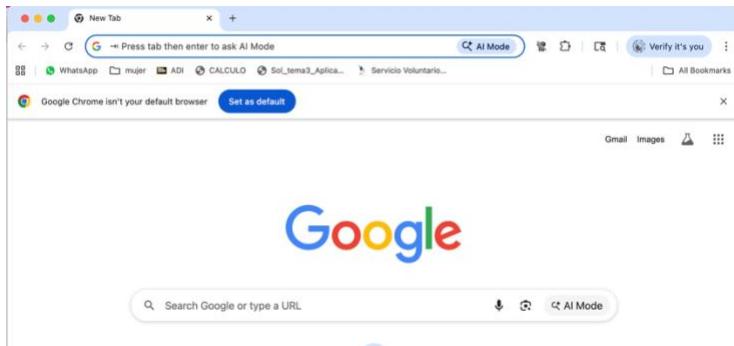


Catalina Cisneros

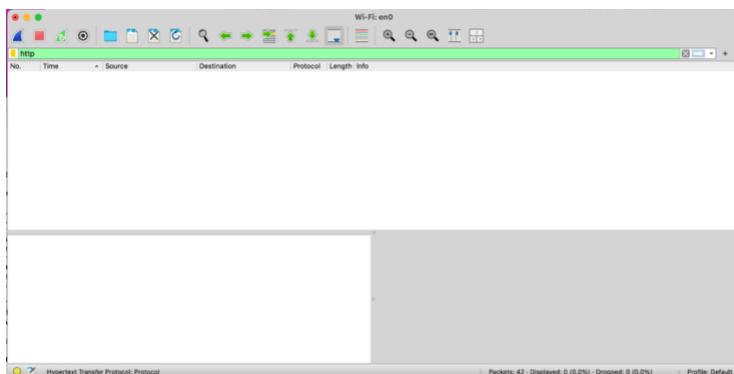
Lab: Wireshark Lab: HTTP

1. The Basic HTTP GET/response interaction

Start up your web browser.



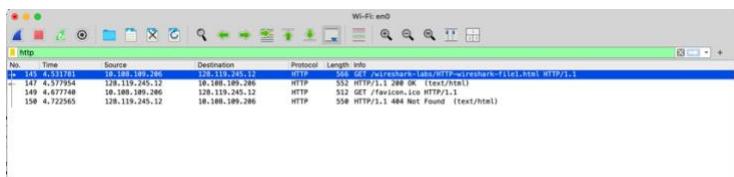
Start Wireshark and wait 2 minutes



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

```
> Frame 59: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface
> Ethernet II, Src: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8), Dst: All-HSRP-routers_64 (00:0c:29:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.108.109.206, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65292, Dst Port: 80, Seq: 1, Ack: 1, Len: 566
  Hypertext Transfer Protocol
    > 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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.104 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
      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-wireshark-file1.html]
```

```
> Frame 78: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface
> Ethernet II, Src: Cisco_54:e0:43 (8c:60:4f:54:e0:43), Dst: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8)
> 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, Ack: 1, Len: 552
  Hypertext Transfer Protocol
    > 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)

