Redes KAD

Seminario Fundamentos de Redes

Enrique Moreno Carmona
Javier Martín Gómez

Índice

1. Objetivos

El objetivo de este seminario es aprender a conectarnos y descargar archivos estando conectados a la red Kad en la aplicación aMule, así como analizar los datos de los paquetes en Wireshark.

2. Introducción

La red KAD es un protocolo distribuido en tablas Hash basado en Kademlia, hay muchas partes que la red KAD hereda y reutiliza. [1]

La red KAD está pensada para ser usada en redes P2P. Al ser una red P2P descentralizada, no se requieren de servidores y desaparece el cuello de botella que se crea por la necesidad de estos. Se conecta directamente a un cliente (con una dirección ip y puerto conocido) que sea compatible con el protocolo Kademlia [2].

Solo 4 grandes clientes admiten la red Kad: aMule, eMule, MLDonkey y Lphant. Sin embargo, comprenden más del 80% de la base de usuarios.

Es compatible con la red de intercambio de archivos eDonkey al proporcionar indexación de palabras clave [1]. eDonkey es una red basada en servidor donde los clientes realizan el archivo de búsquedas. Por otro lado, aMule y eMule son los dos clientes más populares que se pueden conectar a eDonkey y la red de Kad [3].
Además eDonkey usa el hiperenlace “eD2K” para localizar archivos dentro de su red P2P [4].

3. Funcionamiento

Como anteriormente se dijo, no se necesita de un servidor para hacer uso de la red, sino que se conecta directamente con el cliente sabiendo su ip y puerto.

Cada PC actúa como un pequeño servidor y un cliente y se le da la responsabilidad de ciertas palabras clave o fuentes [2]. Para esto, cada PC se transforma en un nodo de la red y comunica con sus vecinos para tener acceso a todas las informaciones de la red [5].

Una de las cosas que KAD hereda de Kademlia es el espacio de objetos virtual y el ordenamiento basado en árbol binario.

La red Kad esencialmente funciona por intercambios efectuados a través del puerto UDP. El puerto TCP sirve para las conexiones que vienen de otros clientes y al intercambio de fuentes entre clientes.[2]

Los paquetes UDP que usa KAD tiene el siguiente formato:

- ID: especifica el identificador del protocolo específico
- OPCODE: determina el código de la operación
- PAYLOAD: datos útiles con tamaño determinado por el datagrama de UDP

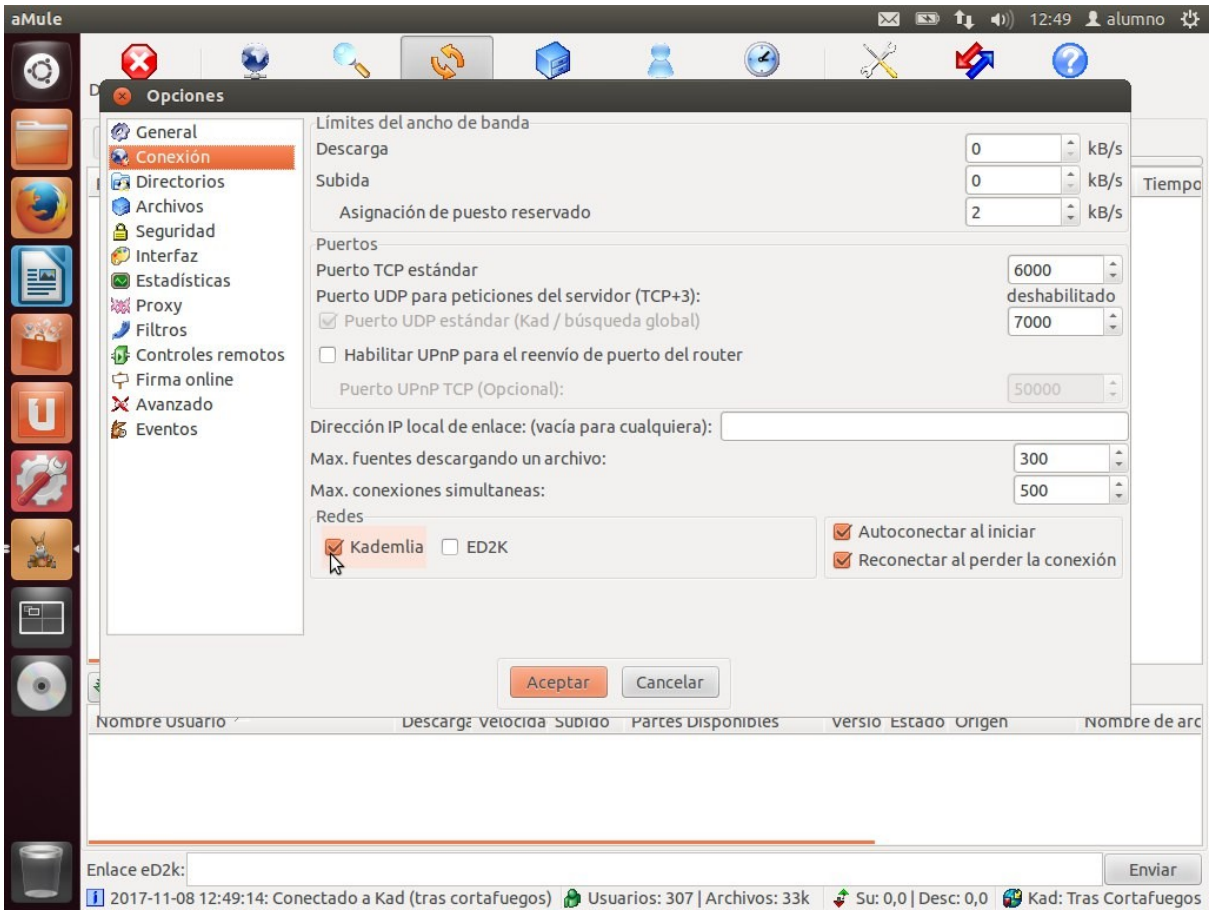
Los intercambios de informaciones y de archivos hechos por eMule o aMule pasan por puertos del PC y son regidos por los protocolos TCP/IP.

