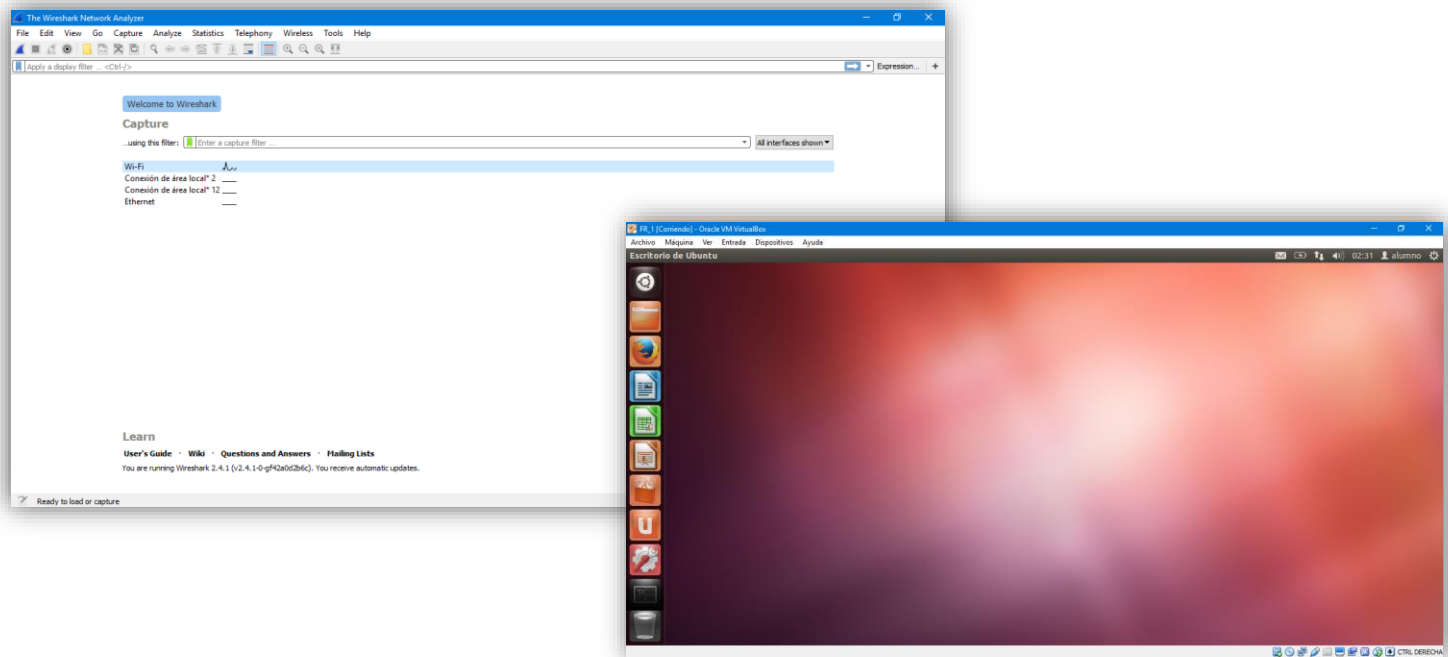


Jose Antonio Ruiz Millán

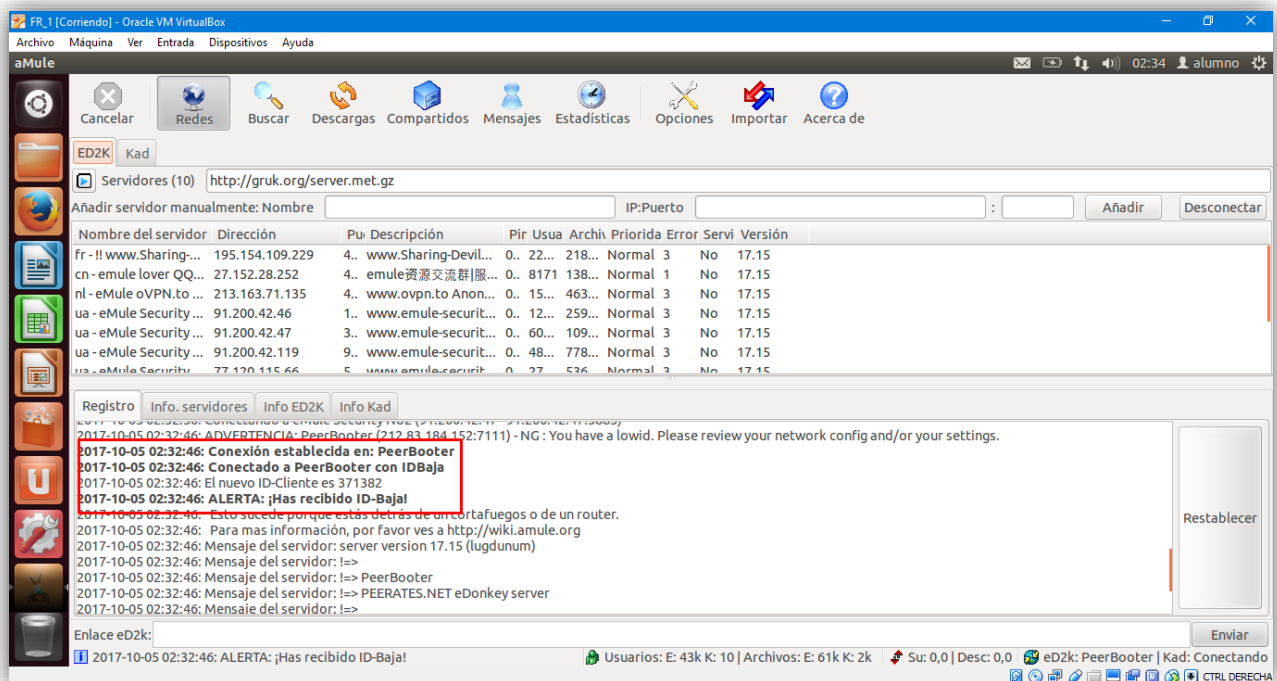
# Seminario 2

Fundamentos de Redes

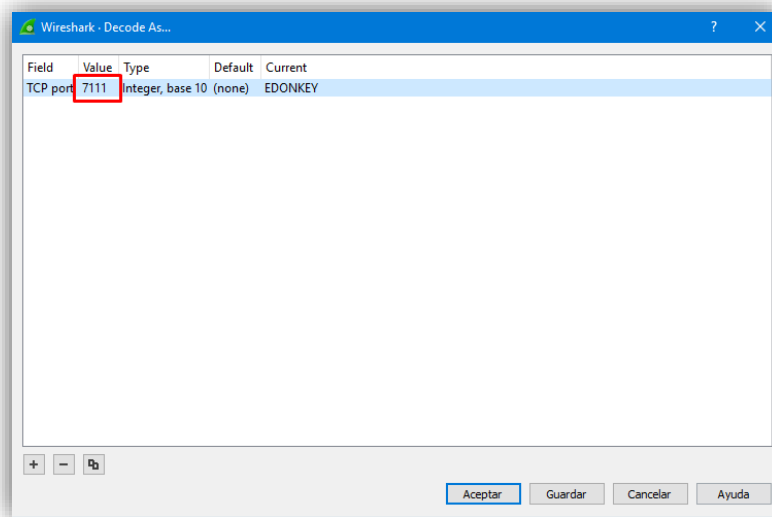
Para comenzar, **arrancamos Wireshark** en la máquina anfitrión y **encendemos nuestra máquina virtual**:



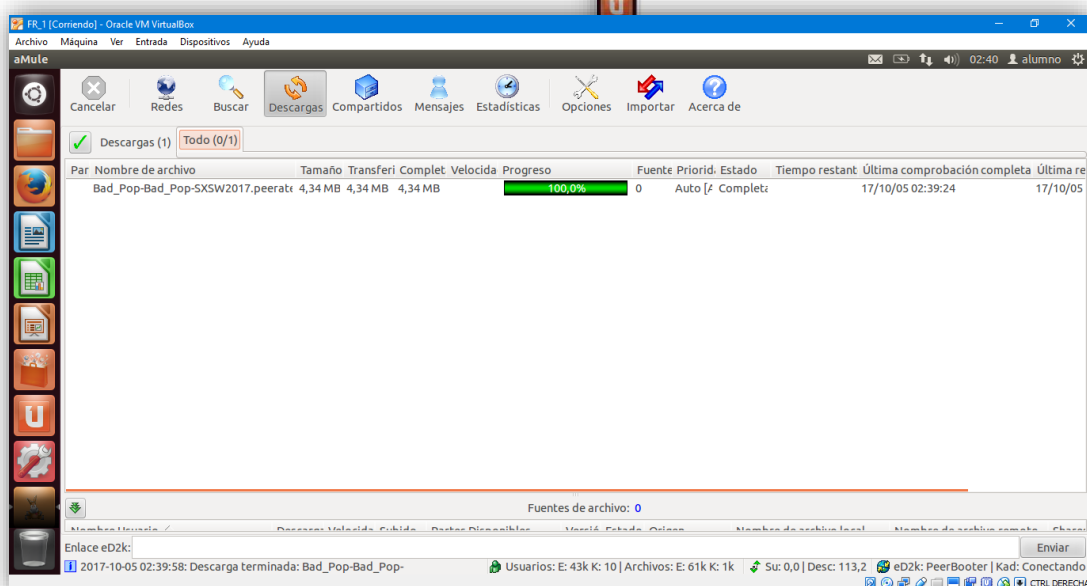
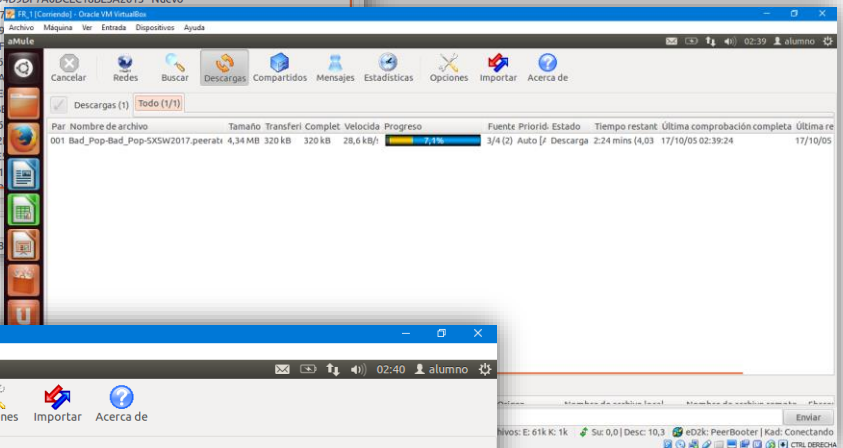
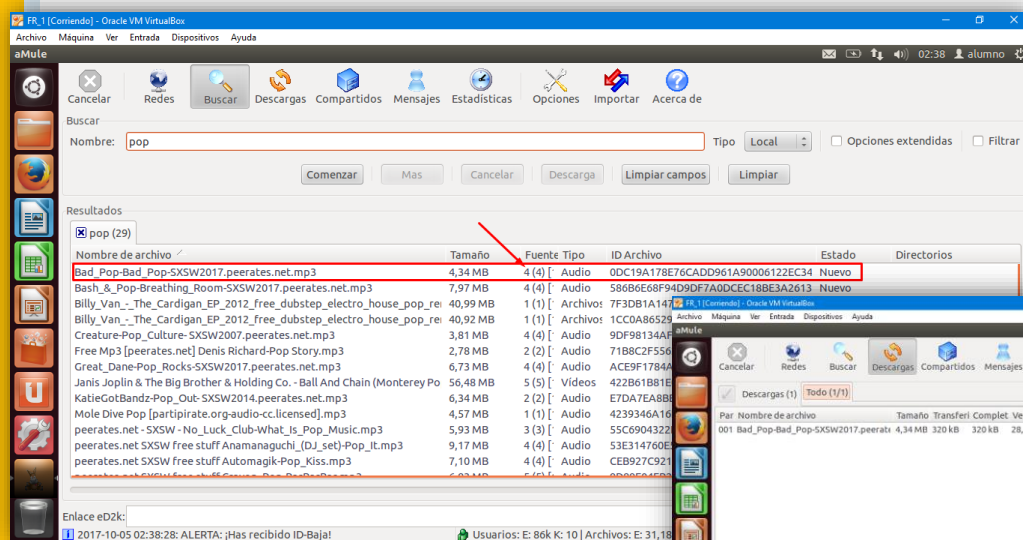
Una vez aquí empezamos a **escanear con el Wireshark**, **arrancamos el aMule** en el virtual y comenzamos:



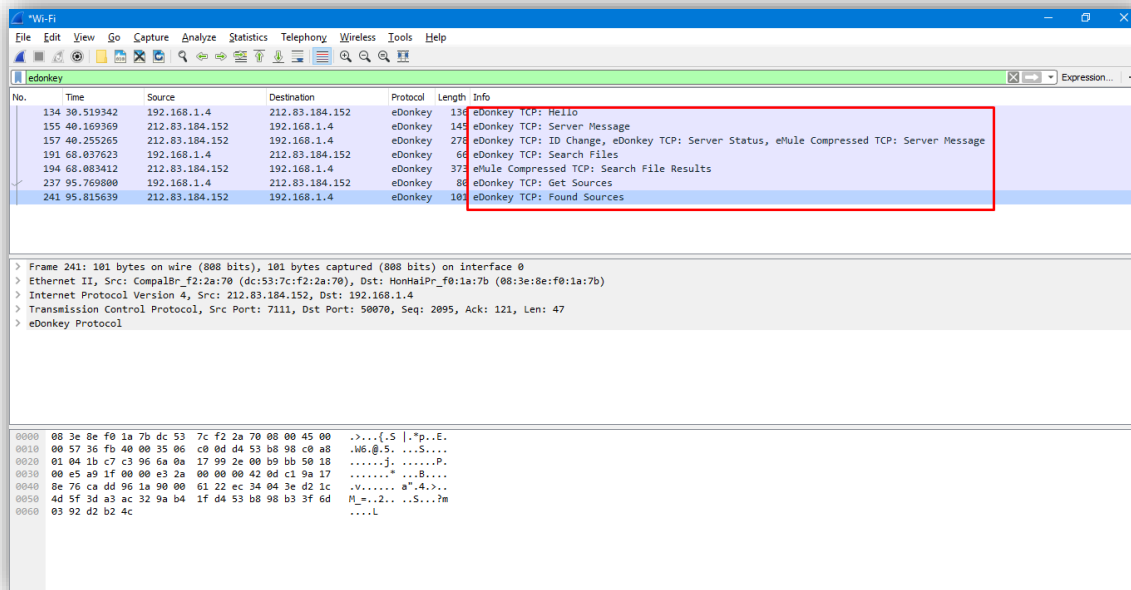
Si nuestro **Wireshark no detecta** los paquetes a través del protocolo edonkey, podemos poner que el puerto por el que nos hemos conectado al servidor que en nuestro caso es **7111** sea un puerto que utiliza el protocolo edonkey.



