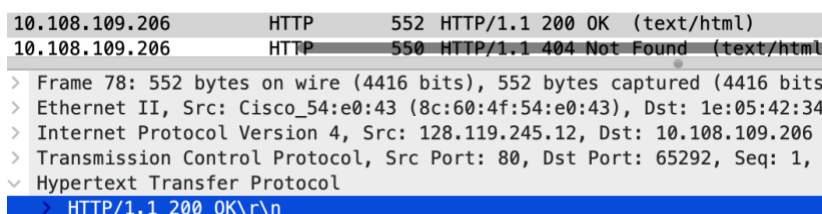
→ Source IP (my computer): 10.108.109.206

→ Destination IP: 128.119.245.12

Source	Destination
10.108.109.206	128.119.245.12
10.108.109.206	128.119.245.12

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

→ The server returned 200 OK.

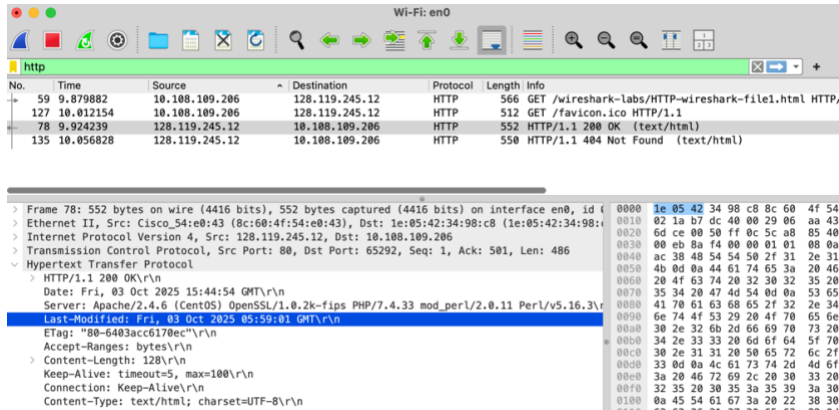


The screenshot shows the status bar of the browser displaying '200 OK' and the corresponding HTTP response details in Wireshark.

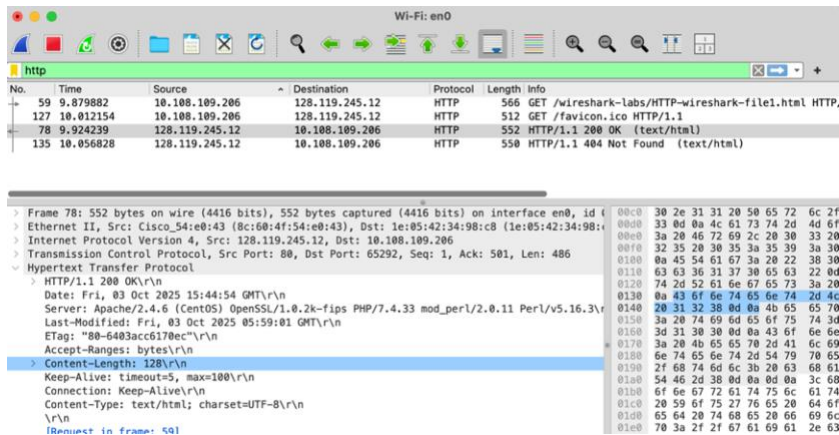
```
10.108.109.206 HTTP 552 HTTP/1.1 200 OK (text/html)
10.108.109.206 HTTP 550 HTTP/1.1 404 Not Found (text/html)

> Frame 78: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits)
> Ethernet II, Src: Cisco_54:e0:43 (8c:60:4f:54:e0:43), Dst: 1e:05:42:34
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.108.109.206
> Transmission Control Protocol, Src Port: 80, Dst Port: 65292, Seq: 1,
> Hypertext Transfer Protocol
> HTTP/1.1 200 OK\r\n
```

