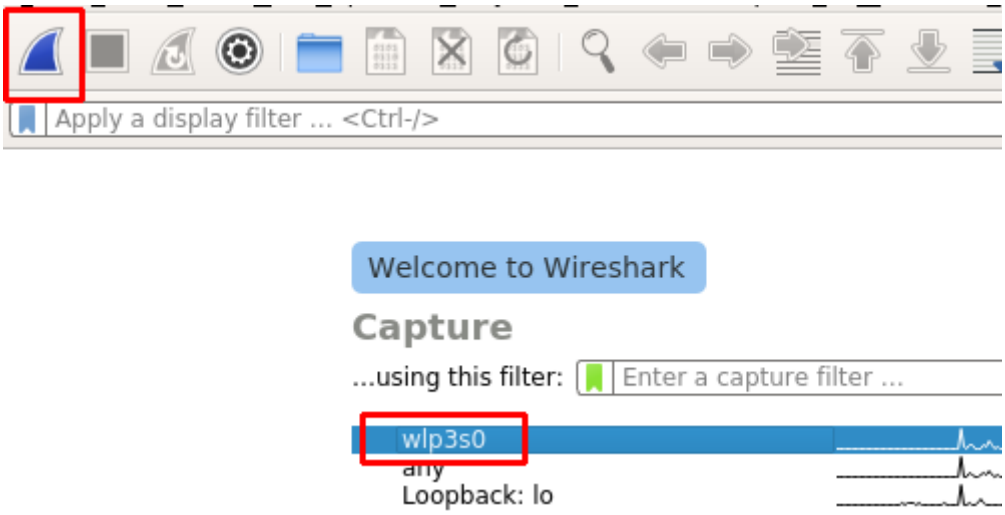
Entrega Cuestiones Seminario 2

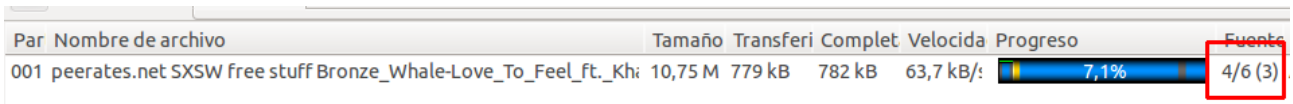
Lo que haremos en esta entrega es documentar con pantallazos, el tráfico de red que se genera al descargar un fichero utilizando el programa aMule, viendo como la descarga se produce desde varias fuentes y como se establece la conexión entre el cliente y el servidor.

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



Seguidamente, conectamos aMule a un servidor que esté disponible.

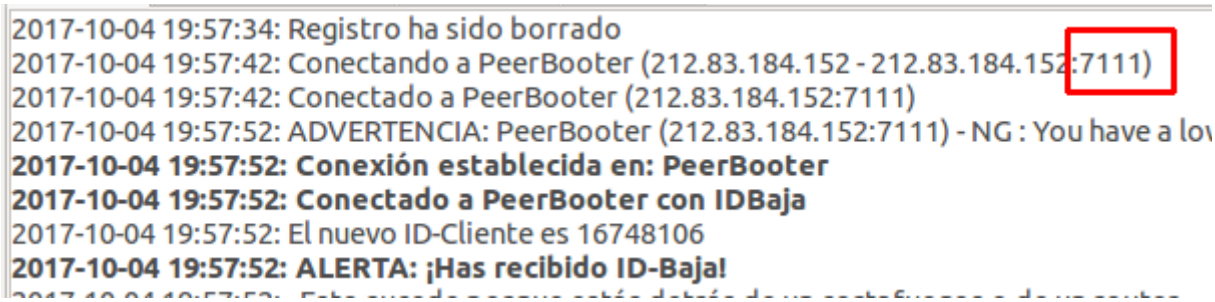
Ahora procedemos a buscar un fichero para descargar en el apartado de *'Buscar'* de aMule. Seleccionamos uno que tenga varias fuentes de descarga y comenzamos con esta.



