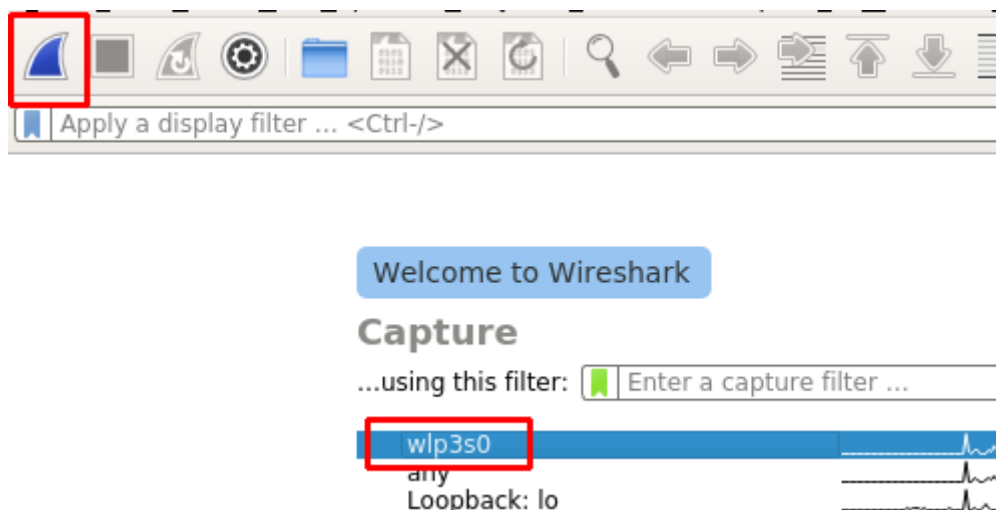


## Entrega Cuestiones Seminario 2

Lo que haremos en esta entrega es documentar con pantallazos, el tráfico de red que se genera al descargar un fichero utilizando el programa aMule, viendo como la descarga se produce desde varias fuentes y como se establece la conexión entre el cliente y el servidor.

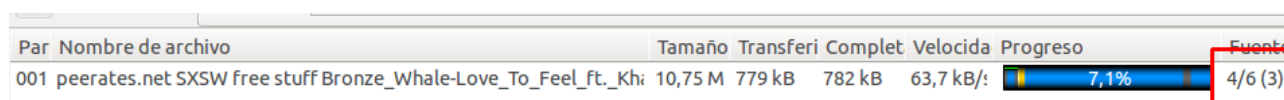
Lo primero que haremos es poner a esnifar el tráfico de la red utilizando WireShark.



Seguidamente, conectamos aMule a un servidor que esté disponible.



Ahora procedemos a buscar un fichero para descargar en el apartado de 'Buscar' de aMule. Seleccionamos uno que tenga varias fuentes de descarga y comenzamos con esta.



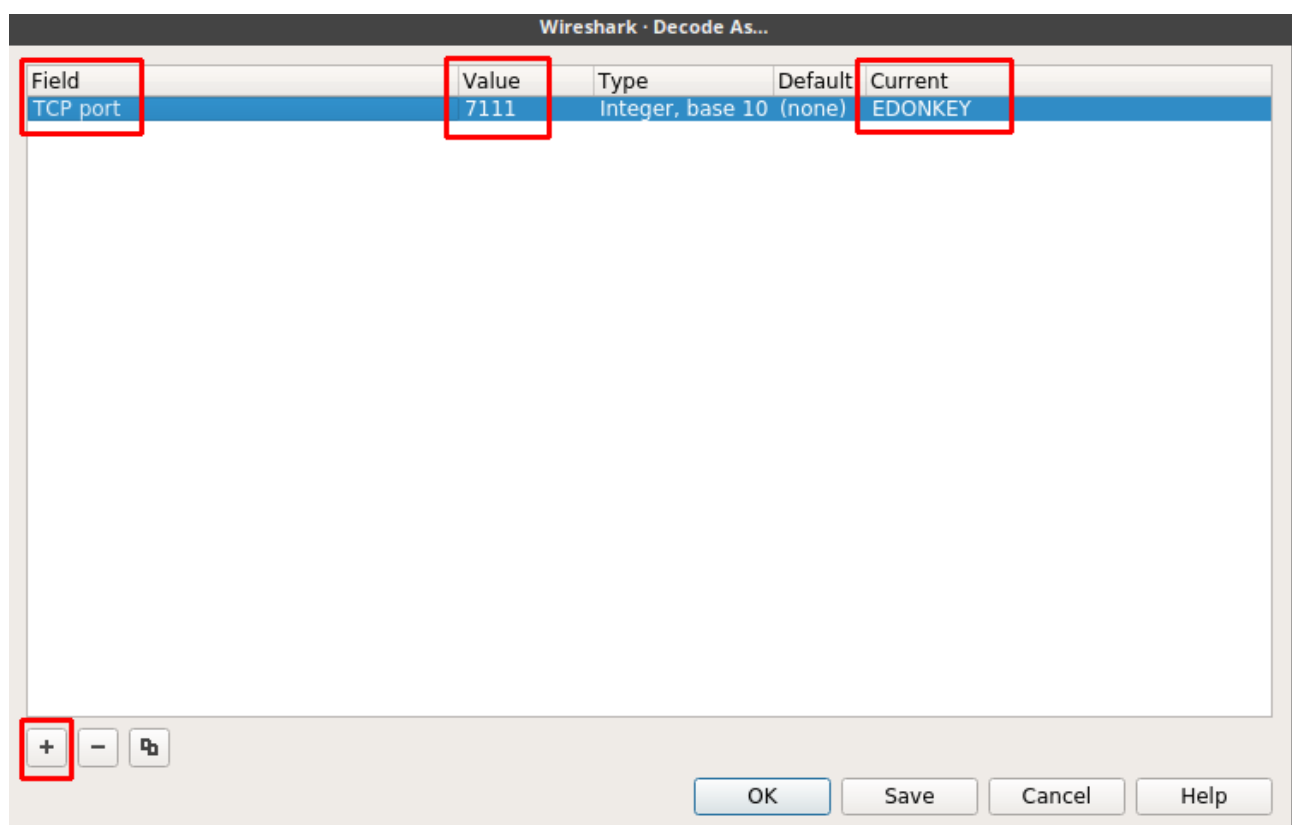
Si nos fijamos en la imagen anterior veremos que el fichero esta siendo descargado de 4 fuentes distintas.

