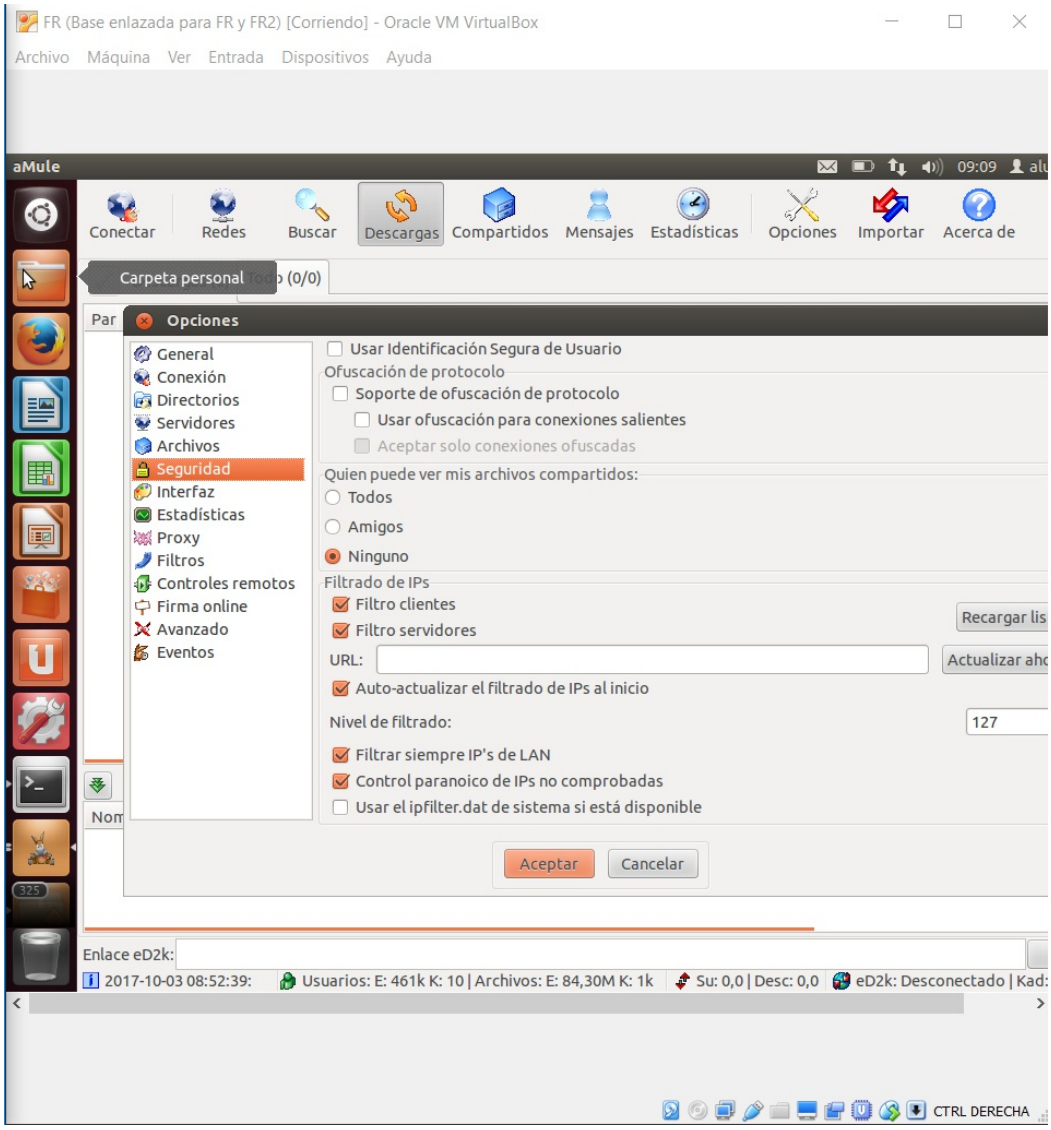
Seminario 2

En este seminario se nos pide que realicemos una captura de tráfico de paquetes mientras realizamos una descarga de la imagen de ubuntu mediante el programa EMule.