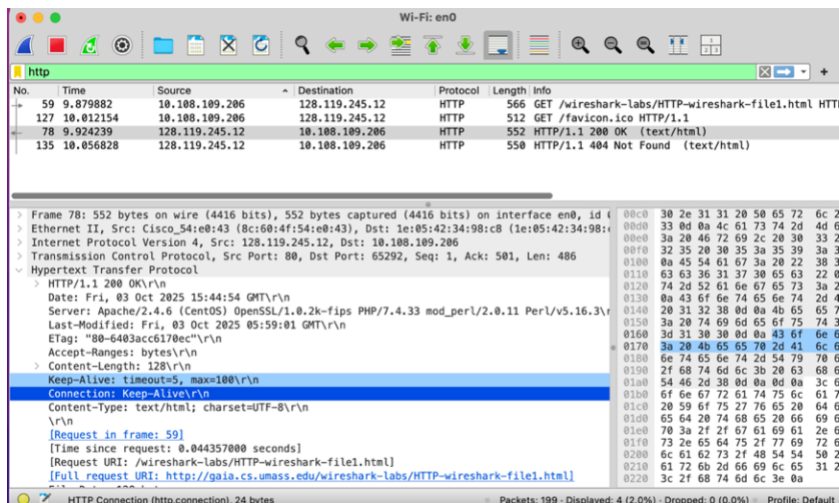
5. When was the HTML file that you are retrieving last modified at the server?
→ the HTML file was last modified on Fri, 03 Oct 2025 05:59:01 GMT = 01:59:01 EST



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

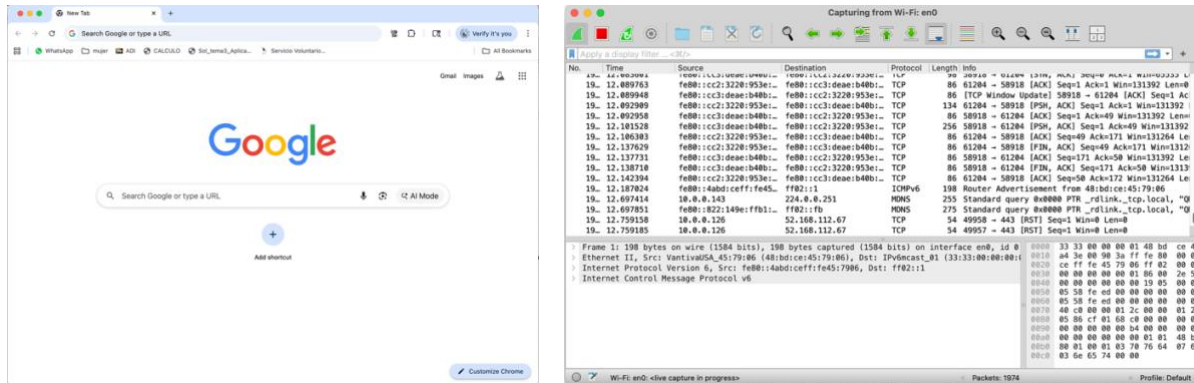


7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
→ Example not shown in main list but visible in raw data is Connection: Keep-Alive

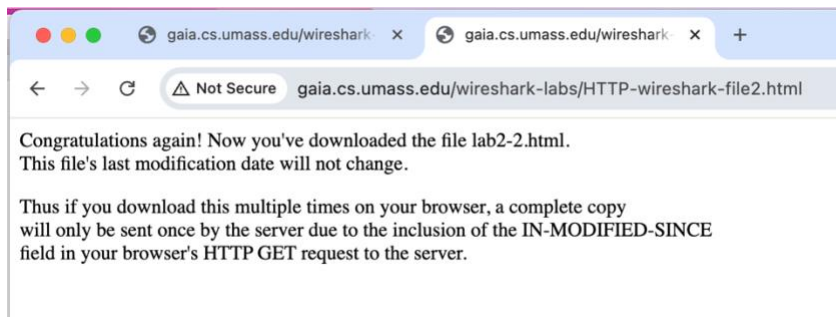


2. The HTTP CONDITIONAL GET/response interaction

Start up my web browser and Wireshark



Enter the given URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html> twice in the browser



Stop packet capture and filter by http

No.	Time	Source	Destination	Protocol	Length	Info
17..	3.095449	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
17..	3.157848	128.119.245.12	10.0.0.126	HTTP	796	HTTP/1.1 200 OK (text/html)
17..	3.241624	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
17..	3.298681	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found (text/html)
19..	15.071304	10.0.0.126	128.119.245.12	HTTP	678	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
19..	15.140701	128.119.245.12	10.0.0.126	HTTP	306	HTTP/1.1 304 Not Modified

Questions

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 did not include an “If-Modified-Since” line.

