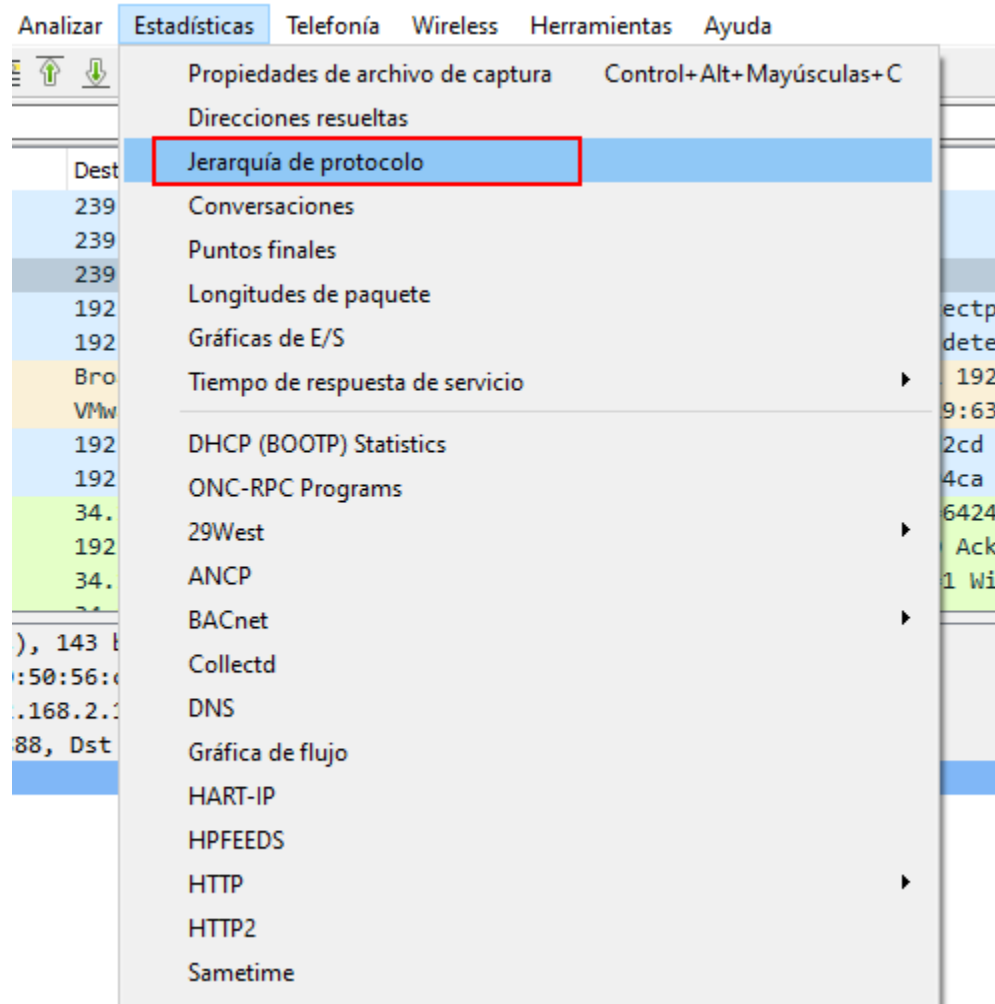


## FTP

Abrimos el fichero pcap con Wireshark. Identificamos que ha sido capturado a nivel de protocolo. Para ello, accedemos a Estadísticas -> Jerarquía de Protocolo.



En la ventana de estadísticas vamos a aplicar un filtro sobre el protocolo DNS.

Protocolo	Porcentaje de paquetes	Paquetes	Porcentaje de bytes	Bytes	Bits/s	End Packets	End I
▼ Frame	100.0	51	100.0	4131	636	0	0
▼ Ethernet	100.0	51	17.3	714	110	0	0
▼ Internet Protocol Version 4	100.0	51	24.7	1020	157	0	0
▼ Transmission Control Protocol	100.0	51	58.0	2397	369	25	816
File Transfer Protocol	100.0	51	10.1	749	115	26	0

Aplicar como filtro	Selected
Prepare as Filter	Not Selected
Buscar	...and Selected
Colorize	...or Selected
Copiar como CSV	...and not Selected
Copiar como YAML	...or not Selected