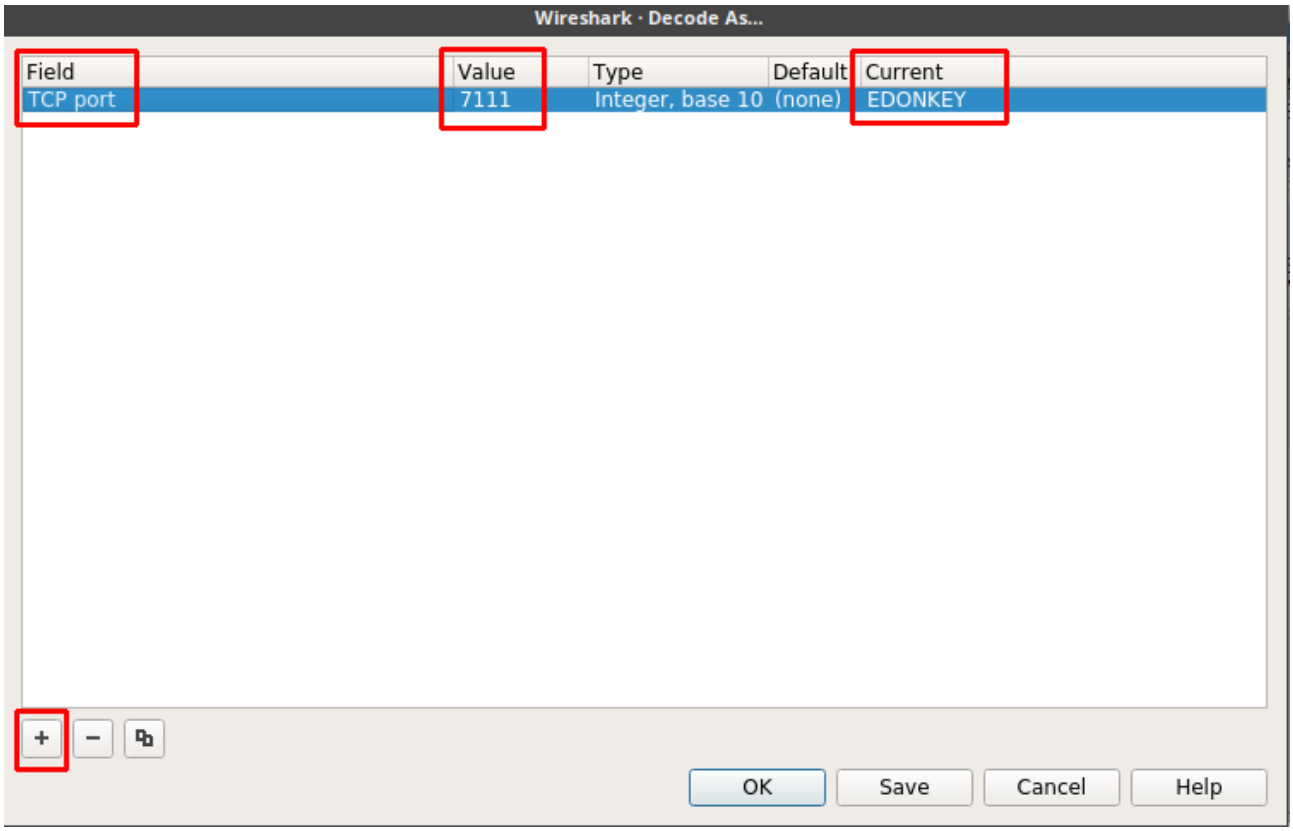
Si nos fijamos en la imagen anterior veremos que el fichero esta siendo descargado de 4 fuentes distintas.

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.

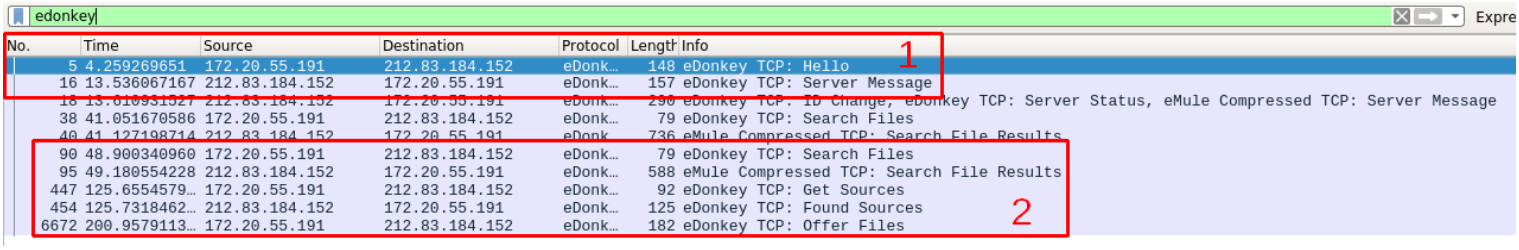
Una vez hecho esto debemos decirle a WireShark que los paquetes provenientes del **puerto 7111** (puerto que utilizaba el servidor al que nos hemos conectado en aMule) los interprete como eDonkey.



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.



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.