No.	Time	Source	Destination	Protocol	Length	Info
17...	3.095449	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HT
17...	3.157848	128.119.245.12	10.0.0.126	HTTP	796	HTTP/1.1 200 OK (text
17...	3.241624	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/
17...	3.298601	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found
19...	15.071304	10.0.0.126	128.119.245.12	HTTP	678	GET /wireshark-labs/HT
19...	15.140701	128.119.245.12	10.0.0.126	HTTP	306	HTTP/1.1 304 Not Modif

```
> Frame 1722: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface en0, id 0
> Ethernet II, Src: VantivaUSA_45:79:06 (46:ff:0b:ca:03:07), Dst: VantivaUSA_45:79:06 (48:bd:ce:45:79:06)
> Internet Protocol Version 4, Src: 10.0.0.126, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59246, Dst Port: 80, Seq: 1, Ack: 1, Len: 500
< Hypertext Transfer Protocol
  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 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) C
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: es-es;q=0.9,fr-FR;q=0.8,fr;q=0.7\r\n
    \r\n
    [Response in frame: 1747]
    [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?

→ Yes, the server returned the file. The “200 OK” status and the presence of a Content-Length field confirm it.

No.	Time	Source	Destination	Protocol	Length	Info
17...	3.095449	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HT
17...	3.157848	128.119.245.12	10.0.0.126	HTTP	796	HTTP/1.1 200 OK (text
17...	3.241624	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/
17...	3.298601	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found
19...	15.071304	10.0.0.126	128.119.245.12	HTTP	678	GET /wireshark-labs/HT
19...	15.140701	128.119.245.12	10.0.0.126	HTTP	306	HTTP/1.1 304 Not Modif


```
> Frame 1747: 796 bytes on wire (6368 bits), 796 bytes captured (6368 bits) on interface en0, id 0
> Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.126
> Transmission Control Protocol, Src Port: 80, Dst Port: 59246, Seq: 1, Ack: 501, Len: 730
< 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, 05 Oct 2025 19:14:52 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, 05 Oct 2025 05:59:01 GMT\r\n
    ETag: "173-6406308158ab6"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 371\r\n
    [Content length: 371]
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\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?

→ Yes, the second GET includes “If-Modified-Since: Sun, 05 Oct 2025 05:59:01 GMT\r\n”

http						
No.	Time	Source	Destination	Protocol	Length	Info
17...	3.095449	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HT
17...	3.157848	128.119.245.12	10.0.0.126	HTTP	796	HTTP/1.1 200 OK (text,
17...	3.241624	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP:/
17...	3.298601	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found
19...	15.071304	10.0.0.126	128.119.245.12	HTTP	678	GET /wireshark-labs/HT
19...	15.140701	128.119.245.12	10.0.0.126	HTTP	306	HTTP/1.1 304 Not Modif:

> Transmission Control Protocol, Src Port: 59247, Dst Port: 80, Seq: 1, Ack: 1, Len: 612

> Hypertext Transfer Protocol

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

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

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) C

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q

Accept-Encoding: gzip, deflate\r\n

Accept-Language: es-es-419;q=0.9,fr-FR;q=0.8,fr;q=0.7\r\n

If-None-Match: "173-6406308158ab6"\r\n

If-Modified-Since: Sun, 05 Oct 2025 05:59:01 GMT\r\n

\r\n

[Response in frame: 1940]

[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.

→ The server replied 304 Not Modified, meaning it did not resend the file and the browser used the cached version.

http						
No.	Time	Source	Destination	Protocol	Length	Info
17...	3.095449	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wire
17...	3.157848	128.119.245.12	10.0.0.126	HTTP	796	HTTP/1.1 200 OK (text/html)
17...	3.241624	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
17...	3.298601	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found (text
19...	15.071304	10.0.0.126	128.119.245.12	HTTP	678	GET /wireshark-labs/HTTP-wire
19...	15.140701	128.119.245.12	10.0.0.126	HTTP	306	HTTP/1.1 304 Not Modified

> Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:03:07 (46:ff:0b:ca:03:07)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.126

> Transmission Control Protocol, Src Port: 80, Dst Port: 59247, Seq: 1, Ack: 613, Len: 240

> Hypertext Transfer Protocol

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: Sun, 05 Oct 2025 19:15:04 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

Connection: Keep-Alive\r\n

Keep-Alive: timeout=5, max=100\r\n

ETag: "173-6406308158ab6"\r\n

\r\n

[Request in frame: 1938]

