Universidad De Granada

Grado ingeniería informática (2017 – 2018)

Fundamentos De Redes

Seminario 2: Wireshark + Edonkey

Trabajo realizado por Antonio Miguel Morillo Chica

---

1. Configurando emule.

Antes de nada deberemos configurar el servicio emule de nustra máquina. Para ello vamos a Opciones > Seguridad y desmarcamos las opcciones:

- Usar identificación Segura de Usuario.
- Usar ofuscación para conexiones salientes.
- Soporte de ofucación de protocolo.

2. Emule (edonkey)

El servicio emule que se usa para el intercambio de archivos con sistema P2P utilizando el protocolo eDonkey 2000 y la red Kad, publicado como software libre.

2.1 Usando Wireshark.

Lo primero que deberemos hacer es abrir wireshark con sudo para poder acceder a las redes y capturar paquetes.

```
sudo wireshark
```

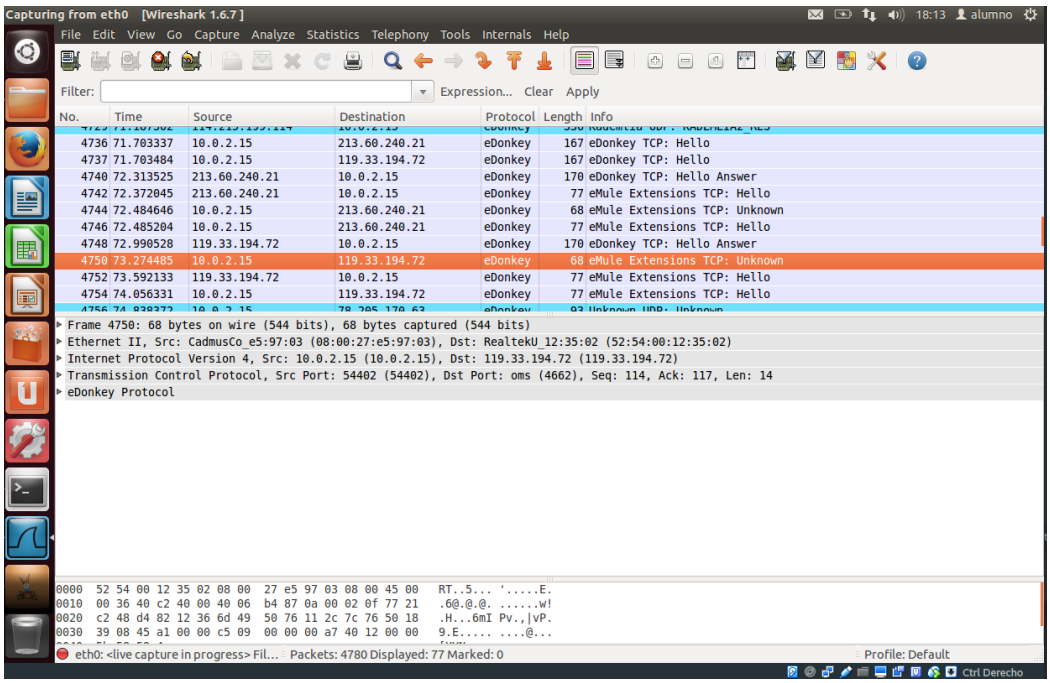
Tras esto abrimos emule y buscamos un archivo a descargar. El que sea, en nuestro caso en la práctica buscamos una imagen del sistema ubuntu. Mientras tanto estaremos cazando el trafico de paquetes. Una vez entrado descargar.

Tras unos segundos cortamos la descarga, cerramos amule y cortamos la lectura de paquetes.

2.2. Analizando los paquetes.

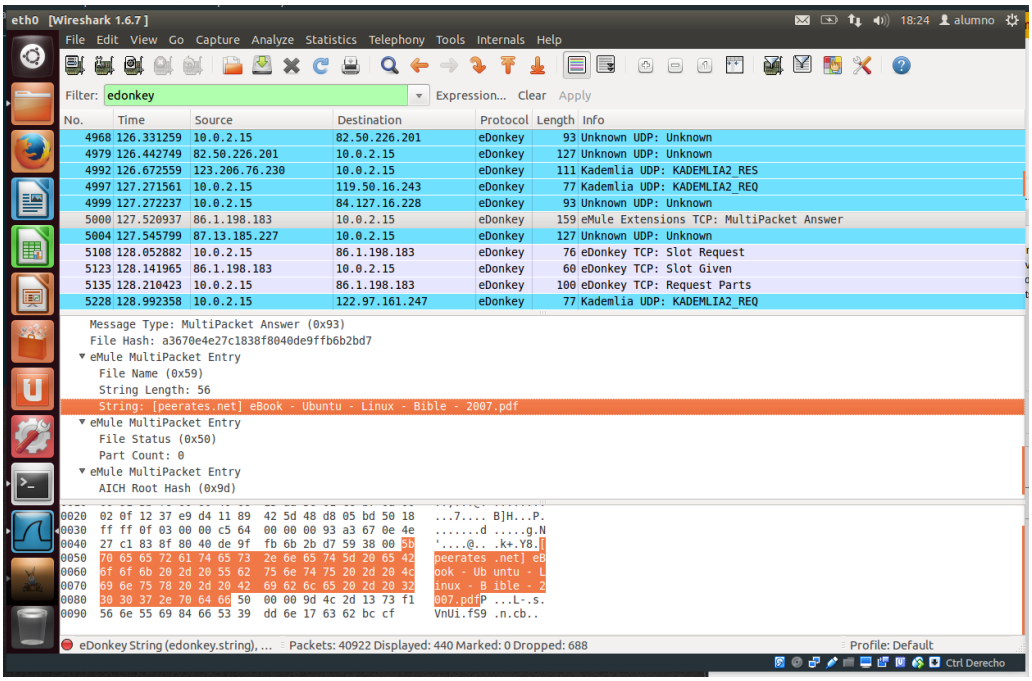
Para analiar los paquetes edonkey y buscarlos unicamente deberemos de escribir en la barra superior de wirehark el nombre del protocolo “edonkey”. Tras esto nos saldrán todos los paquetes enviados con este protocolo.

En la imagen siguiente podemos ver como el protocolo se inicia ante de haber enviado nada ni haber buscado, como podemos ver en la descripción nos dice hola todo el rato y la respuesta de hola.



Ahora vamos a ver el paquete que tiene la recepción de lo que hemos buscado para ellos lo más sencillo es buscar un string. En mi caso no me he bajado la imagen de ubunto sino un archivo pdf que tiene que ver con con el sistema.

Para buscar los string deberemos de ir a Edit > Find Packet y tras esto buscamos por string y en packets details o packets list. Como podemos ver el paquete encontrado es el comienzo de la descarga de este archivo:



2.3. Red KAD.

KAD es un protocolo que está pensado para ser desplegado sobre redes P2P basado en una red estructurada y que usa como método de ordenamiento y búsqueda las DHT (Distributed Hash Tables).

Es una implementación del protocolo Kademlia, el cual aporta la base teórica al protocolo y por tanto, hay muchas partes de Kademlia que KAD hereda y reutiliza. KAD desarrolla la base en forma práctica siguiendo las pautas genéricas de Kademlia y las especificaciones propias del mismo KAD.

El archivo nodes.dat contine pues, la tabla de conexión de la descarga, de que ip se está descargando el archivo. Si no tuviesemos este archivo sería imposible descargar ya que no sabríamos de donde.