```
> Frame 59: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits) on interface
> Ethernet II, Src: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8), Dst: All-HSRP-routers_64 (00:0c:29:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.108.109.206, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 65292, Dst Port: 80, Seq: 1, Ack: 1, Len: 566
  Hypertext Transfer Protocol
    > 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) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.104 Safari/537.36\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3\r\n
      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-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.

```
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)

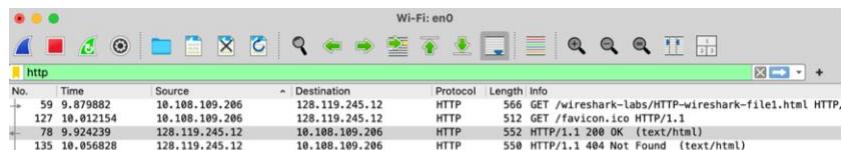
> Frame 78: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface
> Ethernet II, Src: Cisco_54:e0:43 (8c:60:4f:54:e0:43), Dst: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8)
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.108.109.206
> Transmission Control Protocol, Src Port: 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



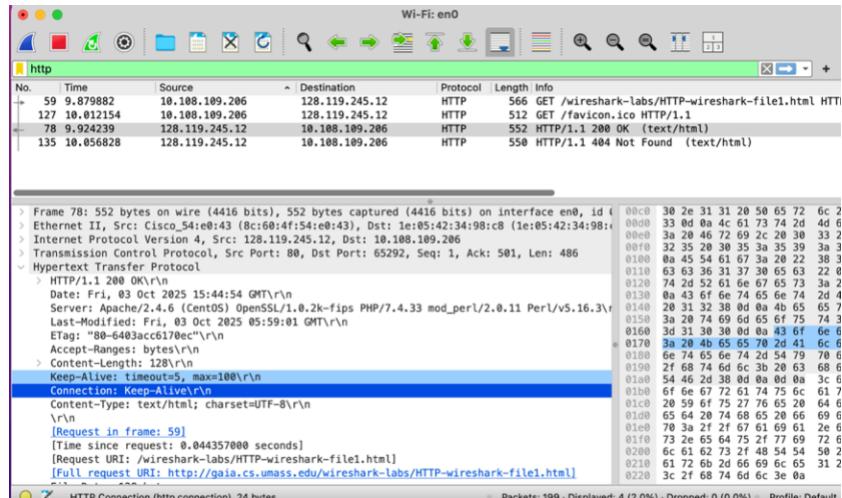
```
> Frame 78: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id (0x0000, Internet Protocol Version 4, Src: Cisco_54:e0:43 (8c:60:4f:54:e0:43), Dst: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8))
> Ethernet II, Src: Cisco_54:e0:43 (8c:60:4f:54:e0:43), Dst: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8)
> 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, Ack: 501, Len: 486
  Hypertext Transfer Protocol
    > 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/1.0.2-k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Fri, 03 Oct 2025 05:59:01 GMT\r\n
      ETag: "80-6403ac6170ec"\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: 59]
```

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



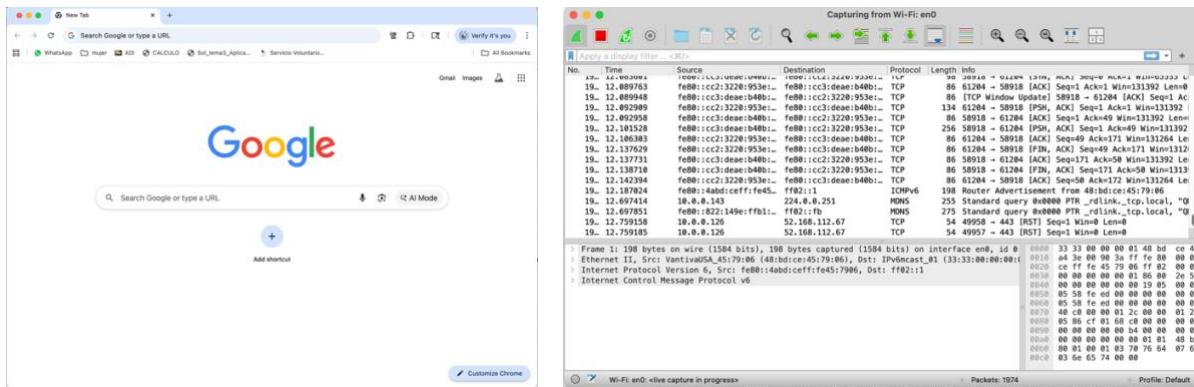
```
> Frame 78: 552 bytes on wire (4416 bits), 552 bytes captured (4416 bits) on interface en0, id (0x0000, Internet Protocol Version 4, Src: Cisco_54:e0:43 (8c:60:4f:54:e0:43), Dst: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8))
> Ethernet II, Src: Cisco_54:e0:43 (8c:60:4f:54:e0:43), Dst: 1e:05:42:34:98:c8 (1e:05:42:34:98:c8)
> 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, Ack: 501, Len: 486
  Hypertext Transfer Protocol
    > 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/1.0.2-k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
      Last-Modified: Fri, 03 Oct 2025 05:59:01 GMT\r\n
      ETag: "80-6403ac6170ec"\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: 59]
```

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

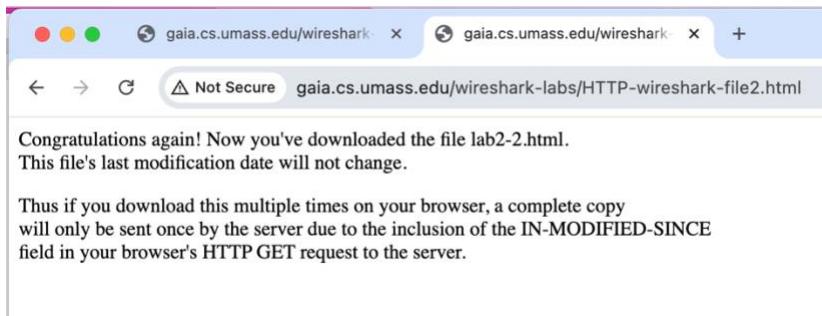


2. The HTTP CONDITIONAL GET/response interaction

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..	3.298601	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..	15.140781	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) (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-419;q=0.9,fr-FR;q=0.8,fr;q=0.7\r\n
    \r\n
  [Response in frame: 1747]
  [Full request URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
```