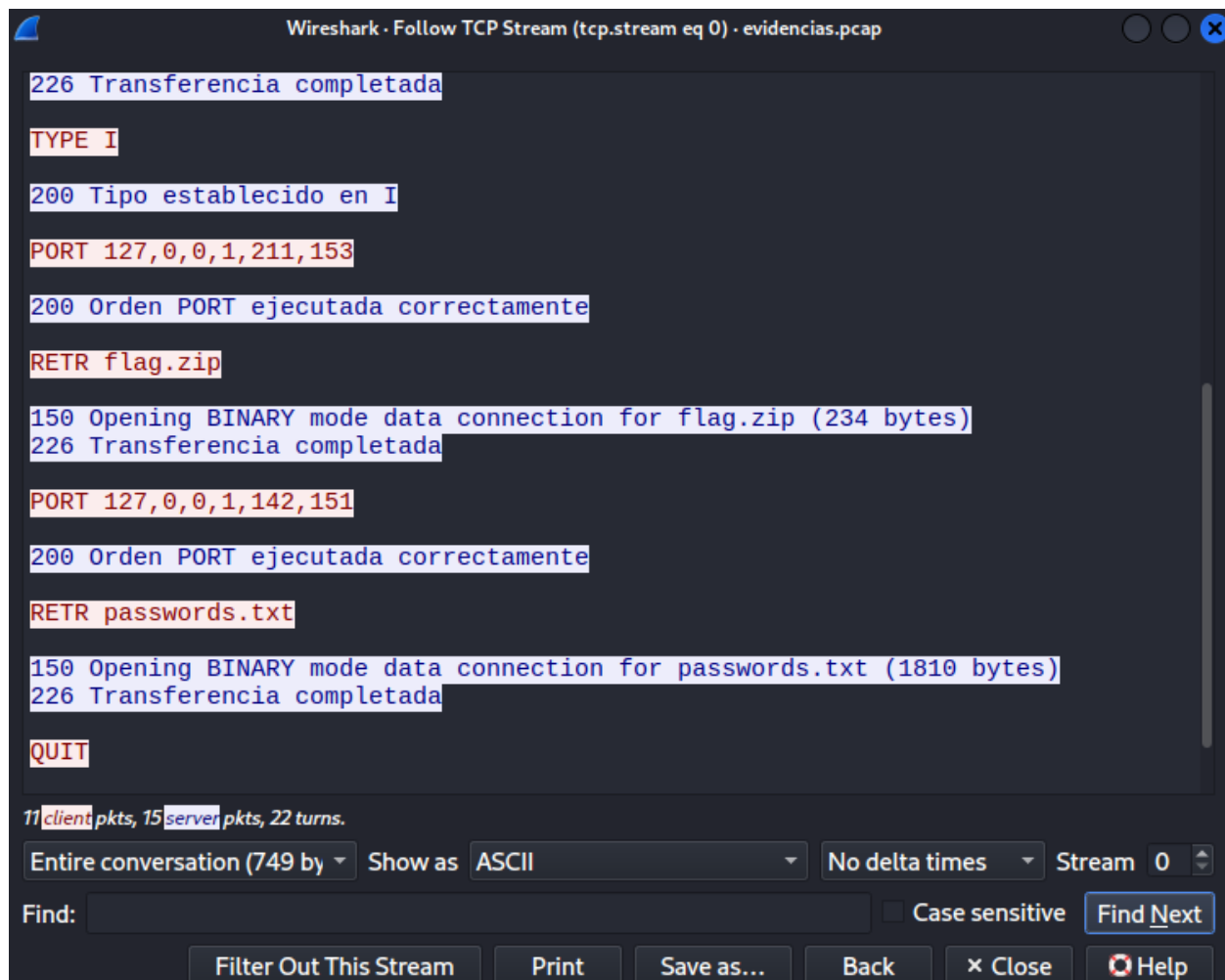
Al tener el filtrado el tráfico procedemos a ver las acciones realizadas en el servidor FTP. Para ello nos colocamos en una de las tramas para hacer clic en botón derecho y “Seguir->Flujo TCP”.

Protocol	Length	Info
FTP	928	127.0.0.1]
FTP		Control+M
FTP		Control+D
FTP		Control+T
FTP		Control+Mayúsculas+T
FTP		Control+Alt+C
FTP		
FTP		Editar nombre resuelto
FTP		
FTP		Aplicar como filtro
FTP		Prepare as Filter
FTP		Filtro de conversión
FTP		Colorear conversación
FTP		SCTP
FTP		Seguir
FTP		Copiar
FTP		Protocol Preferences
FTP		Decode As...
FTP		Mostrar paquete en nueva ventana

Flujo TCP	Control+Alt+Mayúsculas+T
Flujo UDP	Control+Alt+Mayúsculas+U
Flujo TLS	Control+Alt+Mayúsculas+S
Flujo HTTP	Control+Alt+Mayúsculas+H
Flujo HTTP/2	
Flujo QUIC	

Se nos abrirá una ventana con las acciones realizadas. Si nos fijamos se descarga un fichero “flag.zip” y otro passwords.txt.



Hacemos uso de “strings” y “binwalk” para extraer su contenido.

```

$ strings evidencias.pcap
220 Servidor ProFTPD (Debian) [::ffff:127.0.0.1]
  W
USER pepe
  9W
  3X
331 Contrase
a necesaria para pepe
  7X
PASS mipass1234
y230 Usuario pepe conectado
SYST
215 UNIX Type: L8
PORT 127,0,0,1,171,195
200 Orden PORT ejecutada correctamente
LIST
150 Abriendo conexi
n de datos en modo ASCII para file list
-rw-r--r--  1 root    root      40 Jan 21 15:15 flag.txt
-rw-r--r--  1 root    root     234 Jan 21 15:15 flag.zip
-rw-r--r--  1 pepe    pepe    1810 Jan 21 15:14 passwords.txt
226 Transferencia completada
TYPE I
sCY200 Tipo establecido en I
sCYPOR 127,0,0,1,211,153
sCY200 Orden PORT ejecutada correctamente
sCZRETR flag.zip
sCZ150 Opening BINARY mode data connection for flag.zip (234 bytes)
sCZPK
5Rv]p
flag.txtUT
  ux
"F-V^3
5Rv]p
flag.txtUT
  ux
sCZ226 Transferencia completada
sCZ6
  iw
sCZPOR 127,0,0,1,142,151
  >X
200 Orden PORT ejecutada correctamente
  DX
RETR passwords.txt
  4Y
  :Y
  ?Y
150 Opening BINARY mode data connection for passwords.txt (1810 bytes)
danielle
forever
family
jonathan
987654321

```

Descomprimos, y usamos el contenido de password.txt para encontrar la contraseñ

```

$ unzip 1178.zip
Archive: 1178.zip
[1178.zip] flag.txt password: 

```

La contraseña es “karina” y el contenido del fichero flag.txt es el siguiente.

```

$ cat flag.txt
flag{ftp_stream_pcap_with_credentials!}

```