colegio CALASANZ SALAMANCA

Paseo de Canalejas, 139-159
37001 Salamanca
Tel.: 923 26 79 61 | Fax: 923 27 04 54
www.calasanzsalamanca.es
CENTRO PRIVADO CONCERTADO

ANÁLISIS DEL CONTENIDO DE LOS MENSAJES DE PETICIÓN Y RESPUESTA DEL PROTOCOLO HTTP

Instrucciones:

1. El documento de entrega deberá estar en formato pdf. No cumplir con este punto supondrá 0,5 menos en la nota final del ejercicio.
2. Cada pregunta, de la a a) la l), vale un punto.
3. Las respuestas deberán razonarse. Una respuesta no razonada contará la mitad y, si no se ve en la imagen o texto de la trama el dato que justifica tu respuesta, ésta no será válida.

Ejercicio:

1. Captura el tráfico de la red mientras accedes a alguna, o todas, de las siguientes páginas:
   a. http://testhtml5.vulnweb.com/#/about
   b. http://www.cs.toronto.edu/~arnold/427/19s/427_19S/tool/Wireshark/index.html

2. Para la captura y analiza las tramas enviadas y recibidas.

3. Elige una trama HTTP (dedica un tiempo a elegirla para que sea lo más completa posible).

4. Incluye en el documento, antes de cualquier respuesta, la trama completa (mediante captura de imagen o incluyendo todo el texto). Tienen que verse todas las cabeceras de petición y respuesta. Si la trama es muy larga, no incluyas el cuerpo de la respuesta, solo las cabeceras. Si necesitas incluir más imágenes de WireShark para justificar tus respuestas, hazlo.

5. Responde a las siguientes preguntas:

a. ¿Cuál es la IP de la máquina donde se ejecuta el servidor?

```
GET / HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 OPR/122.0.0.0
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
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8


HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 10 Oct 2025 10:40:43 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Access-Control-Allow-Origin: *
Content-Encoding: gzip
```

http

No.	Time	Source	Destination	Protocol	Lengtl	Info
1603	11.827814	10.0.0.207	44.228.249.3	HTTP	472	GET /static/img/logo2.png HTTP/1.1

```
Source Address: 10.0.0.207
```

La ip es: 10.0.0.207

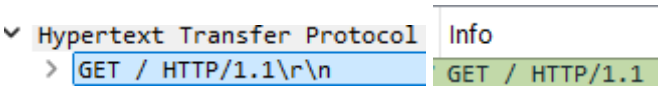
b. ¿Qué versión de HTTP se utiliza?

Protocol	Lengtl	Info
HTTP	547	GET / HTTP/1.1

```
GET / HTTP/1.1
```

Se utiliza la versión 1.1

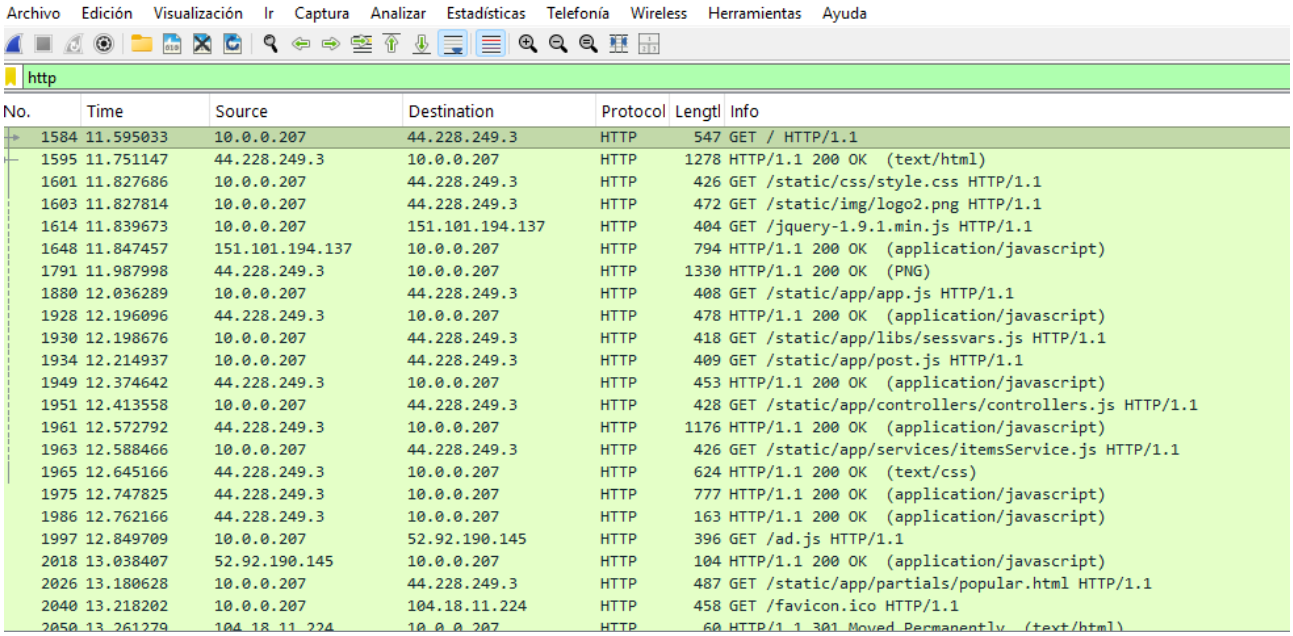
c. ¿Qué método de petición se utiliza?