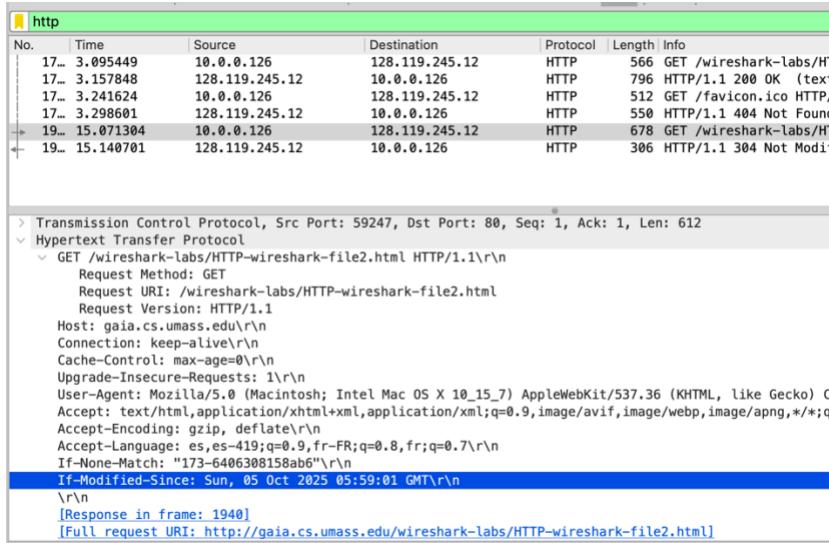
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
- Yes, the server returned the file. The “200 OK” status and the presence of a Content-Length field confirm it.

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


```
> 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: "173-64063008158abb"\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 GET6? 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”



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..	3.298601	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/HTTP-wireshark-file2.html
← 19..	15.140701	128.119.245.12	10.0.0.126	HTTP	306	HTTP/1.1 304 Not Modified

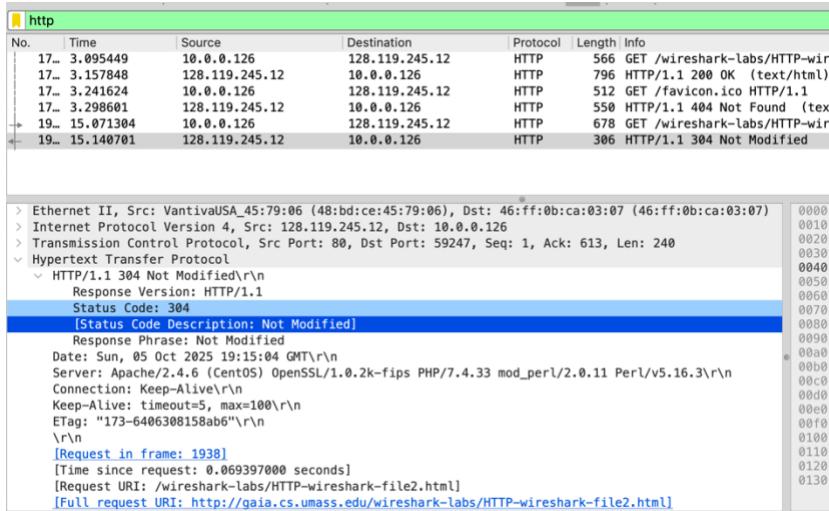
```

> 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.



