

2011-
2012

Actividad 2 Protocolo HTTP. Capturas con sniffer



José Jiménez Arias
IES Gregorio Prieto
2011-2012

1. Inicia sesión en Windows o GNU/Linux.
2. Inicia una captura con el programa sniffer Wireshark.
3. Abre el navegador Firefox, conéctate a un sitio web y para la captura de Wireshark.
4. Sitúate sobre el primer mensaje HTTP, haz clic con el botón derecho del ratón y selecciona "Follow TCP Stream" para analizar el intercambio de mensajes HTTP. Observa la conexión TCP, las peticiones y respuestas HTTP, las cookies, las cookies, las cabeceras, tipos y subtipos MIME, ...etc.

The screenshot shows the 'Follow TCP Stream' window in Wireshark. The 'Stream Content' pane displays the following text:

```

POST /getlicexp HTTP/1.1
User-Agent: Java/1.6.0_26
Host: exp02.eset.com
Accept: text/html, image/gif, image/jpeg, *, q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 468

<?xml version="1.0" encoding="UTF-8"?><GETLICEXP><SECTION
ID="1000103"><LICENSEREQUEST><NODE NAME="UsernamePassword"
VALUE="PSLULNWSKUSEMELBKSKAHMBFMSMKMKMAMQMLMSMA" TYPE="STRING"/><NODE NAME="Product"
VALUE="eav" TYPE="STRING"/><NODE NAME="Version" VALUE="4.0.437.0" TYPE="STRING"/><NODE
NAME="Language" VALUE="c0a" TYPE="DWORD"/><NODE NAME="UpdateTag" VALUE="" TYPE="STRING"/>
<NODE NAME="System" VALUE="6.1" TYPE="STRING"/></LICENSEREQUEST></SECTION></GETLICEXP>

HTTP/1.1 200 OK
Date: Fri, 13 Jan 2012 07:48:12 GMT
Server: Apache/2.2.16 (Debian)
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

b
unknownlic
0
  
```

At the bottom of the window, there are buttons for 'Find', 'Save As', 'Print', and 'Entire conversation (905 bytes)'. There are also radio buttons for 'ASCII', 'EBCDIC', 'Hex Dump', 'C Arrays', and 'Raw' (which is selected). There are also buttons for 'Filter Out This Stream' and 'Close'.

Responde a las siguientes preguntas:

a) ¿Qué versión de HTTP se utiliza?

1.1

¿Qué método se ha usado en la primera petición HTTP?

POST

b) ¿Qué valor tiene la cabecera *Host*?. ¿Para qué las usará el servidor?.

Exp02.eset.com

c) ¿Qué algoritmos de compresión soporta el navegador?

Encoding

d) ¿Se envían *cookies* en la petición HTTP?.

no

e) ¿Qué código de estado tiene la primera respuesta HTTP?

200

¿Qué servidor web responde?

Apache 2.2.16

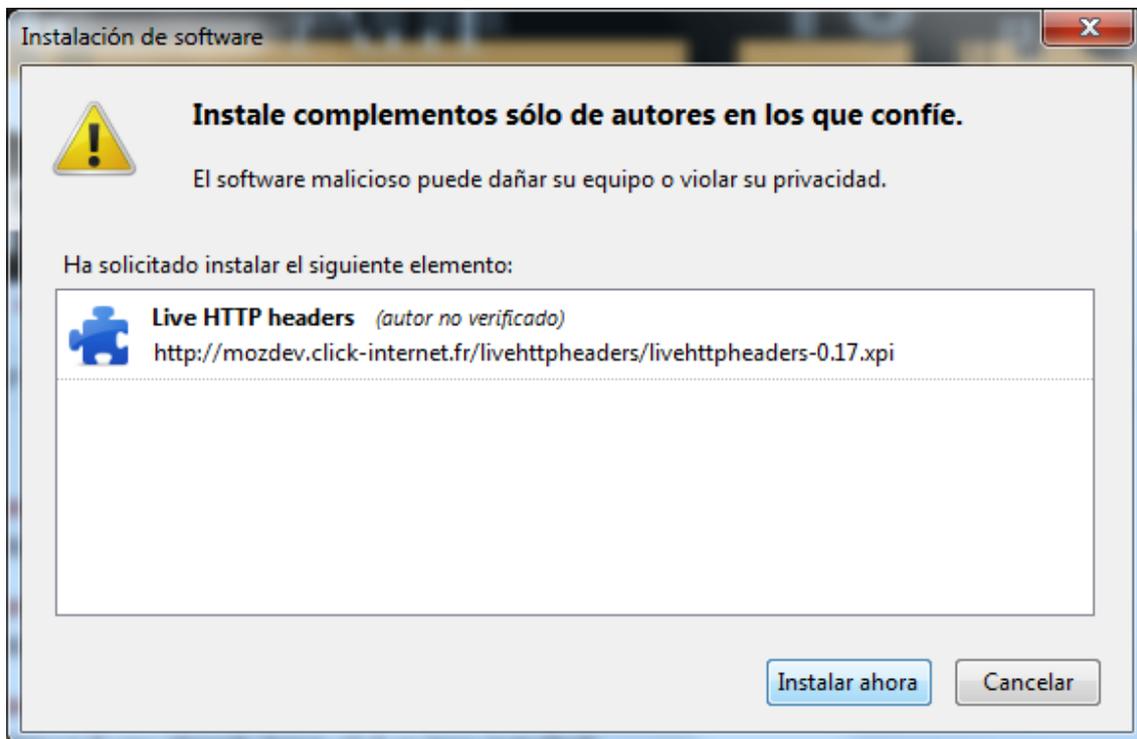
f) ¿De qué tipo MIME es el recurso enviado?.