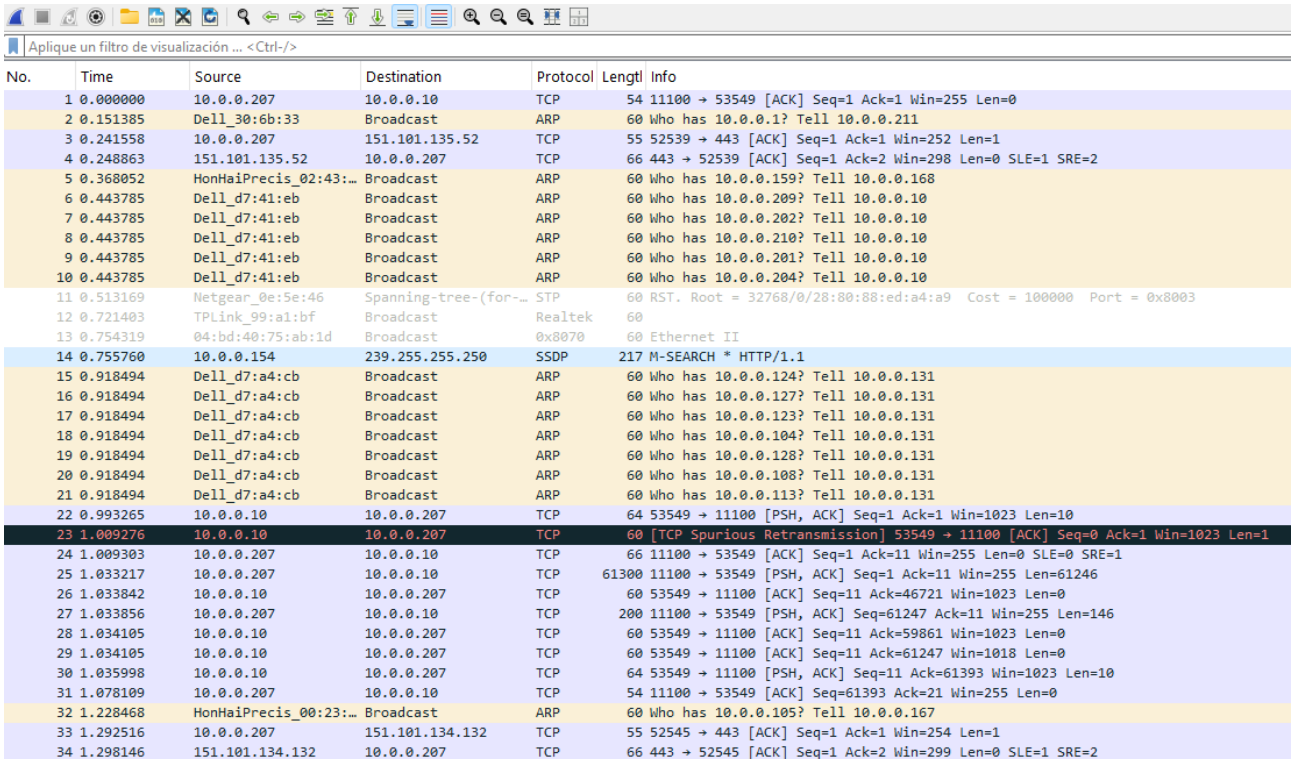
GET

d. ¿Qué recurso se solicita al servidor?

Se le solicita que sea http



Ya que nos facilita la busqueda porque si no tendriamos algo como esto:



e. ¿Qué valor tiene la cabecera Host?

Tiene como valor: `Host: testhtml5.vulnweb.com`

f. ¿Se envían cookies en la petición HTTP?

