



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	Length	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

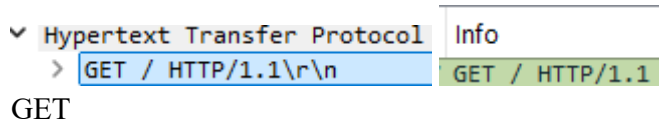
b. ¿Qué versión de HTTP se utiliza?

Protocol	Length	Info
HTTP	547	GET / HTTP/1.1

GET / HTTP/1.1

Se utiliza la versión 1.1

c. ¿Qué método de petición se utiliza?



d. ¿Qué recurso se solicita al servidor?

Se le solicita que sea http

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda						
http						
No.	Time	Source	Destination	Protocol	Length	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)
1880	12.036289	10.0.0.207	44.228.249.3	HTTP	408	GET /static/app/app.js HTTP/1.1
1928	12.196096	44.228.249.3	10.0.0.207	HTTP	478	HTTP/1.1 200 OK (application/javascript)
1930	12.198676	10.0.0.207	44.228.249.3	HTTP	418	GET /static/app/libs/sockjs.js HTTP/1.1
1934	12.214937	10.0.0.207	44.228.249.3	HTTP	409	GET /static/app/post.js HTTP/1.1
1949	12.374642	44.228.249.3	10.0.0.207	HTTP	453	HTTP/1.1 200 OK (application/javascript)
1951	12.413558	10.0.0.207	44.228.249.3	HTTP	428	GET /static/app/controllers/controllers.js HTTP/1.1
1961	12.572792	44.228.249.3	10.0.0.207	HTTP	1176	HTTP/1.1 200 OK (application/javascript)
1963	12.588466	10.0.0.207	44.228.249.3	HTTP	426	GET /static/app/services/itemsService.js HTTP/1.1
1965	12.645166	44.228.249.3	10.0.0.207	HTTP	624	HTTP/1.1 200 OK (text/css)
1975	12.747825	44.228.249.3	10.0.0.207	HTTP	777	HTTP/1.1 200 OK (application/javascript)
1986	12.762166	44.228.249.3	10.0.0.207	HTTP	163	HTTP/1.1 200 OK (application/javascript)
1997	12.849709	10.0.0.207	52.92.190.145	HTTP	396	GET /ad.js HTTP/1.1
2018	13.038407	52.92.190.145	10.0.0.207	HTTP	104	HTTP/1.1 200 OK (application/javascript)
2026	13.180628	10.0.0.207	44.228.249.3	HTTP	487	GET /static/app/partials/popular.html HTTP/1.1
2040	13.218202	10.0.0.207	104.18.11.224	HTTP	458	GET /favicon.ico HTTP/1.1
2050	13.261279	104.18.11.224	10.0.0.207	HTTP	60	HTTP/1.1 301 Moved Permanently (text/html)