1º Configuración de EMule.

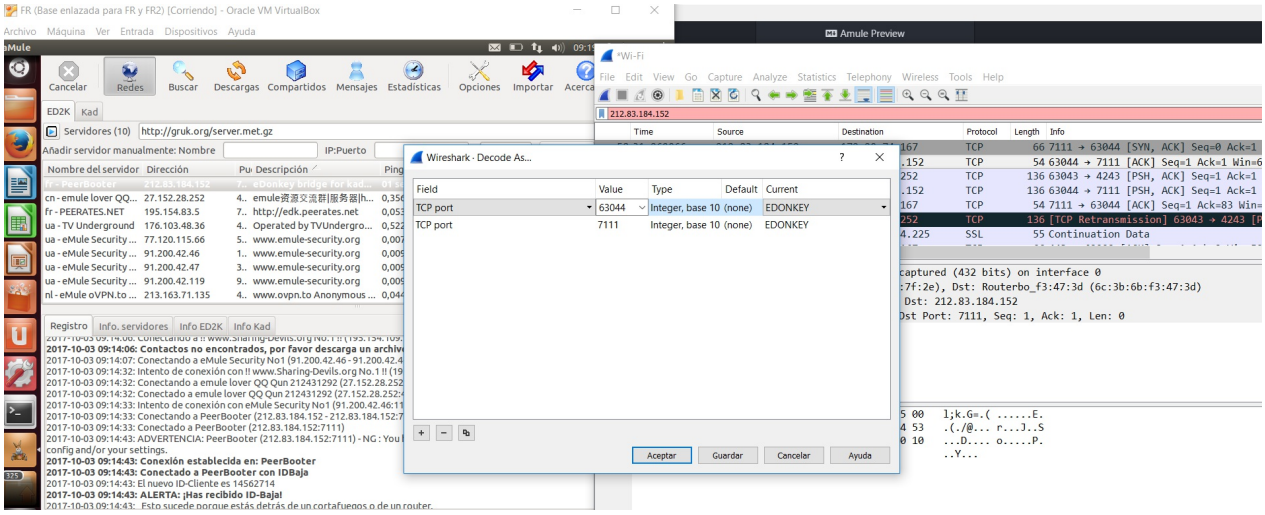
Esta configuración la realizamos en la misma clase, de mano del profesor.
Abrimos la pestaña "Opciones"-->"Seguridad" y desmarcamos las opciones:
·Usar identificación Segura de Usuario.
·Usar ofuscación para conexiones salientes.
·Soporte de ofucación de protocolo.

Esto lo hacemos, como bien explicamos en clase, para que no haya lugar a confusión a la hora de analizar los paquetes. Ya que si no podríamos llegar a confundirnos con esos paquetes "falsos" que envía para camuflar la conexión.



