## 2011-2012

## Actividad 2 Protocolo HTTP. Capturas con sniffer



José Jiménez Arias IES Gregorio Prieto 2011-2012

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.

Follow TCP Stream	- 0 <b>x</b>
Stream Content 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 TO WITH THE PROPERTY OF THE</section </getlicexp>	
<pre>Def 100013"&gt;<licenserequesi><node <br="" name="UsernamePassword">VALUE="PSLULNWSKUSEMELBKSKAHMBEMSMKMKMAMQMLMSMA" TYPE="STRING"/&gt;<node eav"="" name="Produc&lt;br&gt;VALUE=" type="STRING"></node><node name="Version" type="STRING" value="4.0.437.0"></node>&lt; NAME="Language" VALUE="C0a" TYPE="DWORD"/&gt;<node name="UpdateTag" st<br="" value="TYPE=">&gt;<node name="System" type="STRING" value="6.1"></node>HTTP/1.1 200 0K 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</node></node></licenserequesi></pre>	:t" NODE RING"/ ICEXP> ₽
b unknownlic 0 I <u>Find Save As Print</u> Entire conversation (905 bytes) • ASCI © EBCDIC © Hex Dump © C	↓ Arrays   Raw
Help Filter Out This Stream	<u>C</u> lose

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

## Actividad 2 Protocolo HTTP. Capturas con sniffer

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.

In	stalación de software
	Instale complementos sólo de autores en los que confíe. El software malicioso puede dañar su equipo o violar su privacidad.
	Ha solicitado instalar el siguiente elemento:
	Live HTTP headers (autor no verificado) http://mozdev.click-internet.fr/livehttpheaders/livehttpheaders-0.17.xpi
	Instalar ahora Cancelar

2011-2012

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.

🕒 Live HTTF	P headers		X
Cabeceras	Generador Configuraciór	Acerca de	
Cabece	ras HTTP	1	
Host: User-A	img/2010/1co-minus HTTP/ www.w3c.es Agent: Mozilla/5.0 (Window it: image/png image/*:g=0.	.1 NT 6.1; WOW64; rv:9.0.1) Gecko/20100101 Firefox/9.0.1 */*:α=0.5	
Accep Accep Accep	ot-Language: es-es,es;q=0.8 ot-Encoding: gzip, deflate ot-Charset: ISO-8859-1, utf-8	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	E
Conne Refere	ection: keep-alive er: http://www.w3c.es/		
HTTP/ Date: I Server	/1.1 200 OK Fri, 13 Jan 2012 08:08:13 GM :: Apache		
Conte Vary: r TCN: 0	nt-Location: ico-minus.png negotiate choice		_
Last-N Etag: "	Modified: Mon, 29 Mar 2010 "0-b8-f519398f;b33f8df6"	5:13:37 GMT	~
∢ Guarda	III Ir Todo Repetir	Capturar Limpiar	r Cerrar

Usa HTTP 1.1 método→ GET petición de imágenes al Host→www.w3c.es Codigo 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.

🧟 Elements 🕢 Resources 🔕 Network 📴 Scripts 🕂 Timeline 🐚 Profiles 🖳 Audits 🌄 Console								Q Search Network			8	)			
Name Path	Method	Status Text	Туре	Initiator	Size Content	Time Latency	Timeline	649ms	973ms	1.30s	1.62s	1.95s	2.27s	2.59s	
http://www.w3c.es/	GET	200 OK	text/html	http://www.w3c.es/:197 Parser	14.82KB	2.59s									* 11
CSS /css/2010	GET	200 OK	text/css	http://www.w3c.es/:11 Parser	(from cache)	Pending			٥						
es CSS /css/2010	GET	200 ОК	text/css	<u>http://www.w3c.es/:12</u> Parser	(from cache)	1ms 0		(	٥						
advanced	OFT	206	taxtions	http://www.w3c.es/:17	(from oppho)	1ms			a						Ŧ
🖳 🔀 Q, 🧮 🖲 🔕 💷 Documents Stylesheets Images Scripts XHR Fonts WebSockets Other											\$	k			