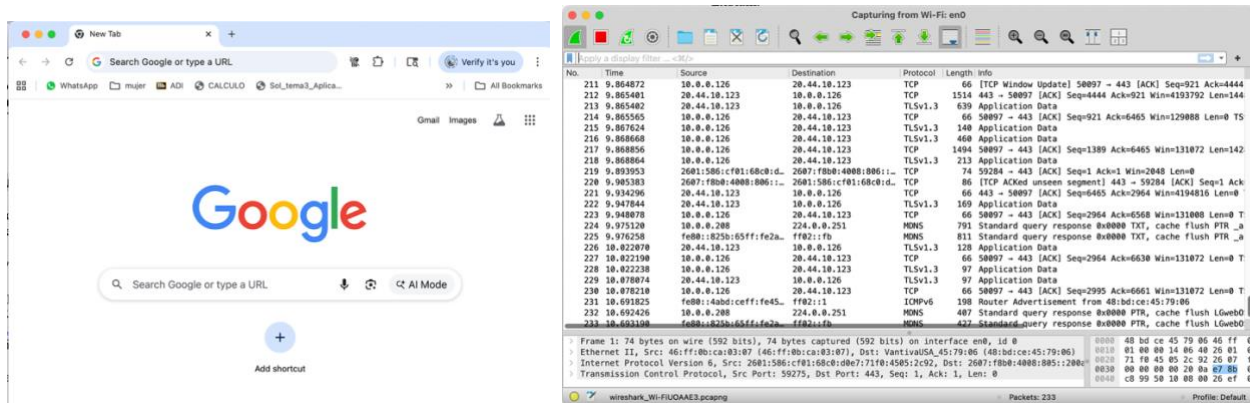
[Time since request: 0.069397000 seconds]

[Request URI: /wireshark-labs/HTTP-wireshark-file2.html]

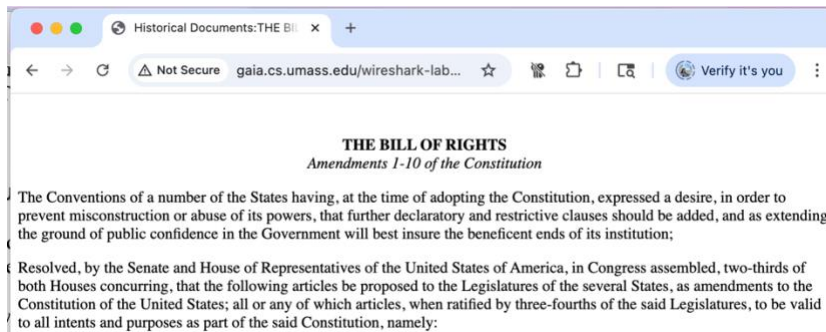
[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]

3. Retrieving Long Documents

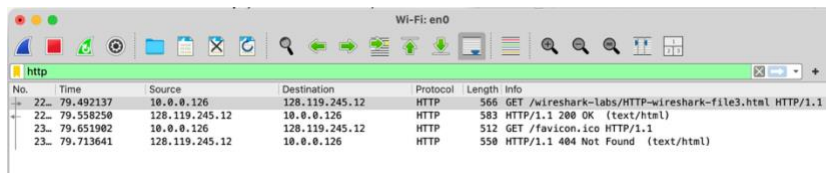
Restart my web browser (cache + history cleared) and Wireshark



Enter the URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>



Stop Wireshark and filter by http



Questions:

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

→ My browser sent 2 GET requests (one for file3.html and one for favicon.ico). The GET for the Bill of Rights is in packet 2279

No.	Time	Source	Destination	Protocol	Length	Info
2279	79.492137	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-
2298	79.558250	128.119.245.12	10.0.0.126	HTTP	583	HTTP/1.1 200 OK (text/html)
2317	79.651902	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
2320	79.713641	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found (text/html)

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

→ The response with the status code appears in packet 2298

No.	Time	Source	Destination	Protocol	Length	Info
2279	79.492137	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-
2298	79.558250	128.119.245.12	10.0.0.126	HTTP	583	HTTP/1.1 200 OK (text/html)
2317	79.651902	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1

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

→ HTTP/1.1 200 OK.

The image shows a Wireshark packet capture of an HTTP response. The top pane shows the packet list with packet 2298 selected. The middle pane shows the packet details for the selected packet, including the Hypertext Transfer Protocol section. The status code is 200 and the phrase is OK.