Los puertos por defecto son TCP 4661 o 4662 y UDP 4665 o 4672, son a veces vigilados y el flujo que está en tránsito por ellos puede ser filtrado o bloqueado, por ello se aconseja reemplazarlos por puertos entre 5000 y 65535.[2]

4. Demo

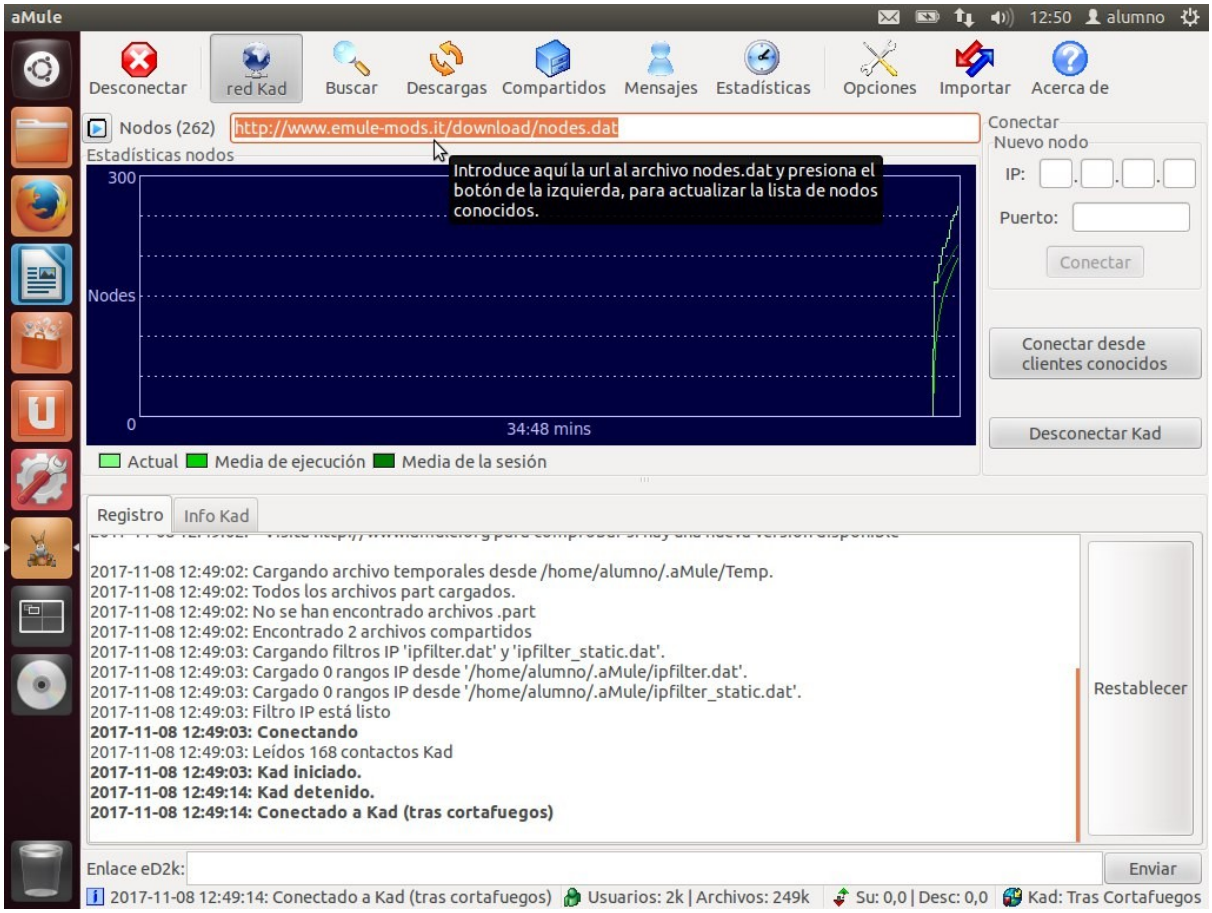
4.1 Conectarse a la red Kad en aMule

1. Iniciar aMule
2. Ir a opciones > Conexión > Redes> Activar casilla Kademlia



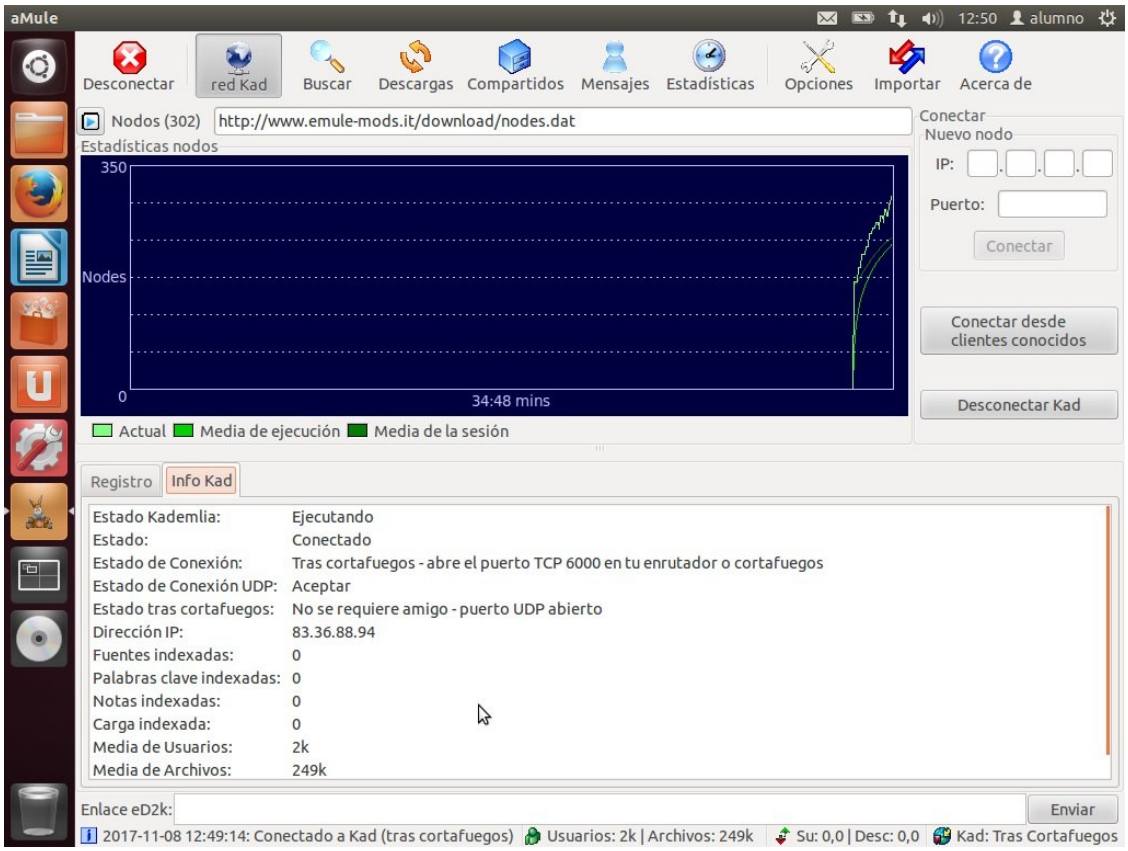
(pulsamos la casilla que está en el cursor para activar la red Kad)

3. Ir a la pestaña de Redes e ir a “Kad”.
4. En la casilla “nodos” poner un enlace a una descarga de archivo tipo “nodes.dat”. En nuestro ejemplo usamos: www.emule-mods.it/download/nodes.dat



5. Pulsamos enter y si no hay problemas se conectará. En caso de que haya habría que probar con otros enlaces de descarga del archivo nodes.dat.

