

*Telefonica*

# WIRESHARK

Analyze



Analyze

Follow Stream



# Analyze

## Follow

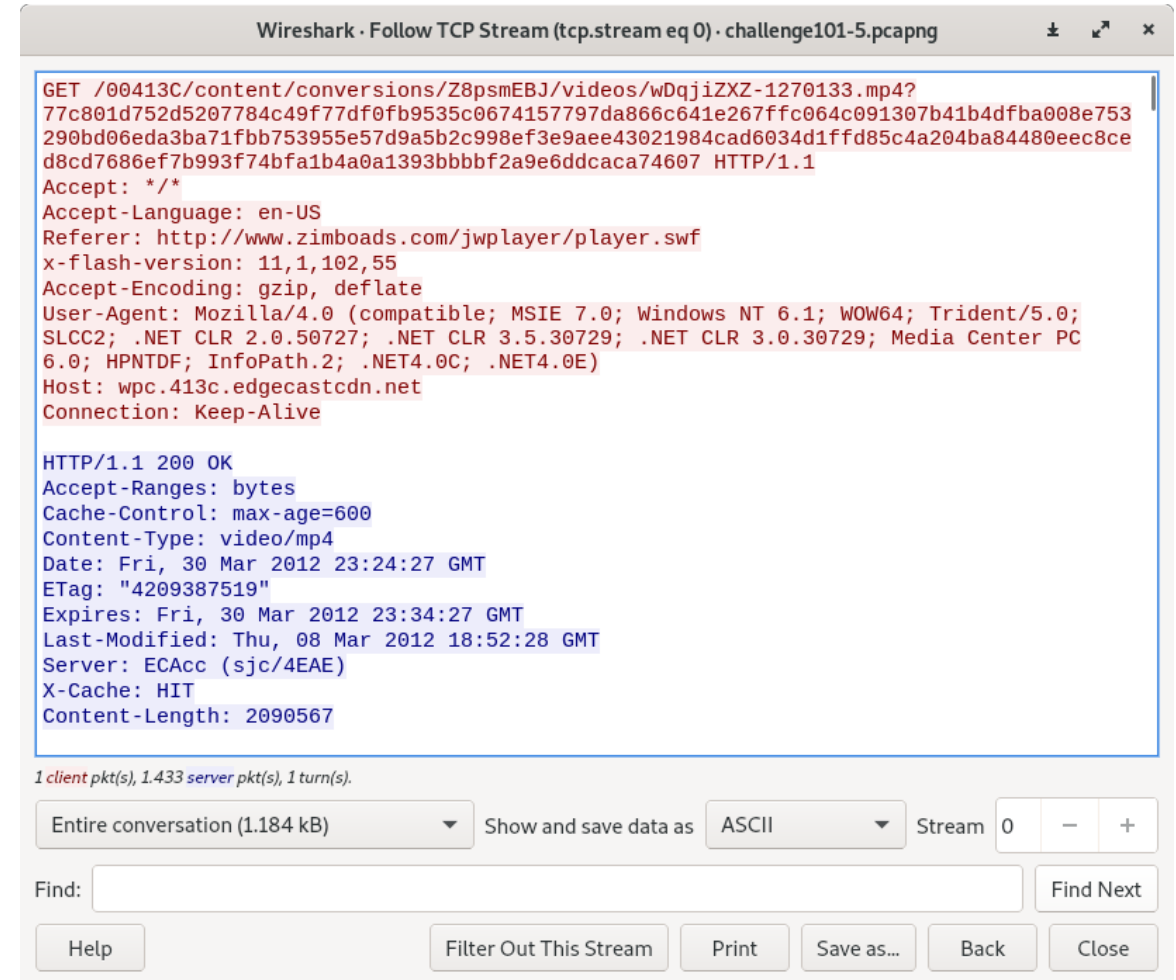
Puede ser muy útil, ver un protocolo en la forma que lo ve la capa de aplicación, puede querer buscar contraseñas, o ver el contenido de una conversación.

- 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 trafico de un sentido estará en rojo y el de sentido contrario, en azul.



# 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

Wireshark · Expert Information · tr-httpdelta.pcapng

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

No display filter set.

☐ Limit to Display Filter ☒ Group by summary Search:  Show... ▼

Help Close

# 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 llevara al panel del listado de paquetes con ese paquete seleccionado. Estará coloreado de igual forma.

Podemos crear una columna con la información de extperto

# Analyze

## Laboratorio 2

Descargar el archivo y analizarlo con Expert Info

*Telefónica*

---