Time	Source	Destination	Protocol	Length	Info
2279	79.492137	10.0.0.126	128.119.245.12	HTTP	566 GET /wireshark-labs/HTTP-
2298	79.558250	128.119.245.12	10.0.0.126	HTTP	583 HTTP/1.1 200 OK (text/ht
2317	79.651902	10.0.0.126	128.119.245.12	HTTP	512 GET /favicon.ico HTTP/1.1
2320	79.713641	128.119.245.12	10.0.0.126	HTTP	550 HTTP/1.1 404 Not Found (

Details of packet 2298:

- [Frame: 2294, payload: 1448-2895 (1448 bytes)]
- [Frame: 2296, payload: 2896-4343 (1448 bytes)]
- [Frame: 2298, payload: 4344-4860 (517 bytes)]
- [Segment count: 4]
- [Reassembled TCP length: 4861]
- [Reassembled TCP Data [...]: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c2030
- ⌵ 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, 05 Oct 2025 19:24:21 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.
 - Last-Modified: Sun, 05 Oct 2025 05:59:01 GMT\r\n
 - ETag: "1194-640630815501d"\r\n
 - Accept-Ranges: bytes\r\n
 - ⌵ Content-Length: 4500\r\n
 - [Content length: 4500]

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

→ The HTTP response needed 4 data-containing TCP segments:

14 Reassembled TCP Segments (4861 bytes):

[Frame: 2292, payload: 0-1447 (1448 bytes)]

[Frame: 2294, payload: 1448-2895 (1448 bytes)]

[Frame: 2296, payload: 2896-4343 (1448 bytes)]

[Frame: 2298, payload: 4344-4860 (517 bytes)]

[Segment count: 4]

Reassembled TCP length: 48611

The image displays the Wireshark network protocol analyzer interface. The top section shows a list of captured packets, with the first four being HTTP GET requests. The bottom section provides a detailed view of the selected packet (Packet 4), showing it is a reassembled TCP segment containing four HTTP GET requests for various resources from the wireshark-labs website.

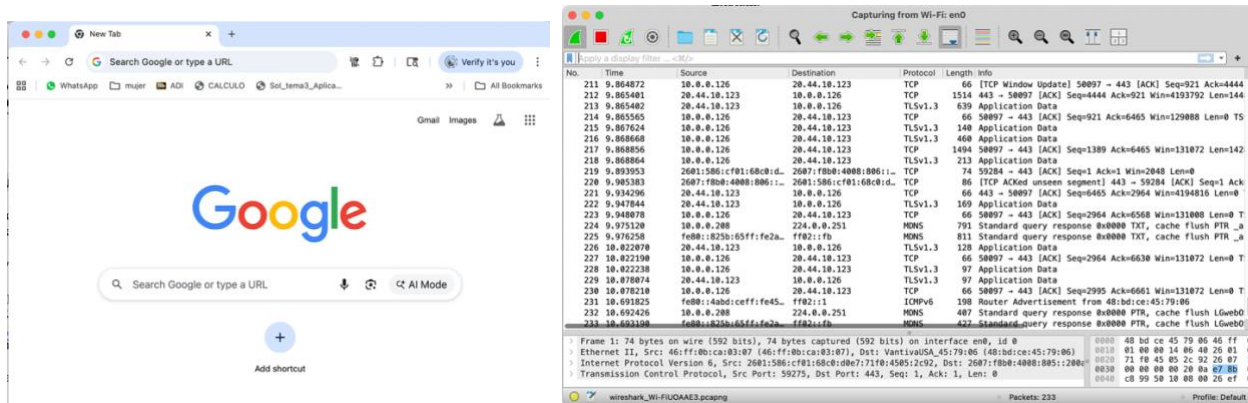
No.	Time	Source	Destination	Protocol	Length	Info
2279	79.492137	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-
2298	79.558250	128.119.245.12	10.0.0.126	HTTP	583	HTTP/1.1 200 OK (text/ht
2317	79.651902	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
2320	79.713641	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found (

Packet 4 Details:

