

CHALLENGE 6

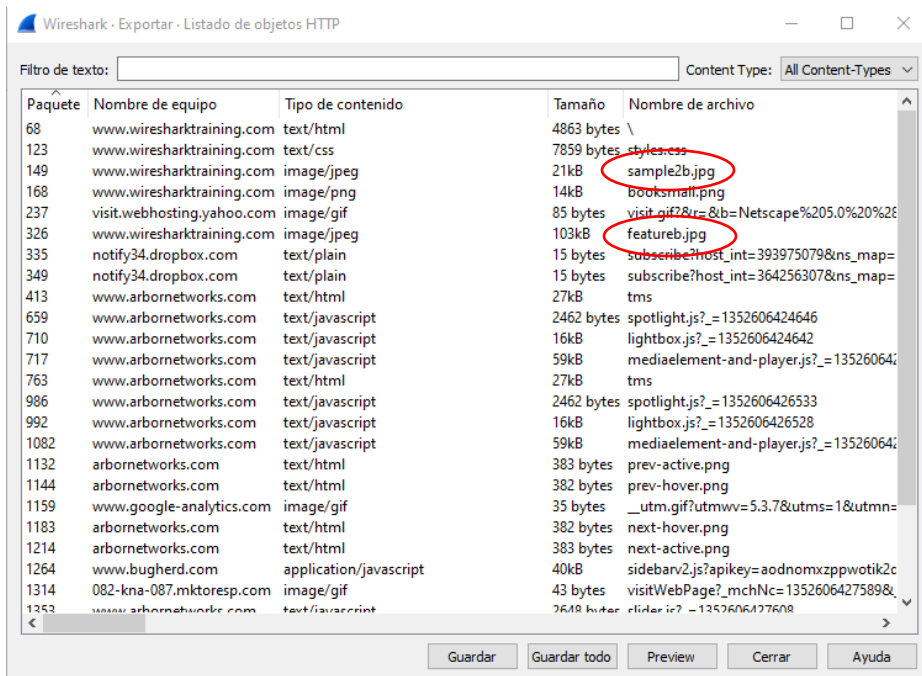


Open **challenge101-6.pcapng** and use the techniques covered in this chapter to answer these Challenge questions. The answer key is located in Appendix A.

Question 6-1.

What two .jpg files can be exported from this trace file?

Exportar objetos | HTTP para averiguar qué objetos HTTP se transfirieron en el archivo de seguimiento. Los dos archivos .jpg son sample2b.jpg y featureb.jpg.

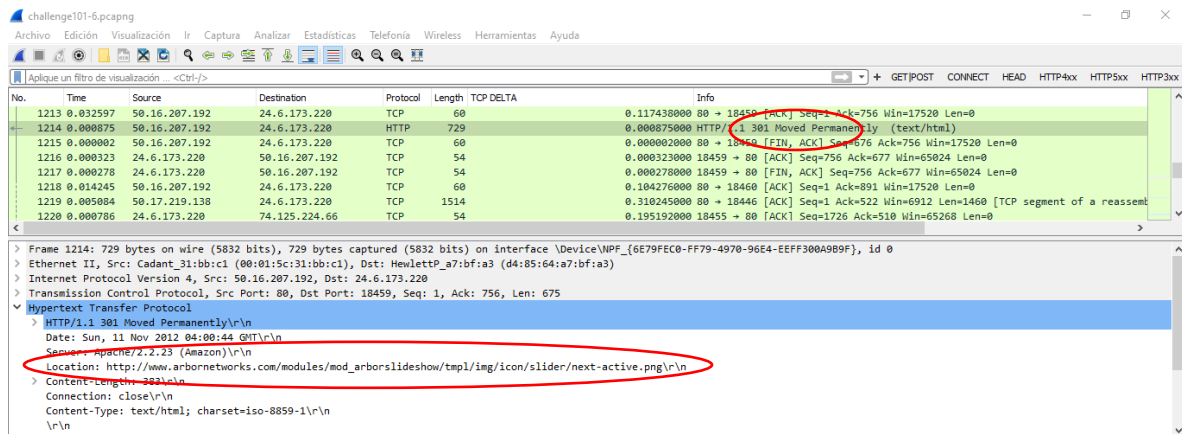


Question 6-2.

On what HTTP server and in what directory does next-active.png reside?