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

Aplique un filtro de visualización ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.207	10.0.0.10	TCP	54	11100 → 53549 [ACK] Seq=1 Ack=1 Win=255 Len=0
2	0.151385	Dell_30:6b:33	Broadcast	ARP	60	Who has 10.0.0.1? Tell 10.0.0.211
3	0.241558	10.0.0.207	151.101.135.52	TCP	55	52539 → 443 [ACK] Seq=1 Ack=1 Win=252 Len=1
4	0.248863	151.101.135.52	10.0.0.207	TCP	66	443 → 52539 [ACK] Seq=1 Ack=2 Win=298 Len=0 SLE=1 SRE=2
5	0.368052	HonHaiPrecis_02:43:...	Broadcast	ARP	60	Who has 10.0.0.159? Tell 10.0.0.168
6	0.443785	Dell_d7:41:eb	Broadcast	ARP	60	Who has 10.0.0.209? Tell 10.0.0.10
7	0.443785	Dell_d7:41:eb	Broadcast	ARP	60	Who has 10.0.0.202? Tell 10.0.0.10
8	0.443785	Dell_d7:41:eb	Broadcast	ARP	60	Who has 10.0.0.210? Tell 10.0.0.10
9	0.443785	Dell_d7:41:eb	Broadcast	ARP	60	Who has 10.0.0.201? Tell 10.0.0.10
10	0.443785	Dell_d7:41:eb	Broadcast	ARP	60	Who has 10.0.0.204? Tell 10.0.0.10
11	0.513169	Netgear_0e:5e:46	Spanning-tree-for-...	STP	60	RST. Root = 32768/0/28:80:88:ed:a4:a9 Cost = 100000 Port = 0x8003
12	0.721403	TPLink_99:a1:bf	Broadcast	Realtek	60	
13	0.754319	04:bd:40:75:ab:1d	Broadcast	0x8070	60	Ethernet II
14	0.755760	10.0.0.154	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
15	0.918494	Dell_d7:a4:cb	Broadcast	ARP	60	Who has 10.0.0.124? Tell 10.0.0.131
16	0.918494	Dell_d7:a4:cb	Broadcast	ARP	60	Who has 10.0.0.127? Tell 10.0.0.131
17	0.918494	Dell_d7:a4:cb	Broadcast	ARP	60	Who has 10.0.0.123? Tell 10.0.0.131
18	0.918494	Dell_d7:a4:cb	Broadcast	ARP	60	Who has 10.0.0.104? Tell 10.0.0.131
19	0.918494	Dell_d7:a4:cb	Broadcast	ARP	60	Who has 10.0.0.128? Tell 10.0.0.131
20	0.918494	Dell_d7:a4:cb	Broadcast	ARP	60	Who has 10.0.0.108? Tell 10.0.0.131
21	0.918494	Dell_d7:a4:cb	Broadcast	ARP	60	Who has 10.0.0.113? Tell 10.0.0.131
22	0.993265	10.0.0.10	10.0.0.207	TCP	64	53549 → 11100 [PSH, ACK] Seq=1 Ack=1 Win=1023 Len=10
23	1.009276	10.0.0.10	10.0.0.207	TCP	60	[TCP Spurious Retransmission] 53549 → 11100 [ACK] Seq=0 Ack=1 Win=1023 Len=1
24	1.009303	10.0.0.207	10.0.0.10	TCP	66	11100 → 53549 [ACK] Seq=1 Ack=11 Win=255 Len=0 SLE=0 SRE=1
25	1.033217	10.0.0.207	10.0.0.10	TCP	61300	11100 → 53549 [PSH, ACK] Seq=1 Ack=11 Win=255 Len=61246
26	1.033842	10.0.0.10	10.0.0.207	TCP	60	53549 → 11100 [ACK] Seq=11 Ack=46721 Win=1023 Len=0
27	1.033856	10.0.0.207	10.0.0.10	TCP	200	11100 → 53549 [PSH, ACK] Seq=61247 Ack=11 Win=255 Len=146
28	1.034105	10.0.0.10	10.0.0.207	TCP	60	53549 → 11100 [ACK] Seq=11 Ack=59861 Win=1023 Len=0
29	1.034105	10.0.0.10	10.0.0.207	TCP	60	53549 → 11100 [ACK] Seq=11 Ack=61247 Win=1018 Len=0
30	1.035998	10.0.0.10	10.0.0.207	TCP	64	53549 → 11100 [PSH, ACK] Seq=11 Ack=61393 Win=1023 Len=10
31	1.078109	10.0.0.207	10.0.0.10	TCP	54	11100 → 53549 [ACK] Seq=61393 Ack=21 Win=255 Len=0
32	1.228468	HonHaiPrecis_00:23:...	Broadcast	ARP	60	Who has 10.0.0.105? Tell 10.0.0.167
33	1.292516	10.0.0.207	151.101.134.132	TCP	55	52545 → 443 [ACK] Seq=1 Ack=1 Win=254 Len=1
34	1.298146	151.101.134.132	10.0.0.207	TCP	66	443 → 52545 [ACK] Seq=1 Ack=2 Win=299 Len=0 SLE=1 SRE=2

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")

http.request and (http.accept contains "image")						
No.	Time	Source	Destination	Protocol	Length	Info
1584	11.595033	10.0.0.207	44.228.249.3	HTTP	547	GET / HTTP/1.1
1603	11.827814	10.0.0.207	44.228.249.3	HTTP	472	GET /static/img/logo2.png HTTP/1.1
2040	13.218202	10.0.0.207	104.18.11.224	HTTP	458	GET /favicon.ico HTTP/1.1

```
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	Length	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.