6. Es posible que haya problemas con el cortafuegos así que habría que abrir los puertos que nos indican en la pestaña “Info Kad”.

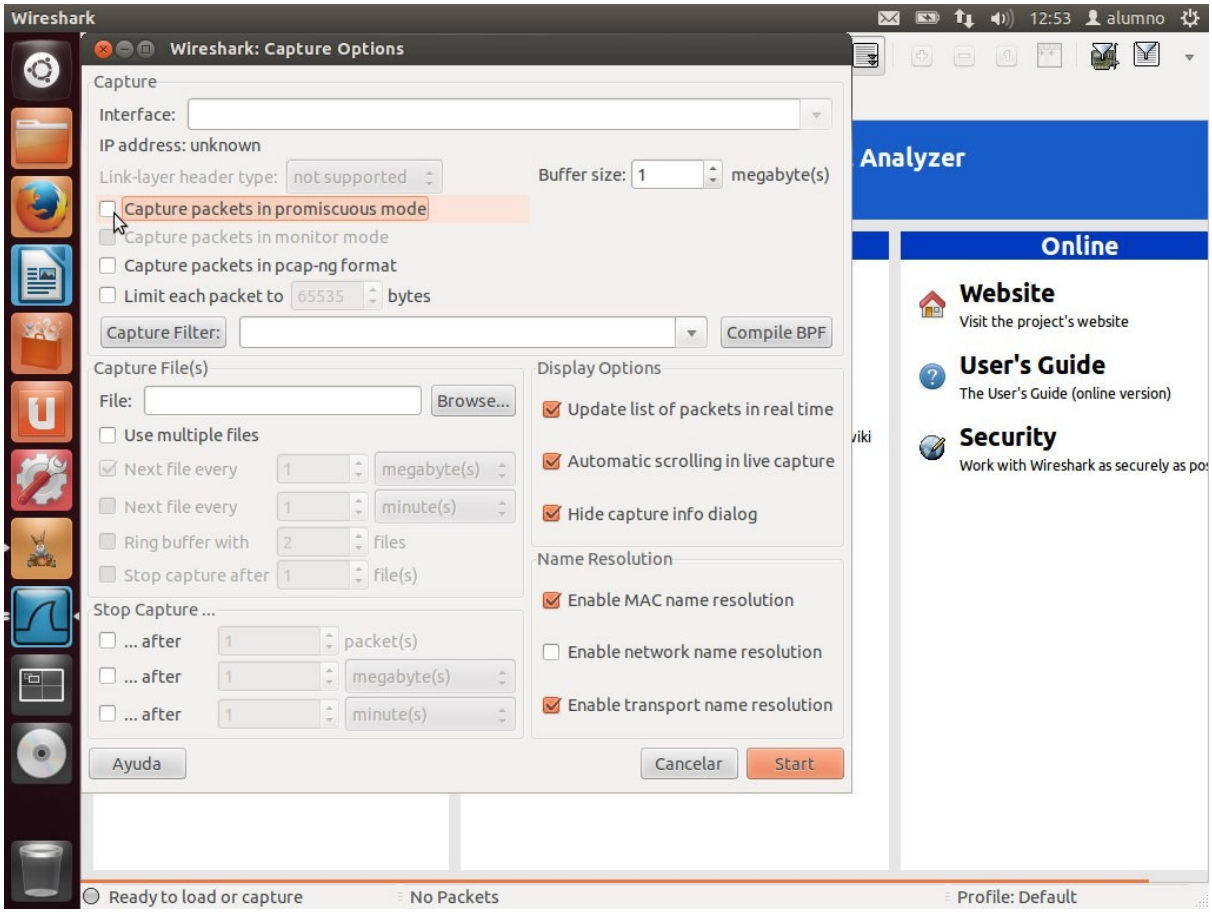


(en este caso tenemos que abrir el puerto 6000).

7. Los puertos se abren en la terminal con el comando “sudo ufw allow NumerodelPuerto” y para ver el estado de los puertos usamos el comando “netstat -plut” y/o “ufw status”.