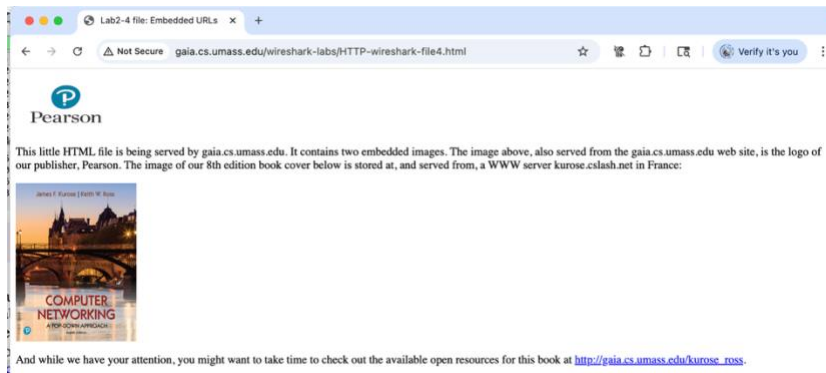
- Frame 2298: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface e
- Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:03:07 (46:f
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.126
- Transmission Control Protocol, Src Port: 80, Dst Port: 59287, Seq: 4345, Ack: 501, Len:
- 4 Reassembled TCP Segments (4861 bytes): #2292(1448), #2294(1448), #2296(1448), #2298(5**
 - [Frame: 2292, payload: 0-1447 (1448 bytes)]
 - [Frame: 2294, payload: 1448-2895 (1448 bytes)]
 - [Frame: 2296, payload: 2896-4343 (1448 bytes)]
 - [Frame: 2298, payload: 4344-4860 (517 bytes)]
- [Segment count: 4]
- [Reassembled TCP length: 4861]
- [Reassembled TCP Data [...]: 485454502f312e3120323030204f4b0d0a446174653a2053756e2c2030
- Hypertext Transfer Protocol
- Line-based text data: text/html (98 lines)

4. HTML Documents with Embedded Objects

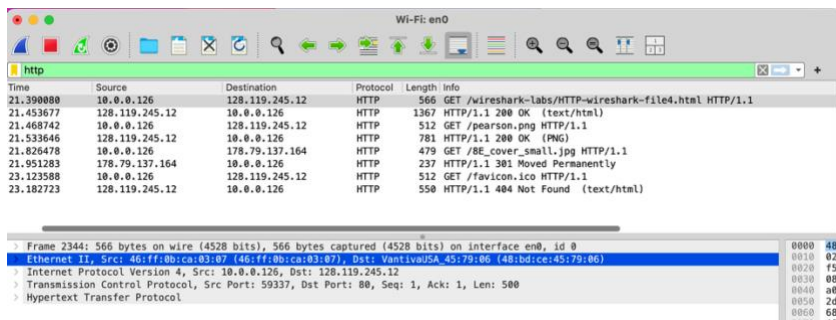
Restart my web browser (cache + history cleared) and Wireshark



Enter the URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>



Stop Wireshark and filter by http

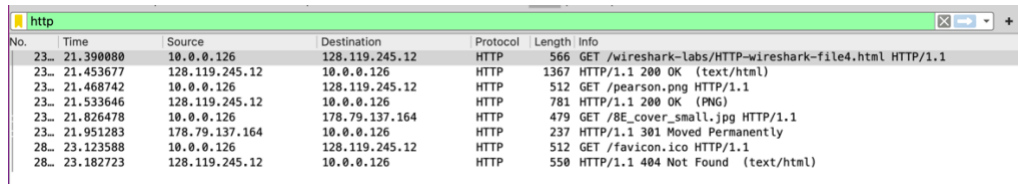


Questions

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

→ My browser sent 4 HTTP GET requests.

- /wireshark-labs/HTTP-wireshark-file4.html → 128.119.245.12
- /pearson.png → 128.119.245.12
- /8E_cover_small.jpg → 178.79.137.164
- /favicon.ico → 128.119.245.12



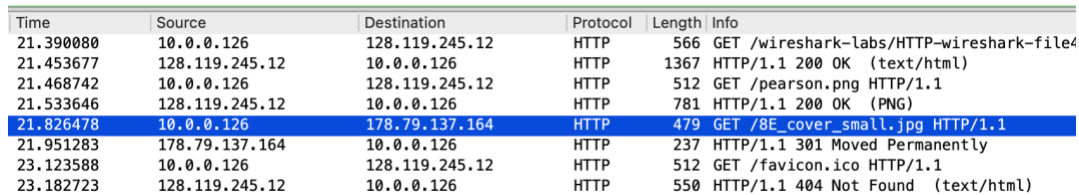
A screenshot of a Wireshark packet capture window. The top bar is green and labeled 'http'. Below it is a table of captured packets. The table has columns: No., Time, Source, Destination, Protocol, Length, and Info. The packets are numbered 23 through 28. Packet 23 is a GET request for /wireshark-labs/HTTP-wireshark-file4.html from 10.0.0.126 to 128.119.245.12. Packet 24 is a 200 OK response. Packet 25 is a GET request for /pearson.png from 10.0.0.126 to 128.119.245.12. Packet 26 is a 200 OK response. Packet 27 is a GET request for /8E_cover_small.jpg from 10.0.0.126 to 178.79.137.164. Packet 28 is a 301 Moved Permanently response. Packet 29 is a GET request for /favicon.ico from 10.0.0.126 to 128.119.245.12. Packet 30 is a 404 Not Found response.