Una vez finalice la descarga volvemos a Wireshark para analizar que es lo que ha sucedido. Lo primero que debemos hacer es detener Wireshark para que deje de esnifar el tráfico y así analizar este con más tranquilidad.

Una vez hecho esto debemos decirle a Wireshark que los paquetes provenientes del **puerto 7111** (puerto que utilizaba el servidor al que nos hemos conectado en aMule) los interprete como eDonkey.

```
2017-10-04 19:57:34: Registro ha sido borrado
2017-10-04 19:57:42: Conectando a PeerBooter (212.83.184.152 - 212.83.184.152:7111)
2017-10-04 19:57:42: Conectado a PeerBooter (212.83.184.152:7111)
2017-10-04 19:57:52: ADVERTENCIA: PeerBooter (212.83.184.152:7111) - NG : You have a lo
2017-10-04 19:57:52: Conexión establecida en: PeerBooter
2017-10-04 19:57:52: Conectado a PeerBooter con IDBaja
2017-10-04 19:57:52: El nuevo ID-Cliente es 16748106
2017-10-04 19:57:52: ALERTA: ¡Has recibido ID-Baja!
```

Para esto vamos a **Analyze > Decode as** y añadimos lo comentado anteriormente de la siguiente manera.



Una vez hecho esto filtramos los paquetes buscando por eDonkey y obtendremos todos los paquetes generados de la descarga.

No.	Time	Source	Destination	Protocol	Length	Info
5	4.259269651	172.20.55.191	212.83.184.152	eDonk...	148	eDonkey TCP: Hello
16	13.536067167	212.83.184.152	172.20.55.191	eDonk...	157	eDonkey TCP: Server Message
18	13.610931927	212.83.184.152	172.20.55.191	eDonk...	290	eDonkey TCP: ID Change, eDonkey TCP: Server Status, eMule Compressed TCP: Server Message
38	41.051670586	172.20.55.191	212.83.184.152	eDonk...	79	eDonkey TCP: Search Files
40	41.127198714	212.83.184.152	172.20.55.191	eDonk...	736	eMule Compressed TCP: Search File Results
90	48.900340960	172.20.55.191	212.83.184.152	eDonk...	79	eDonkey TCP: Search Files
95	49.180554228	212.83.184.152	172.20.55.191	eDonk...	588	eMule Compressed TCP: Search File Results
447	125.6554579...	172.20.55.191	212.83.184.152	eDonk...	92	eDonkey TCP: Get Sources
454	125.7318462...	212.83.184.152	172.20.55.191	eDonk...	125	eDonkey TCP: Found Sources
6672	200.9579113...	172.20.55.191	212.83.184.152	eDonk...	182	eDonkey TCP: Offer Files

En la imagen anterior si nos fijamos en el recuadro marcado con 1, podemos ver que son los paquetes de que la conexión entre cliente y servidor se ha establecido correctamente, enviando el mensaje de ‘Hello’ desde el cliente al servidor y obteniendo la respuesta de este hacia el cliente.

Si nos fijamos en el recuadro marcado con 2, veremos como se ha ido desarrollando el proceso de descarga paso a paso:

1. Iniciar búsqueda de ficheros
2. Resultados encontrados de la búsqueda
3. Buscando fuentes
4. Fuentes encontradas
5. Fichero descargado

Y por ultimo si nos fijamos en el paquete cuya info es “Found Sources” podremos ver las distintas fuentes desde las cuales se podía descargar nuestro fichero.

No.	Time	Source	Destination	Protocol	Length	Info
447	125.6554579...	172.20.55.191	212.83.184.152	eDonk...	92	eDonkey TCP: Get Sources
454	125.7318462...	212.83.184.152	172.20.55.191	eDonk...	125	eDonkey TCP: Found Sources
6672	200.9579113...	172.20.55.191	212.83.184.152	eDonk...	182	eDonkey TCP: Offer Files

Internet Protocol Version 4, Src: 212.83.184.152, Dst: 172.20.55.191	
Transmission Control Protocol, Src Port: 7111, Dst Port: 55764, Seq: 8617, Ack: 135, Len: 59	
eDonkey Protocol	
eDonkey Message	
Protocol: eDonkey (0xe3)	
Message Length: 54	
Message Type: Found Sources (0x42)	
File Hash: a07e1269ba344effa2a7a88ab9b69402	
Address List Size: 6	
<div> <div>Address[1/6]</div> <div>IP: 109.3.146.210</div> <div>Port: 19634</div> </div> <div> <div>Address[2/6]</div> <div>IP: 212.83.155.28</div> <div>Port: 20673</div> </div> <div> <div>Address[3/6]</div> <div>IP: 163.172.50.154</div> <div>Port: 8116</div> </div> <div> <div>Address[4/6]</div> <div>IP: 212.83.184.152</div> <div>Port: 16307</div> </div> <div> <div>Address[5/6]</div> <div>IP: 62.210.28.77</div> <div>Port: 15711</div> </div> <div> <div>Address[6/6]</div> <div>IP: 212.83.155.4</div> <div>Port: 20673</div> </div>	