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
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
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/HTTP-wireshark-file2.html
← 19..	15.140701	128.119.245.12	10.0.0.126	HTTP	306	HTTP/1.1 304 Not Modified

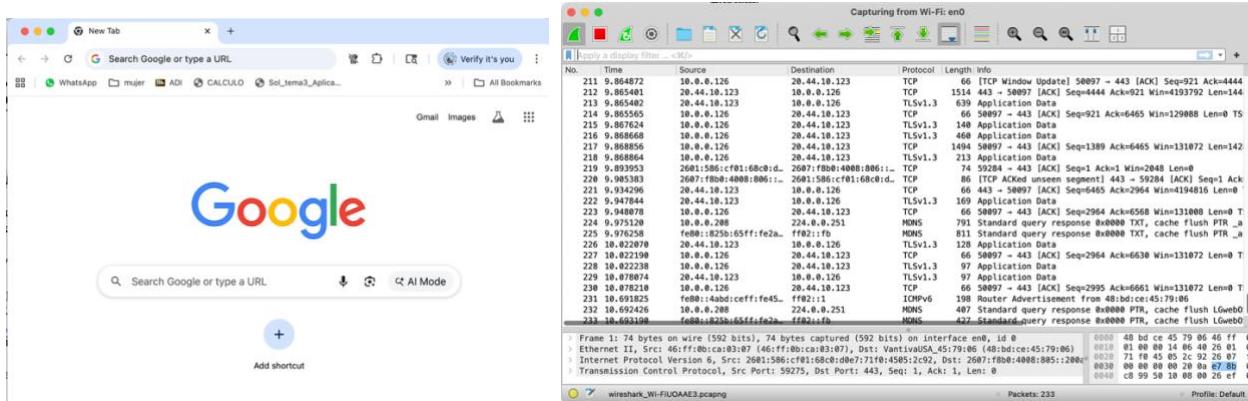
```

> 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

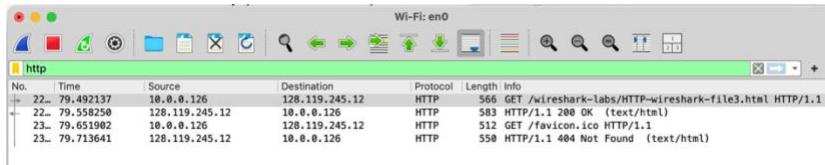
Restart my web browser (cache + history cleared) and Wireshark



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

The screenshot shows a web browser window with the title "Historical Documents: THE BILL". The address bar shows the URL "gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html". The page content is titled "THE BILL OF RIGHTS" and "Amendments 1-10 of the Constitution". The text on the page discusses the Bill of Rights and its purpose. Below the text, there is a note about the Senate and House of Representatives proposing amendments to the Constitution.

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 or 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 screenshot shows the Wireshark interface with the 'http' display filter applied. The details pane displays the reassembled TCP data, which includes four segments (Frame 2294, payload 1448-2895 bytes; Frame 2296, payload 2896-4343 bytes; Frame 2298, payload 4344-4860 bytes; Segment count: 4). Below this, the HTTP response is shown with the following details:

- Protocol: HyperText Transfer Protocol
- Status Code: 200
- Status 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]

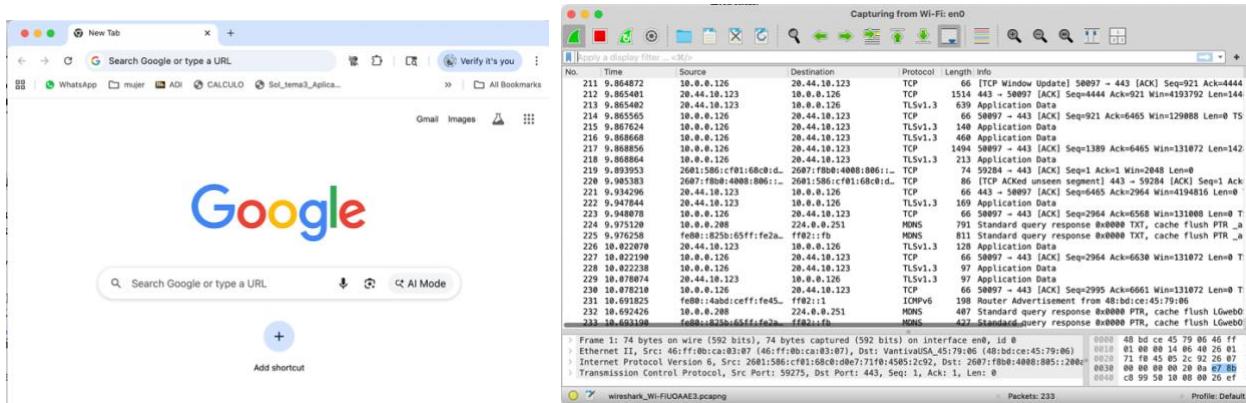
Reassembled TCP length: 48611

	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 (

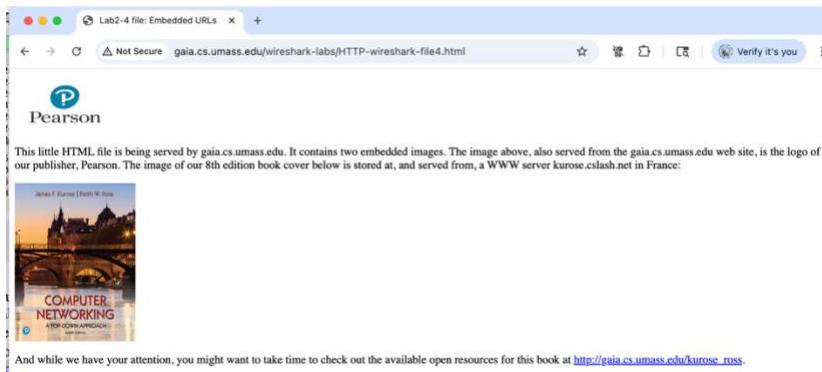
> Frame 2298: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface
> Ethernet II, Src: VantivaUSA_45:79:06 (48:bd:ce:45:79:06), Dst: 46:ff:0b:ca:03:07 (46:
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.126
> Transmission Control Protocol, Src Port: 80, Dst Port: 59287, Seq: 4345, Ack: 501, Len:
 < [4 Reassembled TCP Segments (4861 bytes): #2292(1448), #2294(1448), #2296(1448), #2298(
 [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

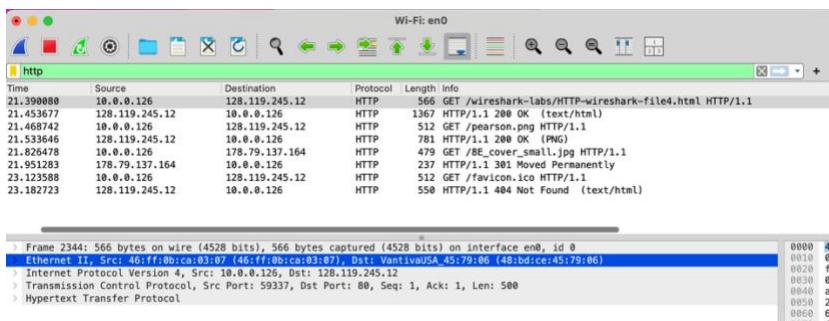


Enter the URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>



And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_moss.

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

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
23..	21.453677	128.119.245.12	10.0.0.126	HTTP	1367	HTTP/1.1 200 OK (text/html)
23..	21.468742	10.0.0.126	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
23..	21.533646	128.119.245.12	10.0.0.126	HTTP	781	HTTP/1.1 200 OK (PNG)
23..	21.826478	10.0.0.126	178.79.137.164	HTTP	479	GET /8E_cover_small.jpg HTTP/1.1
23..	21.951283	178.79.137.164	10.0.0.126	HTTP	237	HTTP/1.1 301 Moved Permanently
28..	23.123588	10.0.0.126	128.119.245.12	HTTP	512	GET /favicon.ico HTTP/1.1
28..	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.

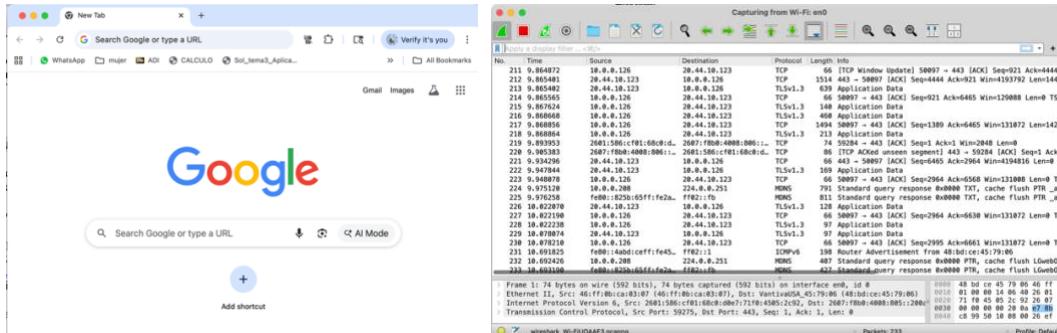
→ The two images were downloaded in parallel.

→ 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 difference. Because the browser initiated both requests to different servers nearly simultaneously, it retrieved the two images in parallel rather than serially.

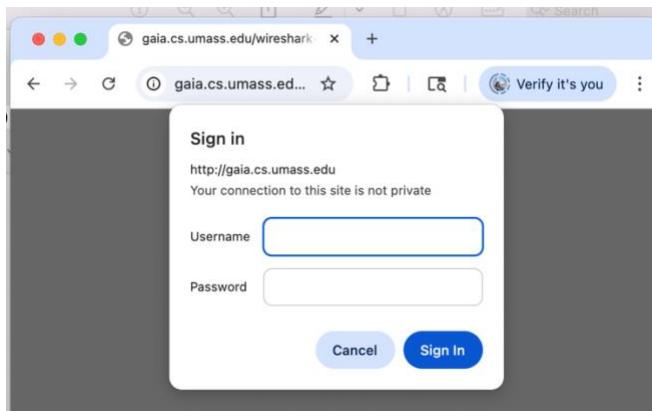
Time	Source	Destination	Protocol	Length	Info
21.390080	10.0.0.126	128.119.245.12	HTTP	566	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
21.453677	128.119.245.12	10.0.0.126	HTTP	1367	HTTP/1.1 200 OK (text/html)
21.468742	10.0.0.126	128.119.245.12	HTTP	512	GET /pearson.png HTTP/1.1