No.	Time	Source	Destination	Protocol	Length	Info
23	21.390080	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
24	21.453677	128.119.245.12	10.0.0.126	HTTP	1367	HTTP/1.1 200 OK (text/html)
25	21.468742	10.0.0.126	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
26	21.533646	128.119.245.12	10.0.0.126	HTTP	781	HTTP/1.1 200 OK (PNG)
27	21.826478	10.0.0.126	178.79.137.164	HTTP	479	GET /8E_cover_small.jpg HTTP/1.1
28	21.951283	178.79.137.164	10.0.0.126	HTTP	237	HTTP/1.1 301 Moved Permanently
29	23.123588	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
30	23.182723	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found (text/html)

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.

→ The two images were downloaded in parallel.

→ The GET for pearson.png was sent to 128.119.245.12 at 21.468 s, and the GET for 8E_cover_small.jpg was sent to 178.79.137.164 at 21.826 s. Only about 0.36 seconds of different. Because the browser initiated both requests to different servers nearly simultaneously, it retrieved the two images in parallel rather than serially.

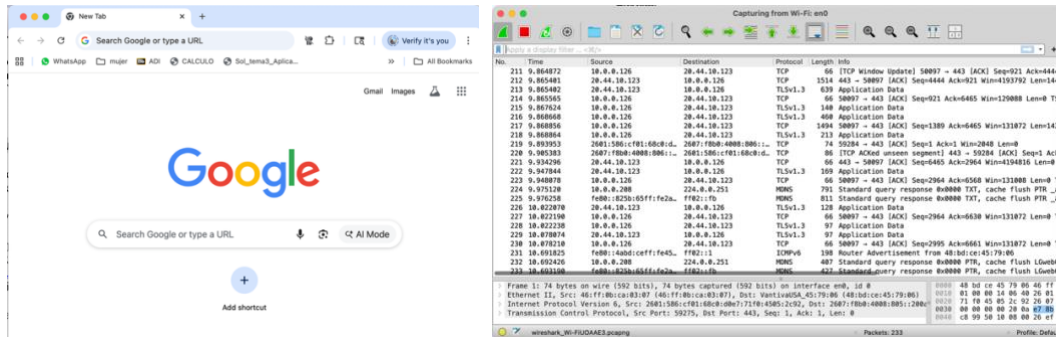


A screenshot of a Wireshark packet capture window. The top bar is green and labeled 'http'. Below it is a table of captured packets. The table has columns: Time, Source, Destination, Protocol, Length, and Info. The packets are numbered 23 through 30. The packet at time 21.826478 is highlighted in blue. This packet is a GET request for /8E_cover_small.jpg from 10.0.0.126 to 178.79.137.164.

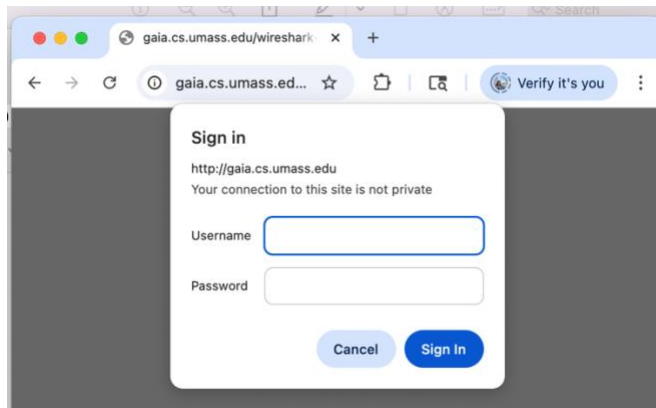
Time	Source	Destination	Protocol	Length	Info
21.390080	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file4
21.453677	128.119.245.12	10.0.0.126	HTTP	1367	HTTP/1.1 200 OK (text/html)
21.468742	10.0.0.126	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
21.533646	128.119.245.12	10.0.0.126	HTTP	781	HTTP/1.1 200 OK (PNG)
21.826478	10.0.0.126	178.79.137.164	HTTP	479	GET /8E_cover_small.jpg HTTP/1.1
21.951283	178.79.137.164	10.0.0.126	HTTP	237	HTTP/1.1 301 Moved Permanently
23.123588	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
23.182723	128.119.245.12	10.0.0.126	HTTP	550	HTTP/1.1 404 Not Found (text/html)