Si, la encontramos con un identificador único en unas cabeceras más abajo:

```
GET /static/css/style.css HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36 OPR/122.0.0.0
Accept: text/css,*/*;q=0.1
Referer: http://testhtml5.vulnweb.com/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8


HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 10 Oct 2025 10:40:43 GMT
Content-Type: text/css
Content-Length: 570
Last-Modified: Fri, 10 May 2013 09:00:28 GMT
Connection: keep-alive
ETag: "518cb72c-23a"
Expires: Sun, 09 Nov 2025 10:40:43 GMT
Cache-Control: max-age=2592000
Accept-Ranges: bytes

ETag: "518cb72c-23a"
```

g. ¿Qué idioma utiliza el navegador?

Utiliza en: `<html lang="en"`

Aunque en la cabecera GET se acepta el español y/o el ingles:

```
Accept-Language: es-ES,es;q=0.9,en;q=0.8
```

h. ¿Qué código de estado tiene la respuesta HTTP?

La 2xx el cual indica que todo está correcto:

```
HTTP/1.1 200 OK
```

i. ¿Qué servidor web y versión se utiliza?

Se está utilizando Mozilla con la versión 5.0:

```
User-Agent: Mozilla/5.0
```

j. ¿De qué tipo MIME es el recurso recibido?

El tipo de archivo que permiten son: html, avif, webp, apng, */*

```
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
```

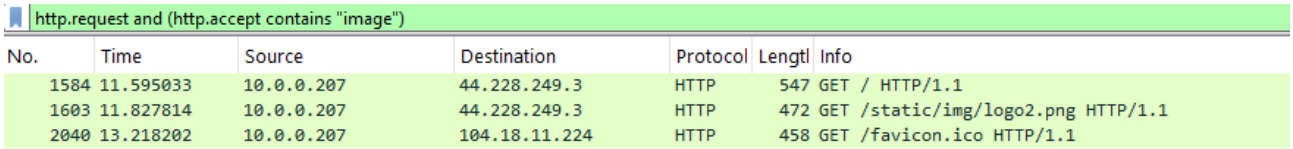
k. ¿Se han utilizado conexiones persistentes?

Ha sido una conexión en donde se ha mantenido correctamente

```
Connection: keep-alive
```

l. ¿Existen peticiones y respuestas de imágenes?

Si, aplicando el siguiente filtro de búsqueda: http.request and (http.accept contains "image")



```
GET /static/img/logo2.png HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/138.0.0.0 Safari/537.36 OPR/122.0.0.0
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://testhtml5.vulnweb.com/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8


HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 10 Oct 2025 10:40:43 GMT
Content-Type: image/png
Content-Length: 2736
Last-Modified: Thu, 02 May 2013 14:50:21 GMT
Connection: keep-alive
ETag: "51827d2d-ab0"
Expires: Sun, 09 Nov 2025 10:40:43 GMT
Cache-Control: max-age=2592000
Accept-Ranges: bytes
```

```
GET /static/app/app.js HTTP/1.1
Host: testhtml5.vulnweb.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/138.0.0.0 Safari/537.36 OPR/122.0.0.0
Accept: */*
Referer: http://testhtml5.vulnweb.com/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9,en;q=0.8


HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 10 Oct 2025 10:40:43 GMT
Content-Type: application/javascript
Content-Length: 1884
Last-Modified: Tue, 14 May 2013 09:19:07 GMT
Connection: keep-alive
ETag: "5192018b-75c"
Expires: Sun, 09 Nov 2025 10:40:43 GMT
Cache-Control: max-age=2592000
Accept-Ranges: bytes
```

O buscar en la captura el tipo de archivo que se acepta:

http

No.	Time	Source	Destination	Protocol	Lengtl	Info
1584	11.595033	10.0.0.207	44.228.249.3	HTTP	547	GET / HTTP/1.1
1595	11.751147	44.228.249.3	10.0.0.207	HTTP	1278	HTTP/1.1 200 OK (text/html)
1601	11.827686	10.0.0.207	44.228.249.3	HTTP	426	GET /static/css/style.css HTTP/1.1
1603	11.827814	10.0.0.207	44.228.249.3	HTTP	472	GET /static/img/logo2.png HTTP/1.1
1614	11.839673	10.0.0.207	151.101.194.137	HTTP	404	GET /jquery-1.9.1.min.js HTTP/1.1
1648	11.847457	151.101.194.137	10.0.0.207	HTTP	794	HTTP/1.1 200 OK (application/javascript)
1791	11.987998	44.228.249.3	10.0.0.207	HTTP	1330	HTTP/1.1 200 OK (PNG)

****Nota:** Si alguna de las preguntas no pudieras responderla porque no había en la trama información sobre ese dato, busca otra trama que si la tenga. Incluye imagen de la misma.