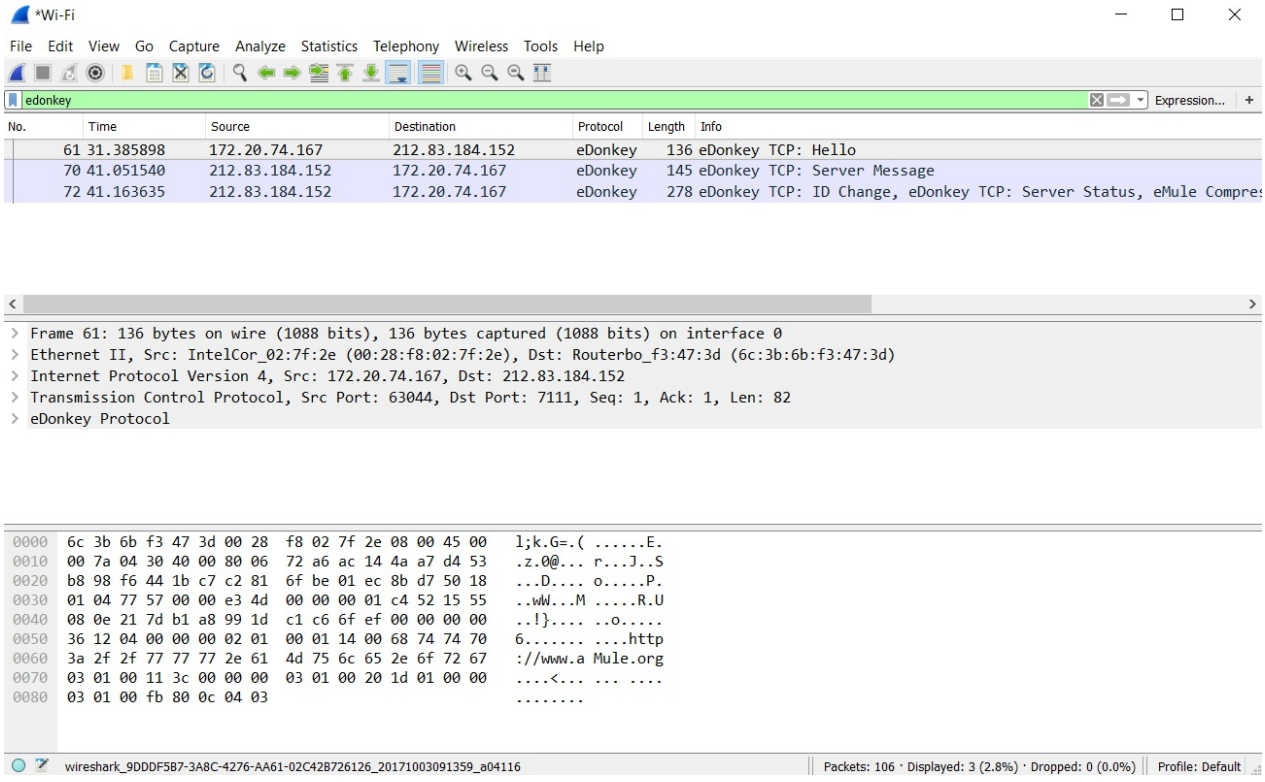
2º Inicializar el programa y comprobar conexiones

Acabamos de iniciar Wireshark, lo hemos puesto en marcha. Hemos puesto a buscar dirección de conexión, lo ha conseguido y este es el resultado.



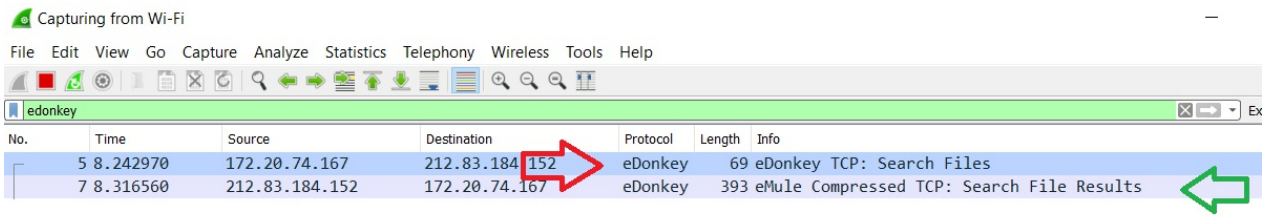
Hemos comprobado que hoy nos ha conectado a una IP(212.83.184.152) por y escucha en dos puertos el 63044 y el 7111, por defecto Wireshark es capaz de reconocer los paquetes EDonkey, pero estos están camuflados para evitar que las ISP´s hagan de las suyas. Por tanto una vez analizados y sabiendo cuales son las IP´s y los puertos de conexión, podemos decirle a nuestro Wireshark cuáles son los paquetes que debe reconocer como EDonkey.