21.533646	128.119.245.12	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

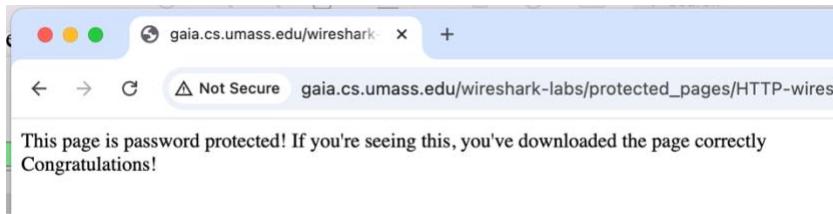


Enter the URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

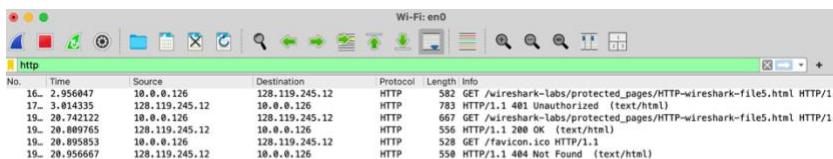


Enter username and password

- 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.

The Wireshark interface shows a sequence of network frames. Frame 1700 is an initial GET request to 'wireshark-labs/protected_pages/HTTP-wireshark-file5.htm'. Frame 1783 is the 401 Unauthorized response, which includes the status code 401 and the phrase 'Unauthorized'. The response also contains the 'WWW-Authenticate' header with the value 'Basic realm="wireshark-students only"'. The server information at the bottom indicates Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3.

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.

The Wireshark interface shows two GET requests to 'wireshark-labs/protected_pages/HTTP-wireshark-file5.htm'. The second request (Frame 1994) includes an 'Authorization' header with the value 'Basic dXNlcjpwYXNzd29yZD'. The detailed view for this frame shows the full request and response headers, including the Authorization header and the response body which contains the challenge for the user to enter their credentials.

→ Decoding the credentials

The form displays the message: 'The Form.SizeLimit is 10000000bytes. Please, do not post more data using this form.' Below it, it says 'Source data from the Base64 string:' followed by a text area containing 'wireshark-students'. A note below the text area says: 'Type (or copy-paste) some text to a textbox bellow. The text can be a Base64 string to decode or any string to encode to a Base64 string.' At the bottom, there are buttons for 'Choose File' (with 'no file selected') and 'Convert the source data'.