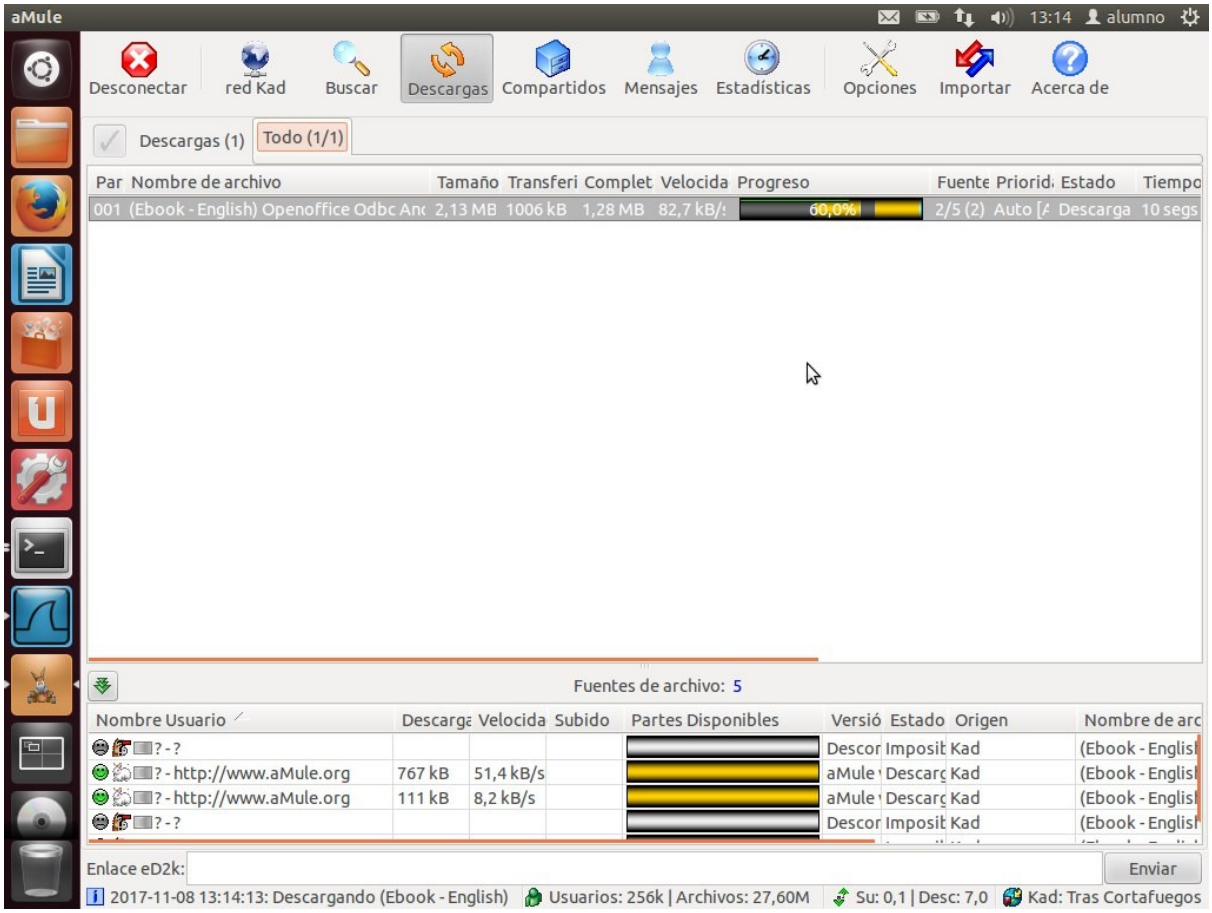
4.2 Capturar paquetes con Wireshark

8. Iniciamos wireshark desde la terminal con “sudo wireshark”.
9. Desactivamos el modo Promiscuo, vamos a Capture > options > desactivar la casilla “Capture packets in promiscuous mode > pulsamos start.