5 HTTP Authentication

Restart my web browser (cache + history cleared) and Wireshark

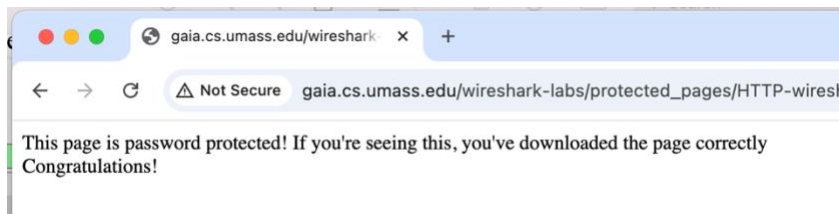


Enter the URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

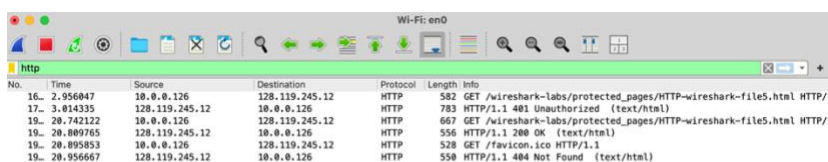


Enter username and password

- Username: wireshark-students
- Password: network



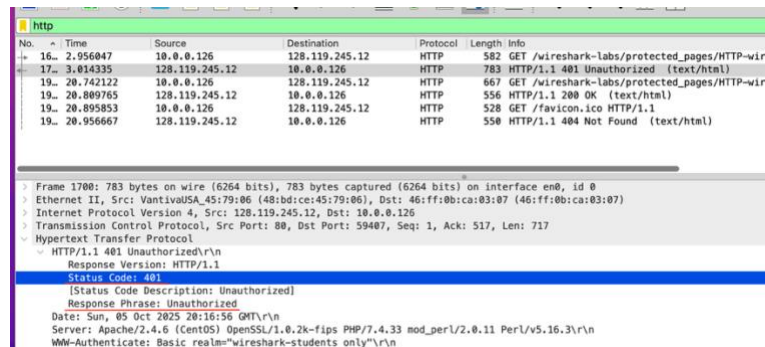
Stop Wireshark and filter by http



Questions

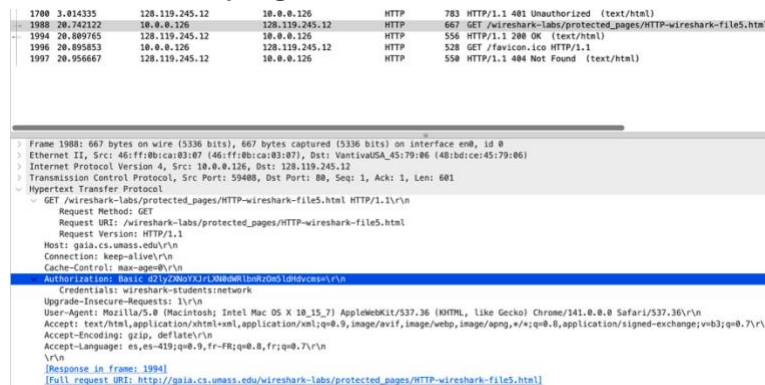
18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

→ The server replied with HTTP/1.1 401 Unauthorized, meaning the page is protected and my browser didn't have the authorization needed to access it.



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

→ When my browser sent the second GET request, it added an Authorization field that included my login credentials encoded in Base64.



→ Decoding the credentials

The `Form.SizeLimit` is 10000000bytes. Please, do not post more data using this form.

Source data from the Base64 string:

wireshark-students

Type (or copy-paste) some text to a textbox below. The text can be a Base64 string to decode or any string to encode to a Base64.

d2lyZXNoYXJrLXN0dWRlbnRzOm5=

or select a file to convert to a Base64 string.

Choose File no file selected

Convert the source data