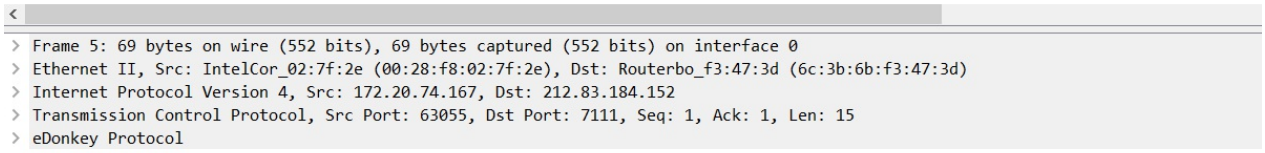
Realizamos pues, la busqueda de paquetes EDonkey y el resultado es:

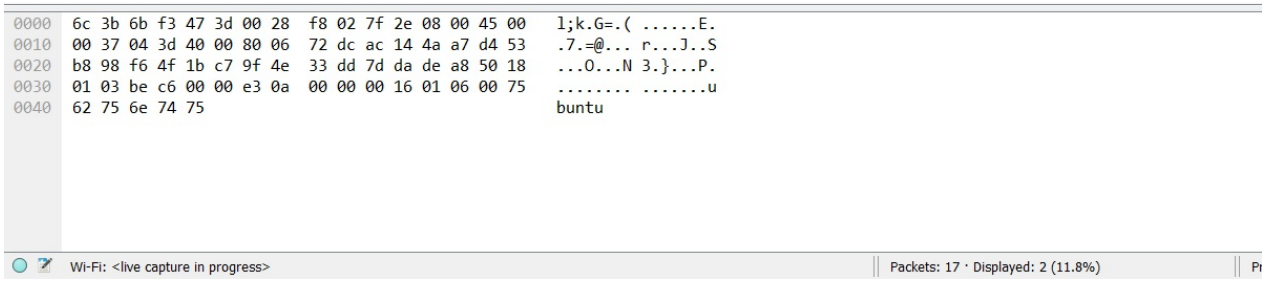


En esta foto podemos comprobar los mensajes de conexión:
1º Hello: en el que nuestra máquina "saluda" a la dirección de destino.
2º La respuesta: en la que el "servidor" nos responde dandonos una ID para nuestra conexión, y nos avisa de que abramos ciertos puertos o nuestra ID sera baja.

A continuación, hemos buscado una imagen ubuntu y estas son la petición de busqueda(ROJO) y la respuesta de: "archivo encontrado"(VERDE).