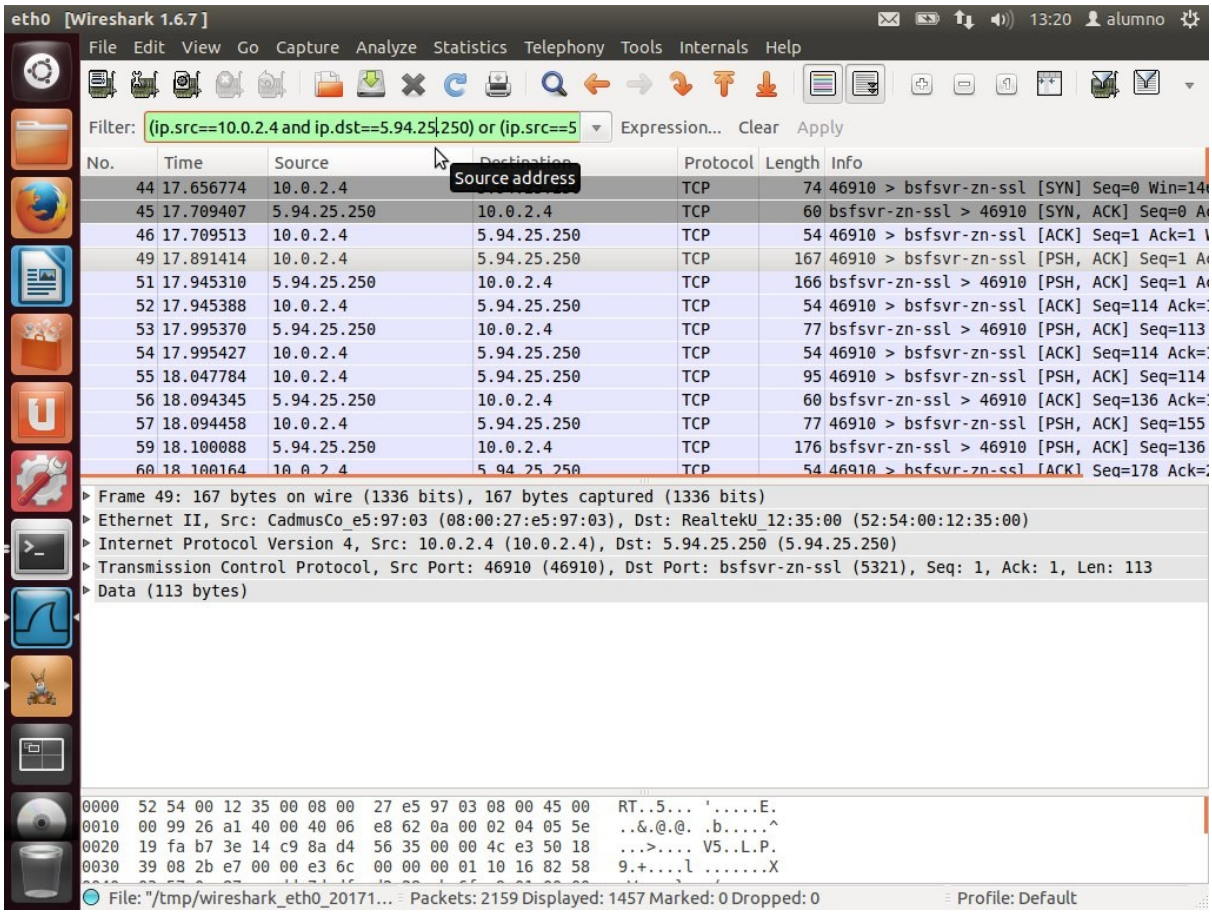
(desactivar la casilla del modo promiscuo, donde está el cursor)

10. En aMule vamos a la pestaña de descargas y descargamos cualquier cosa, en nuestro caso es un Ebook de linux que pesa muy poco para realizar la descarga rápido.



