

Telefónica

WIRESHARK

Analyze



Analyze
Follow Stream



Analyze

Follow

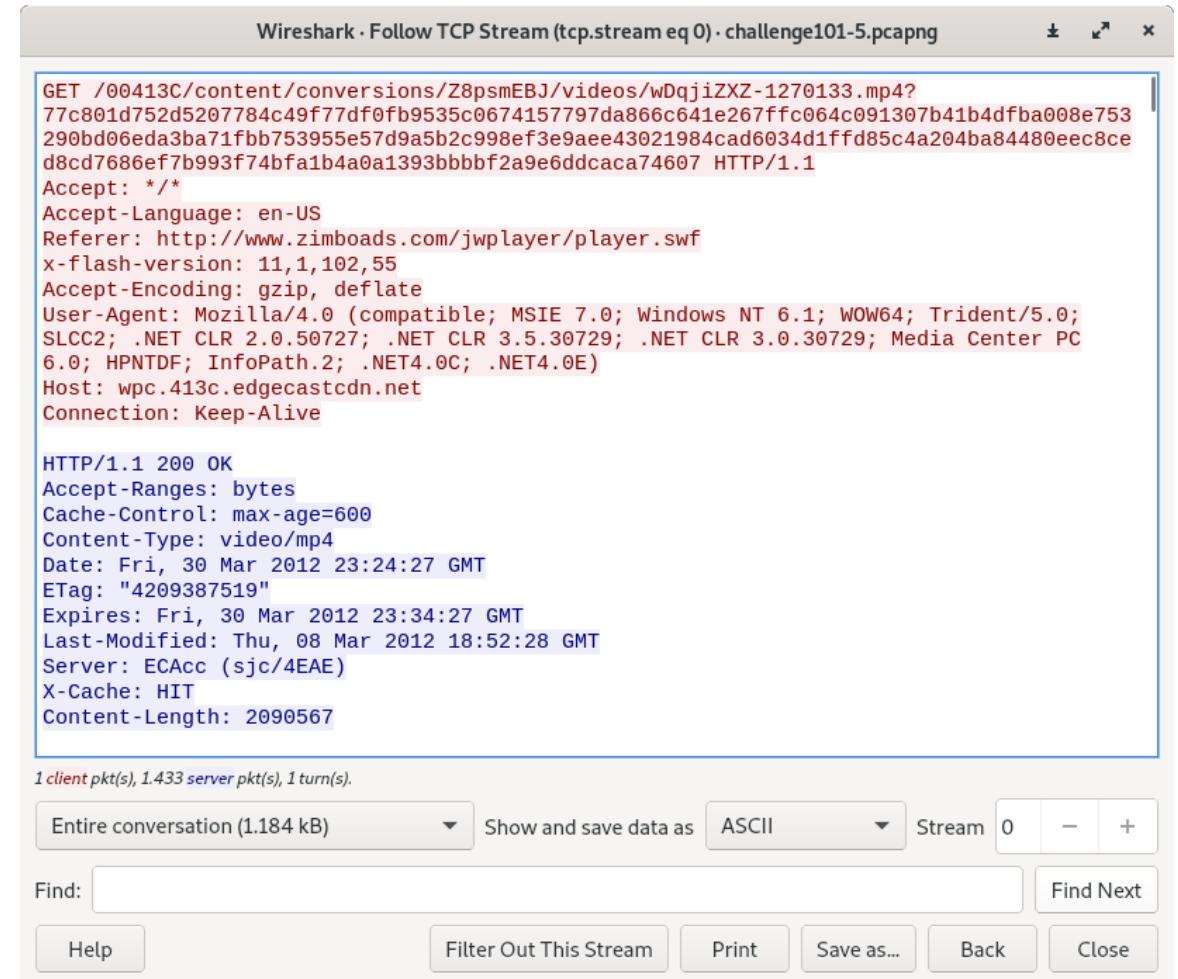
Puede ser muy útil, ver un protocolo en la forma que lo ve la capa de aplicación, puede querer buscar contraseñas, o ver el contenido de una conversación.

- Seleccione el paquete UDP, TCP, TLS o HTTP de la lista de paquetes y selecciónde desde el menú Analyze -> Follow -> (TCP|UDP|TLS|HTTP) stream o seleccione el paquete y acceda a Follow stream con el botón derecho del ratón.
- Wireshark, establecerá un filtro de visualización adecuado y abrirá un cuadro de diálogo, con todos los datos de la secuencia TCP, en orden

Analyze

Follow

El contenido de la transmisión, se mostrará en la misma secuencia que aparece en la red y el tráfico de un sentido estará en rojo y el de sentido contrario, en azul.



