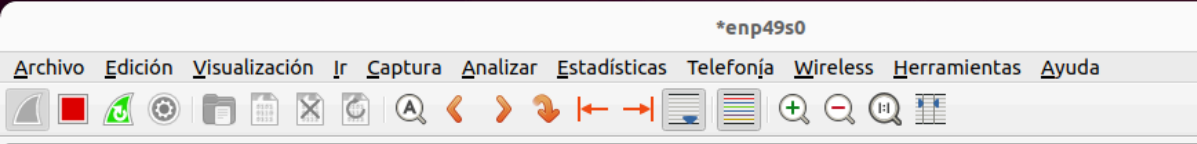


1. Start up your web browser.

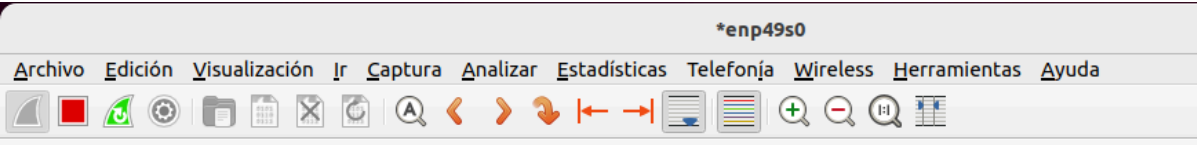
2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don't yet begin packet capture). Enter "http" (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We're only interested in the HTTP protocol here, and don't want to see the clutter of all captured packets).

Una vez arrancado Wireshark, comprobamos las entradas de conexión a nuestro ordenador



No.	Time	Source	Destination	Protocol	Length	Info
826	76.521302478	10.1.2.148	142.250.201.78	TCP	1466	60762 → 443 [ACK]
827	76.521304072	10.1.2.148	142.250.201.78	TCP	1466	60762 → 443 [ACK]
828	76.521305217	10.1.2.148	142.250.201.78	TLSv1.3	560	Application Data
829	76.521334457	10.1.2.148	142.250.201.78	TLSv1.3	213	Application Data
830	76.526345264	142.250.201.78	10.1.2.148	TCP	66	443 → 60762 [ACK]
831	76.527426273	142.250.201.78	10.1.2.148	TCP	66	443 → 60762 [ACK]
832	76.533361960	142.250.201.78	10.1.2.148	TCP	66	443 → 60762 [ACK]
833	76.533816460	142.250.201.78	10.1.2.148	TCP	66	443 → 60762 [ACK]
834	76.533816829	142.250.201.78	10.1.2.148	TCP	66	443 → 60762 [ACK]

Si ya hemos realizado la acción, deberemos aplicar en el buscador un filtro con "http" y debería de salir como en la siguiente imagen



No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

Lógicamente no veremos ninguna entrada ya que para buscar la conexión http deberemos hacer conexión con alguna web

3. Enter the following to your browser

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

Your browser should display the very simple, one-line HTML file.

A continuación, entraremos en el link que nos propone la actividad y deberemos ver el siguiente mensaje:



4. Stop Wireshark packet capture.

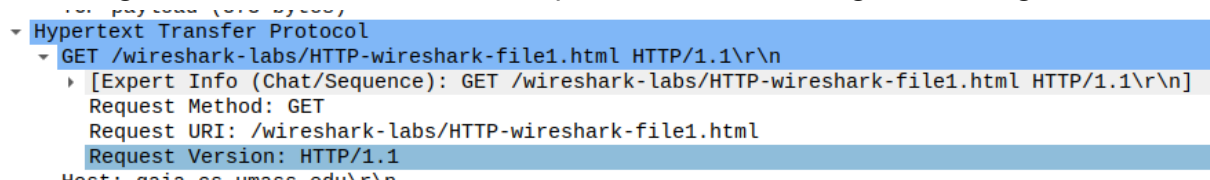
Si vemos el mensaje el siguiente paso sera parar nuestra captura

Una vez parada, para comprobar que lo tenemos bien, podemos aplicar de nuevo el filtro de "http" y en este caso si veremos las siguientes entradas