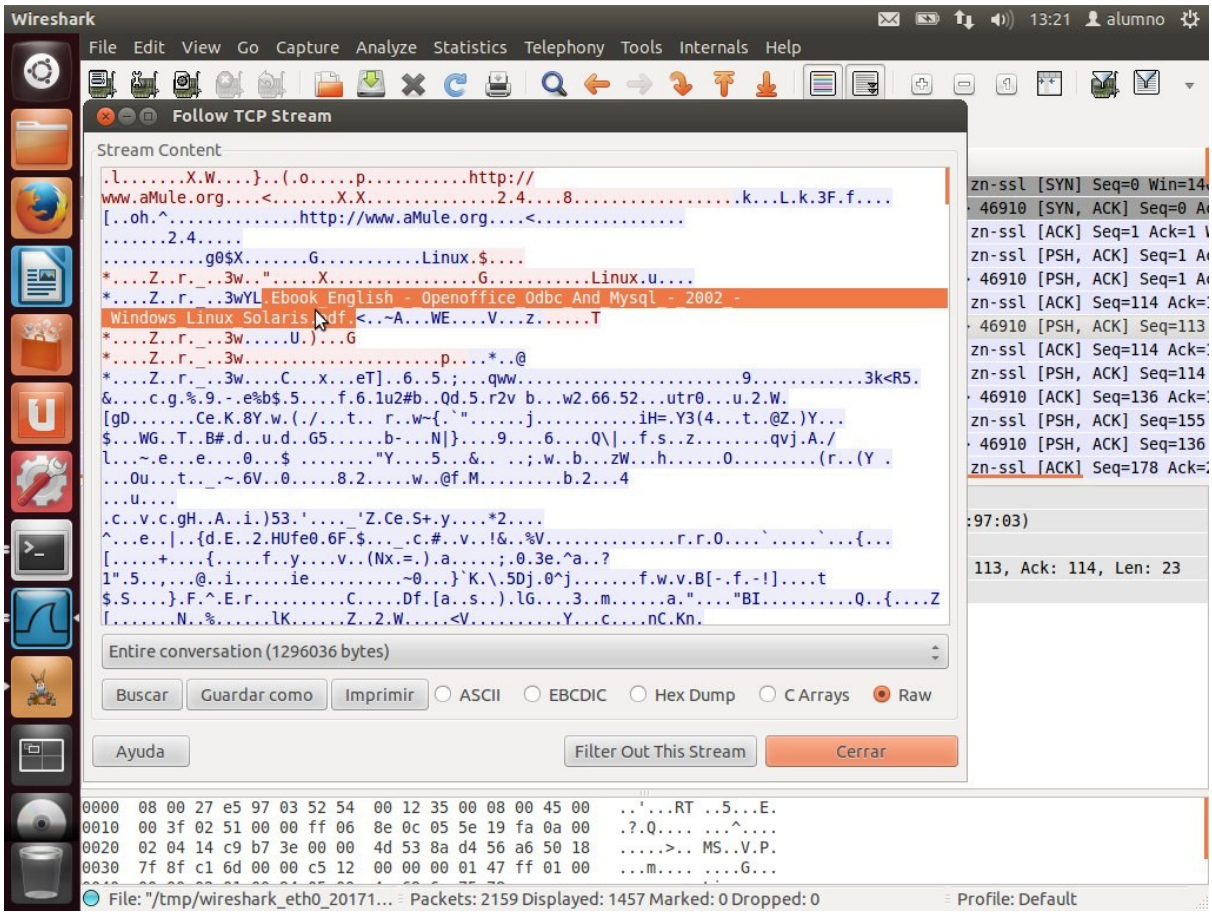
11. Pausamos wireshark.

12. filtramos los datos en wireshark con el comando: (ip.src==nuestraIP and ip.dst ==IPservidor) or (ip.src==IPservidor and ip.dst==nuestraIP).