The screenshot shows the Wireshark interface with a "Follow TCP Stream" dialog open. The title bar reads "Wireshark · Follow TCP Stream (tcp.stream eq 0) · challenge101-5.pcapng". The main pane displays an HTTP request and response. The request is highlighted in red:

```
GET /00413C/content/conversions/Z8psmEBJ/videos/wDqjiZXZ-1270133.mp4?
77c801d752d5207784c49f77df0fb9535c0674157797da866c641e267ffc064c091307b41b4dfba008e753
290bd06eda3ba71fbb753955e57d9a5b2c998ef3e9aeee43021984cad6034d1ffd85c4a204ba84480eec8ce
d8cd7686ef7b993f74bfa1b4a0a1393bbbbf2a9e6ddcaca74607 HTTP/1.1
Accept: /*
Accept-Language: en-US
Referer: http://www.zimboards.com/jwplayer/player.swf
x-flash-version: 11,1,102,55
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; HPNTDF; InfoPath.2; .NET4.0C; .NET4.0E)
Host: wpc.413c.edgecastcdn.net
Connection: Keep-Alive
```

The response is highlighted in blue:

```
HTTP/1.1 200 OK
Accept-Ranges: bytes
Cache-Control: max-age=600
Content-Type: video/mp4
Date: Fri, 30 Mar 2012 23:24:27 GMT
ETag: "4209387519"
Expires: Fri, 30 Mar 2012 23:34:27 GMT
Last-Modified: Thu, 08 Mar 2012 18:52:28 GMT
Server: ECAcc (sjc/4EAE)
X-Cache: HIT
Content-Length: 2090567
```

Below the main pane, the status bar shows "1 client pkt(s), 1.433 server pkt(s), 1 turn(s)". The bottom of the dialog contains various buttons: "Entire conversation (1.184 kB)", "Show and save data as ASCII", "Stream 0", "Find", "Help", "Filter Out This Stream", "Print", "Save as...", "Back", and "Close".

Analyze

Follow

Por defecto, se muestran los datos de ambas direcciones, pero se puede seleccionar la dirección a ver con el botón Entire conversation.

Los datos, se pueden ver en varios formatos

- ASCII
- UTF-8 / UTF-16
- RAW
- HEX DUMP
- YAML

Analyze

[Follow](#)

Podemos cambiar entre streams con el botón **Stream**

Podemos buscar texto, introduciendo el texto en el cuadro de edición y pulsando **Find Next**

Analyze

Laboratorio 1

Abrir el archivo de los laboratorios 3 y 4 de la parte de **filtrado** e intentar resolverlos utilizando esta facilidad

Analyze Expert Info



Analyze

Expert Info

Es un registro de anomalías detectadas por Wireshark, en un archivo de captura

La idea, es tener una mejor visión del comportamiento de red, de esta forma, se detectarán posibles problemas de red, mucho más rápido

Analyze

Expert Info

Severidad

- **Chat**, información flujo de trabajo habitual
- **Note**, aplicación devolución código de error
- **Warning**, código de error inusual
- **Error**, problema grave

Severity	Summary	Group	Protocol	Count
Warning	This frame is a (suspected) out-of-order segment	Sequence	TCP	1
Warning	Connection reset (RST)	Sequence	TCP	5
	17 52382 → 80 [RST, ACK] Seq=666 Ack=9117 Win=0 Len=0	Sequence	TCP	
	54 80 → 52425 [RST, ACK] Seq=265 Ack=175 Win=0 Len=0	Sequence	TCP	
	55 52424 → 80 [RST, ACK] Seq=1074 Ack=1780 Win=0 Len=0	Sequence	TCP	
	65 52448 → 80 [RST, ACK] Seq=666 Ack=507 Win=0 Len=0	Sequence	TCP	
	107 52516 → 80 [RST, ACK] Seq=666 Ack=9060 Win=0 Len=0	Sequence	TCP	
Note	This frame is a (suspected) retransmission	Sequence	TCP	10
Chat	Connection finish (FIN)	Sequence	TCP	5
Chat	GET /minitri.flg HTTP/1.1\r\n	Sequence	HTTP	30
Chat	Connection establish acknowledge (SYN+ACK): server port 80	Sequence	TCP	7
Chat	Connection establish request (SYN): server port 80	Sequence	TCP	23

Analyze

Expert Info

Hay algunos grupos de Expert Info

- **Checksum**, checksum inválido
- **Sequence**, secuencia sospechosa o se han detectado retransmisiones.
- **Response code**, problema con el código de respuesta de la aplicación
- **Request code**, una solicitud de una aplicación
- **Undecoded**, disecto incompleto o los datos, no se pueden decodificar.
- **Reassembled**, problemas con el reensamblado de paquetes
- **Protocol Violation**, violación de las especificaciones del protocolo
- **Malformed**, paquete con un formato incorrecto

Analyze

Expert Info

Summary, nos ofrece un texto con una explicación adicional

Deplegando el árbol del grupo correspondiente, tendremos acceso a los paquetes y haciendo click, wireshark, nos lleva al panel del listado de paquetes con ese paquete seleccionado. Estará coloreado de igual forma.

Podemos crear una columna con la información de experto

Analyze

Laboratorio 2

Descargar el archivo y analizarlo con Expert Info

Telefónica