1103	gibdonnetworks.com	text/html	302 bytes	next-move.png
1214	arbornetworks.com	text/html	383 bytes	next-active.png

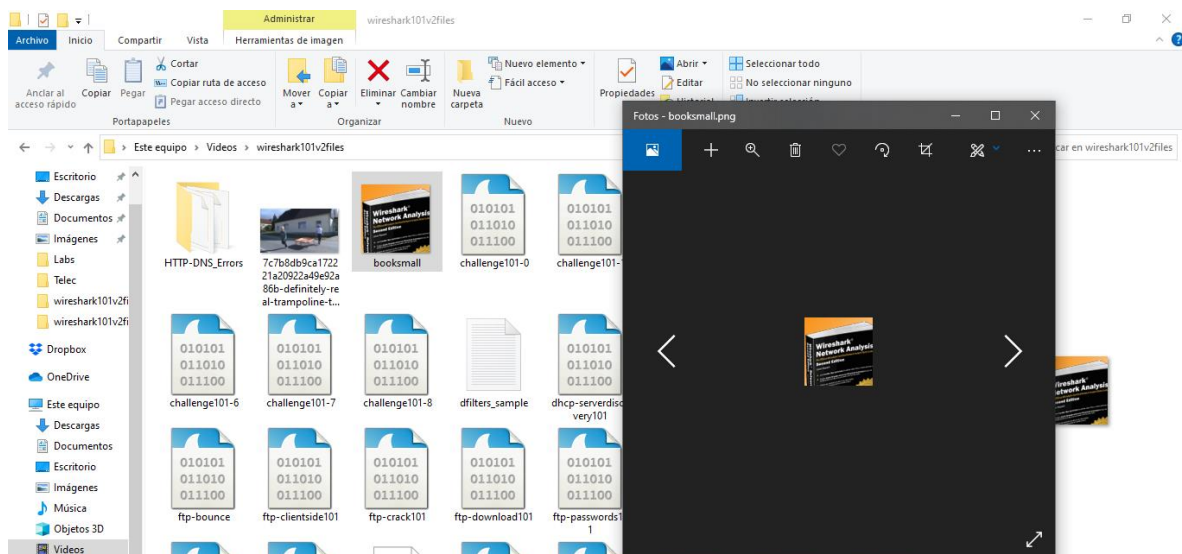
Cuando hace clic en esta entrada para saltar al paquete 1214, vemos una respuesta 301 Moved Permanently que indica que el archivo está en https://www.arbornetworks.com/modules/mod_arborslideshow/tmpl/img/icon/slider/next-active.png.



Question 6-3.

Export booksmall.png from this trace file. What is in the image?

Seleccionamos booksmall.png y seleccionamos Guardar como. Este archivo muestra la mitad superior del libro WiresharkNetwork Analysis sobre un fondo naranja



Question 6-4.

Reassemble TCP stream 7. What type of browser is the client using in this stream?

Este cliente está utilizando Firefox para navegar www.wiresharktraining.com

challenge101-6.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.stream eq 7

No.	Time	Source	Destination	Protocol	Length	TCP DELTA	Info
58	0.001701	24.6.173.220	67.195.61.65	TCP	66		0.000000000 18382 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
59	0.034412	67.195.61.65	24.6.173.220	TCP	66		0.034412000 80 → 18382 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=256
60	0.000234	24.6.173.220	67.195.61.65	TCP	54		0.000234000 18382 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
61	0.000962	24.6.173.220	67.195.61.65	HTTP	388		0.000962000 GET / HTTP/1.1
62	0.037689	67.195.61.65	24.6.173.220	TCP	60		0.037689000 80 → 18382 [ACK] Seq=1 Ack=335 Win=6912 Len=0
63	0.020743	67.195.61.65	24.6.173.220	TCP	1514		0.020743000 80 → 18382 [ACK] Seq=1 Ack=335 Win=6912 Len=1460 [TCP segment of a reassembled
64	0.000005	67.195.61.65	24.6.173.220	TCP	71		0.000005000 80 → 18382 [PSH, ACK] Seq=1461 Ack=335 Win=6912 Len=17 [TCP segment of a reassembled
65	0.000078	24.6.173.220	67.195.61.65	TCP	54		0.000078000 18382 → 80 [ACK] Seq=335 Ack=1470 Win=65700 Len=0

> Frame 61: 388 bytes on wire (3104 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0

> Ethernet II, Src: HewlettP_a7:bfa3 (d4:85:64:a7:bfa3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)

> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 67.195.61.65

> Transmission Control Protocol, Src Port: 18382, Dst Port: 80, Seq: 1, Ack: 1, Len: 334

> Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Host: www.wiresharktraining.com\r\n

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100102 Firefox/16.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

Accept-Language: en-US,en;q=0.5\r\n

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

> Cookie: BX=01831g189nv2a8b=3&s=ns\r\n