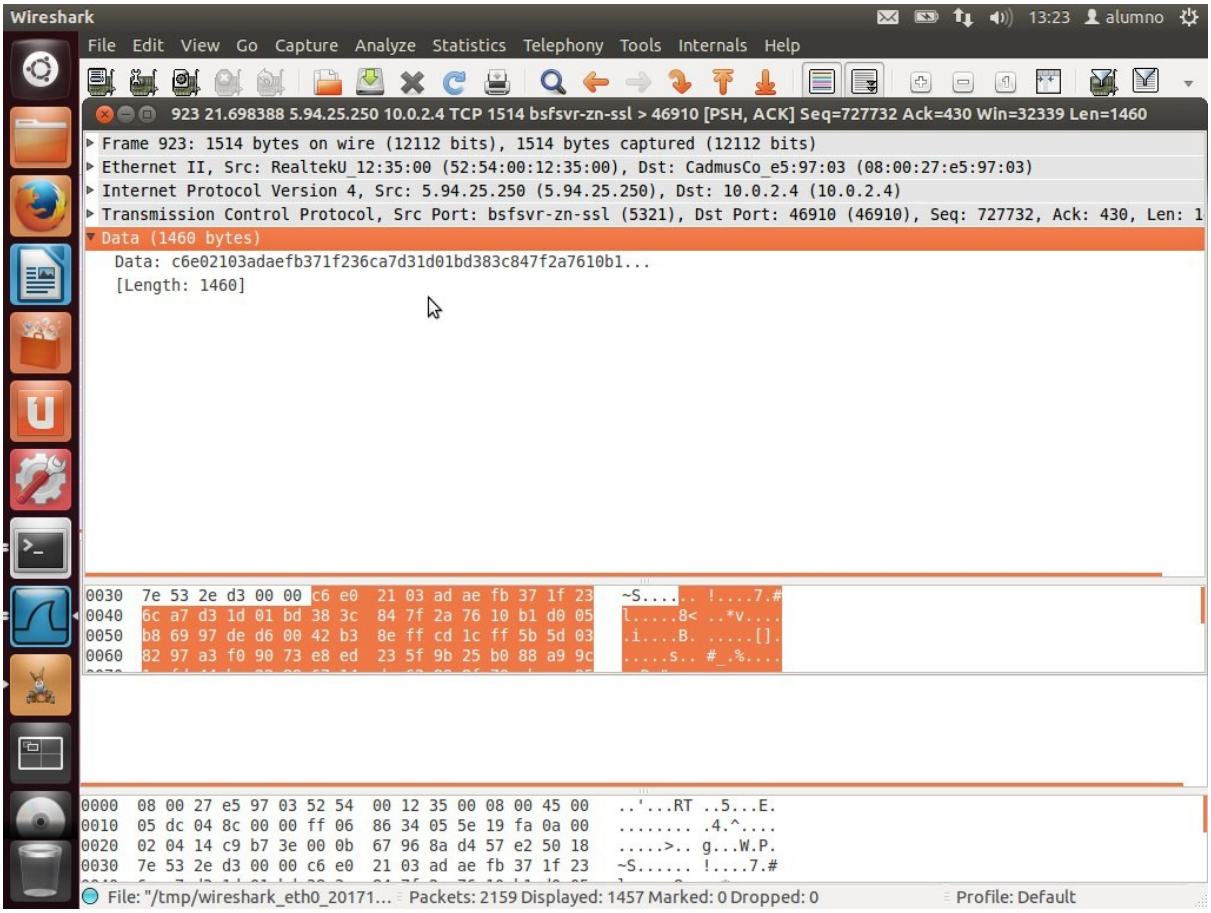


4.3 Analizar los paquetes

13. Si le damos click derecho a algún paquete y luego a “follow tcp stream” podemos ver el archivo que nos hemos descargado.



14. Pulsando doble click en cualquier paquete se nos abre otra ventana donde tenemos información detallada de cada paquete.[6]
    a. La primera línea “frame XX” podemos ver un resumen del frame en el que estamos.
    b. La línea de “Ethernet” simplemente tenemos la ip destino y la ip origen.
    c. La tercera línea es “Internet Protocol”. En esta parte podemos ver las IP destino y origen así como la longitud en bytes del encabezado.
    d. La cuarta línea (TCP) es donde vemos los puertos origen y destino ya que en la capa de transporte se comunican mediante el uso de puertos.
    e. La parte final (DATA) es la parte de datos. Aquí se ven qué datos se envían a través del medio. Esta parte es importante ya que sabremos si se usa ssh o rsh/rlogin. En caso de usarse ssh los datos estarán encriptados en cambio si es rsh/rlogin no lo están y los datos se envían en texto plano por lo que podemos capturar el paquete y leer el nombre de usuario y/o la contraseña.



(podemos ver que se usa ssh ya que el contenido de “Data” está encriptado)

5. Conclusiones

La red Kad no es ni mejor ni peor que la eD2K, cada una tiene sus ventajas y desventajas.
La red Kad, al tratarse de una red totalmente descentralizada, su mayor ventaja es que puede expandirse infinitamente sin que esto afecte a su rendimiento de la red, con esto aumentan las posibilidades de disponibilidad de ficheros existentes, ya que los mismos son indexados por millones de nodos.

Otra ventaja es que al restar conectado a una red Kad, aunque se estropeen o desconecten los servidores puedes seguir descargando ya que las buśquedas en Kad se realizan en toda la red y no en servidores determinados.

Una desventaja de la buśqueda a través de Kad con respecto a eD2K es que la Kad no te devuelve unos valores de disponibilidad/fuentes de archivo tan acertados como eD2K. Sin embargo, no se tiene el límite de 201 resultados para cada búsqueda que tiene eD2K ni existe la posibilidad de que te echen del servidor por realizar demasiadas búsquedas en poco tiempo.

6. Bibliografía

[1]: https://syssec.kaist.ac.kr/~yongdaek/doc/kad_attack_securecomm.pdf
[2]: https://es.wikipedia.org/wiki/Kademlia
[3]: https://es.wikipedia.org/wiki/Kad
[4]: https://es.wikipedia.org/wiki/ED2k
[5]: https://forum.emule-project.net/index.php?showtopic=39066
[6]: Inspección de paquetes en Wireshark: https://www.techrepublic.com/blog/linux-and-open-source/use-wireshark-to-inspect-packets-on-your-network/