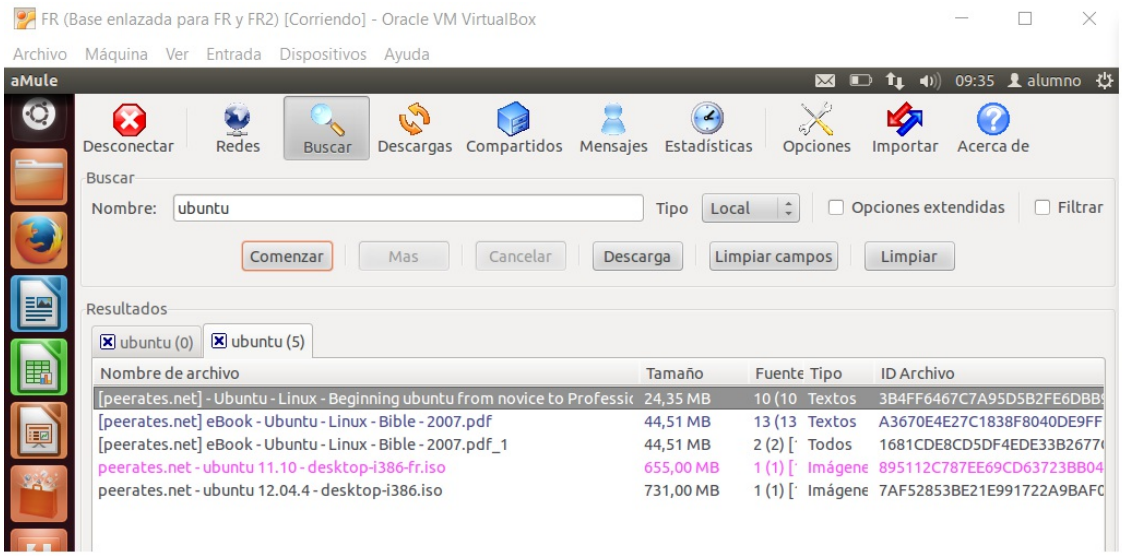




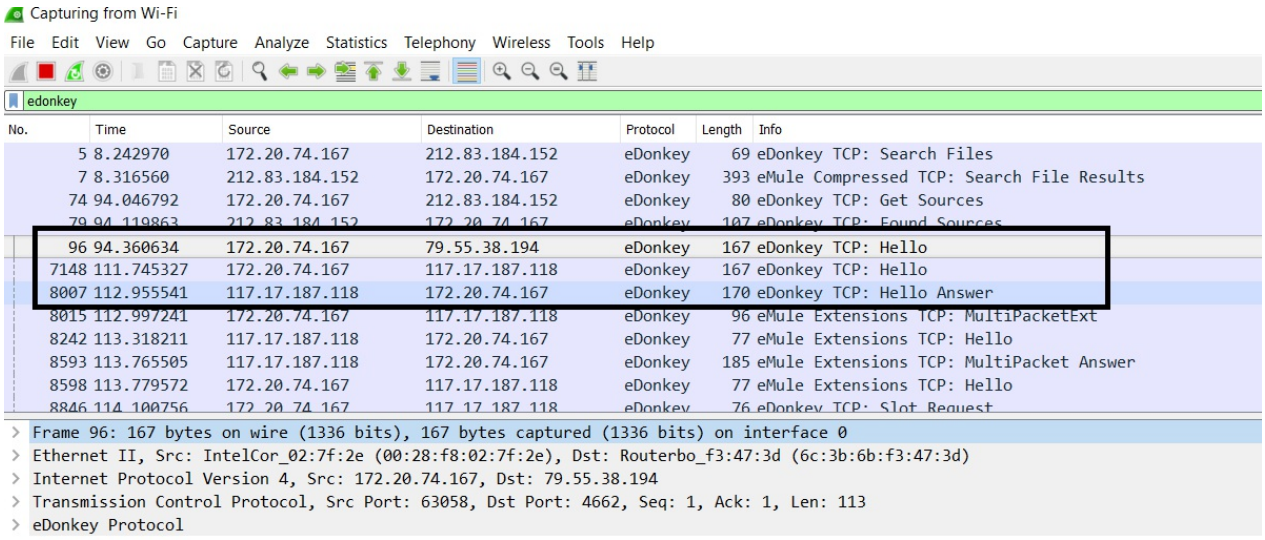


3º Conexión establecida y descarga

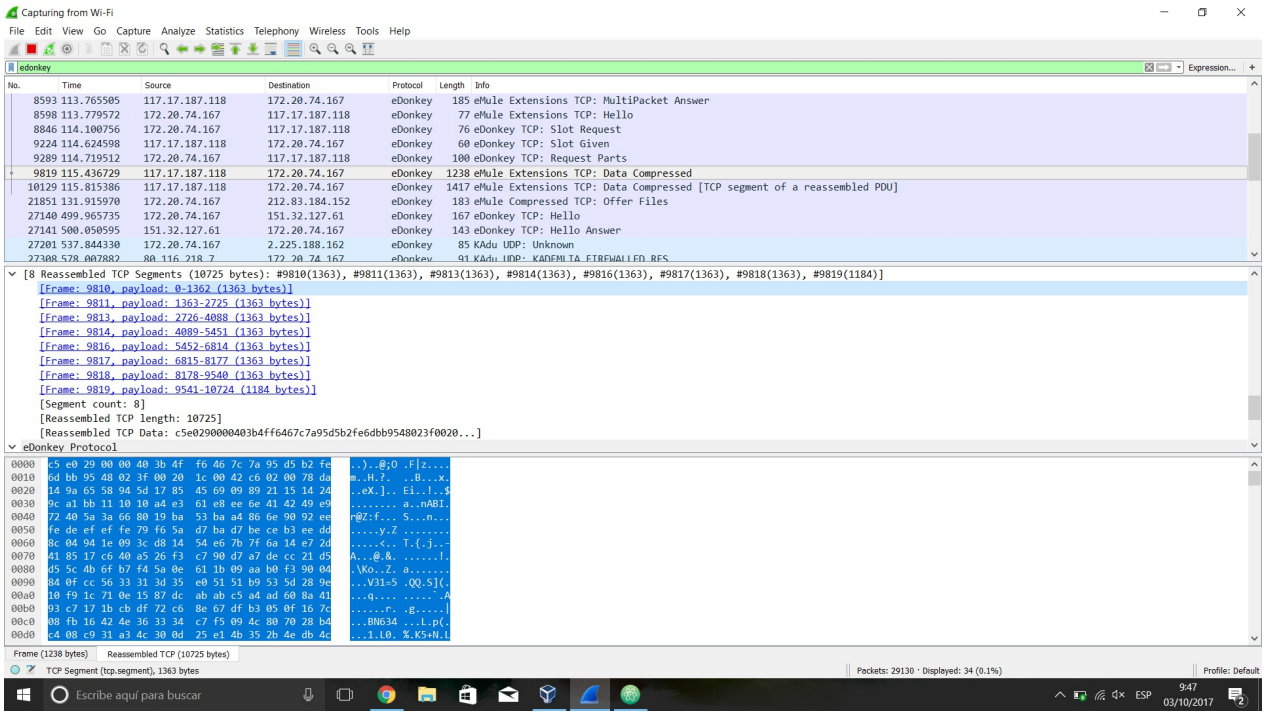
Vamos a descargar la imagen ubuntu y para ello hemos escogido una con varias fuentes para comprobar que ocurre.



Lo primero que comprobamos gracias a Wireshark es que hacemos dos ping de Hello a 2 direcciones distintas: 79.55.38.194 y 117.17.187.118.
Aunque solo una de las dos nos responde: 117.17.187.118



En esta foto se muestra como la dirección 117.17.187.118 nos está dando los paquetes de la imagen solicitada.



A su vez más abajo comprobamos como se vuelve a repetir el proceso de Hello y Hello answ er a otra dirección.

Así hemos podido ver como se realizan las conexiones a diferentes IP's a la hora de buscar un recurso que tienen varias fuentes y como se realizan las peticiones de este

Aclaración de algunos paquetes y protocolo

En algunas imagenes podemos apreciar mensajes que en la info muestran: "Request Parts" esos son los mensajes en los que le pedimos a esta IP los paquetes.
Una vez descargado del todo mandamos un último aviso: Slot Release, dando una especie de "Adios y gracias amijo".

Una vez explicada la transferencia de paquetes, diré que todo se ha realizado por TCP, por la sencilla razón de que es una Imagen ISO, un archivo que neceista tener la consistencia al 100%, hasta el último bit de información y datos.

node.dat

Este archivo es una especia de libro de direcciones de los clientes. Y es necesario para tener conexión a dichos clientes. Es decir, si no tuvieramos este archivo o no estuviera conectado, no encontrariamos direcciones de las que descargar lo que buscamos.

Realizado por: J.Javier Galera Garrido