Text/Html

g) ¿ Se han utilizado conexiones persistentes, es decir, en la misma conexión TCP haya varias peticiones y respuestas HTTP?

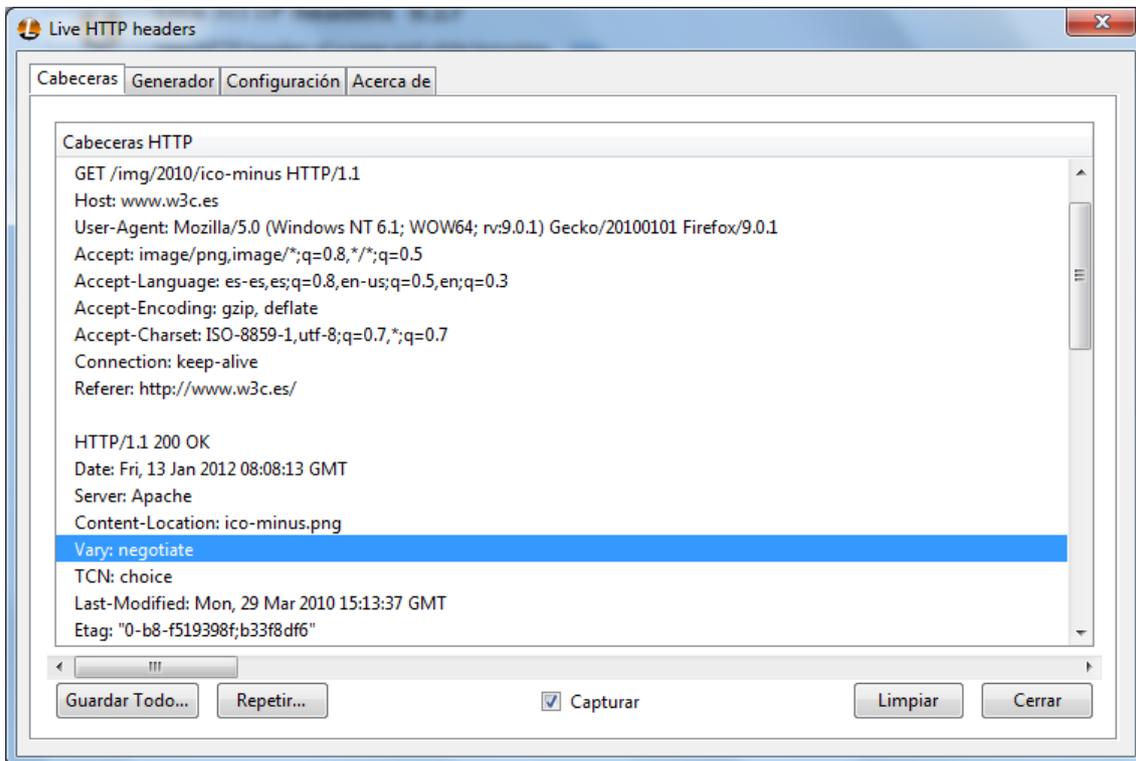
No

5. Descarga e instala en Firefox el complemento Live HTTP Headers. Reinicia el navegador.



6. Acceder al menú, herramientas, Live HTTP Headers.

7. Acceder de nuevo al sitio web elegido y consulta y documente las cabeceras con la utilidad instalada.



Usa HTTP 1.1

método → GET

petición de imágenes al Host → www.w3c.es Código de estado → 200

Servidor Apache

8. Inicia el navegador *Google Chrome*.
9. Pincha en el botón con una herramienta en la parte superior derecha. Accede a Herramientas, Herramientas para desarrolladores.
10. Acceder al sitio web mencionado e investigar la herramienta para desarrolladores. Observé y documente las peticiones realizadas, qué método usan, cuáles son los códigos de respuesta, qué tipos de recursos se han recibido del servidor, cuál es el código de las páginas HTML enviadas, etc.

Name	Path	Method	Status	Type	Initiator	Size	Time	Latency	Timeline
	http://www.w3c.es/	GET	200 OK	text/html	http://www.w3c.es/:197 Parser	14.82KB 14.63KB	2.59s	649ms	849ms, 973ms, 1.30s, 1.62s, 1.95s, 2.27s, 2.69s
	minimum/css/2010	GET	200 OK	text/css	http://www.w3c.es/:11 Parser	(from cache)	Pending	649ms	
	es/css/2010	GET	200 OK	text/css	http://www.w3c.es/:12 Parser	(from cache)	1ms	0	
	advanced	GET	206	text/css	http://www.w3c.es/:17 Parser	(from cache)	1ms		