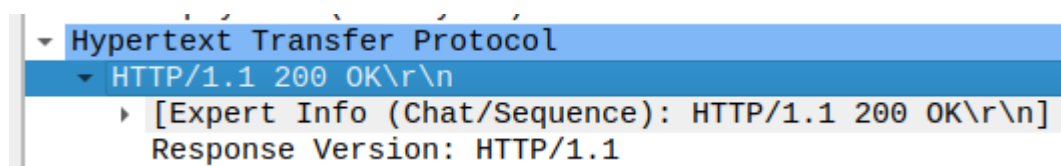
A screenshot of the Wireshark network protocol analyzer. The packet list pane shows two captured packets. The first packet, number 5019, is an HTTP GET request from 10.1.2.148 to 185.125.190.98. The second packet, number 5020, is the corresponding HTTP 204 No Content response from 185.125.190.98 to 10.1.2.148. The packet details pane for packet 5020 is expanded, showing the Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol layers. The HTTP layer shows '204 No Content'.

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

Mi navegador usa la versión 1.1 como podemos ver en la siguiente imagen



Y aqui podemos ver como la version del servidor tambien es 1.1



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

```
Accept-Content-Type: application/javascript\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: es-ES,es;q=0.9\r\n
\r\n
[Full request URI: http://gaia.cs.umass.
[HTTP request 1/1]
[Response in frame 65]
```

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

Mi direccion IP es: 10.1.2.148 y la direccion de la pagina es 185.125.190.98

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

No.	Time	Source	Destination	Protocol	Length	Info
49	2.399700911	172.20.10.3	128.119.245.12	HTTP	627	GET /wireshark-labs/HTTP-wire
54	2.571202156	128.119.245.12	172.20.10.3	HTTP	293	HTTP/1.1 304 Not Modified
57	2.574290598	172.20.10.3	128.119.245.12	HTTP	542	GET /wireshark-labs/HTTP-wire
65	2.734232796	128.119.245.12	172.20.10.3	HTTP	540	HTTP/1.1 200 OK (text/html)

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

```
Date: Mon, 23 Sep 2024 17:24:32 GMT\r\n
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips F
Last-Modified: Mon, 23 Sep 2024 05:59:01 GMT\r\n
```

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

```
Frame Number: 65
Frame Length: 540 bytes (4320 bits)
Capture Length: 540 bytes (4320 bits)
```

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.

```
[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
```

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, en la primera respuesta HTTP no encontramos ningun “if-modified-since”

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

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?

Si, en la segunda respuesta de HTTP encontramos la siguiente información:

```
If-Modified-Since: Mon, 23 Sep 2024 05:59:01 GMT\r\n\r\n
```

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.

En este caso tenemos el código 200 OK, esto significa que ha encontrado la página web correctamente

57	2.5/4290598	172.20.10.3	128.119.245.12	HTTP	542	GET /wireshark-labs/
65	2.734232796	128.119.245.12	172.20.10.3	HTTP	540	HTTP/1.1 200 OK (tex

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?

Mi navegador envió 2 paquetes GET

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

```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 304 Not Modified\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
      [HTTP/1.1 304 Not Modified\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 304
      [Status Code Description: Not Modified]
      Response Phrase: Not Modified
      Date: Mon, 23 Sep 2024 17:24:32 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
```

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

El código de estado más común que deberías encontrar es 200 OK

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

tcp.analysis.retransmission						
No.	Time	Source	Destination	Protocol	Length	Info
176	11.448504949	34.149.100.209	172.20.10.3	TCP	112	[TCP Retransmission]
203	11.653723021	35.201.103.21	172.20.10.3	TCP	1167	[TCP Spurious Retran
227	11.793902229	172.20.10.3	35.201.103.21	TCP	275	[TCP Retransmission]
243	11.858781568	34.160.90.233	172.20.10.3	TCP	873	[TCP Spurious Retran
257	11.879101633	35.244.181.201	172.20.10.3	TCP	709	[TCP Spurious Retran
279	12.050032758	172.20.10.3	34.160.90.233	TCP	104	[TCP Retransmission]
280	12.058026729	172.20.10.3	35.244.181.201	TCP	104	[TCP Retransmission]
296	12.105020923	34.160.90.233	172.20.10.3	TCP	112	[TCP Spurious Retran
330	12.234316182	34.98.75.36	172.20.10.3	TCP	376	[TCP Spurious Retran
381	12.677615964	34.160.144.191	172.20.10.3	TCP	374	[TCP Spurious Retran
410	13.097967010	172.20.10.3	34.160.144.191	TCP	201	[TCP Retransmission]

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

Mando dos mensajes de respuesta

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.