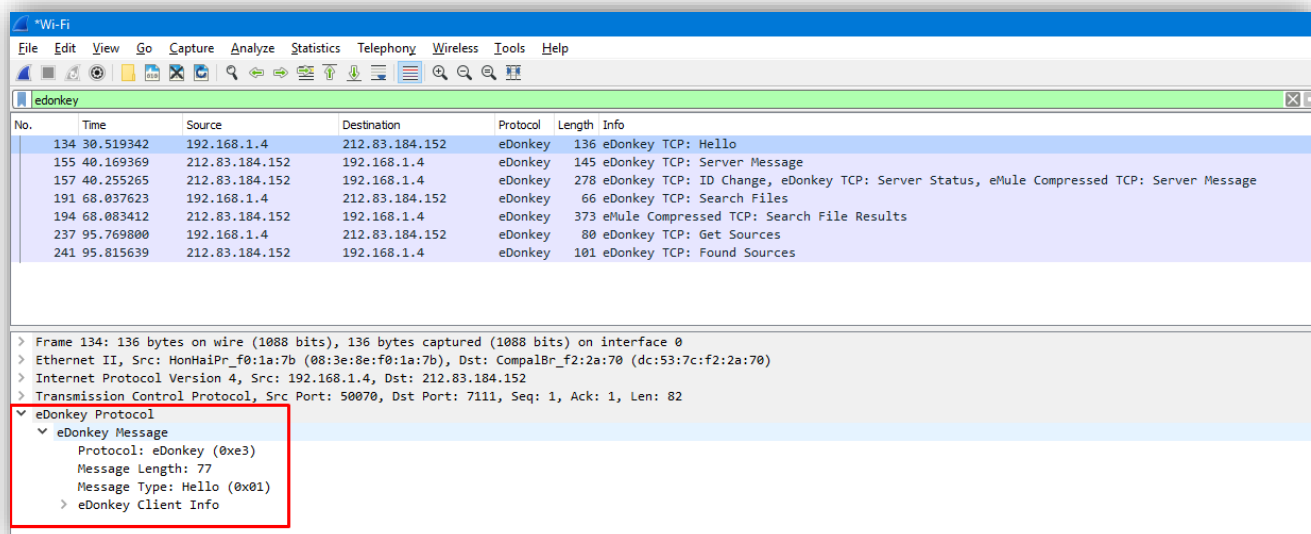
Una vez hecho, ya podemos irnos al aMule y buscar un **fichero** que tenga **varias fuentes**, y una vez tengamos uno, **lo descargamos**.



Ya tenemos el fichero descargado y toda la secuencia escaneada a través del Wireshark, vamos a examinar los paquetes que hemos detectado.



Podemos ver los paquetes que hemos detectado como nuestra virtual conecta con el servidor, este le responde... etc. Sigamos mirando los paquetes:



Si pinchamos en el primer paquete, podemos ver como la máquina virtual envía un “saludo” al servidor para conectarse.

No.	Time	Source	Destination	Protocol	Length	Info
134	30.519342	192.168.1.4	212.83.184.152	eDonkey	136	eDonkey TCP: Hello
155	40.169369	212.83.184.152	192.168.1.4	eDonkey	145	eDonkey TCP: Server Message
157	40.255265	212.83.184.152	192.168.1.4	eDonkey	278	eDonkey TCP: ID Change, eDonkey TCP: Server Status, eMule Compressed TCP: Server Message
191	68.037623	192.168.1.4	212.83.184.152	eDonkey	66	eDonkey TCP: Search Files
194	68.083412	212.83.184.152	192.168.1.4	eDonkey	373	eMule Compressed TCP: Search File Results
237	95.769800	192.168.1.4	212.83.184.152	eDonkey	80	eDonkey TCP: Get Sources
241	95.815639	212.83.184.152	192.168.1.4	eDonkey	101	eDonkey TCP: Found Sources

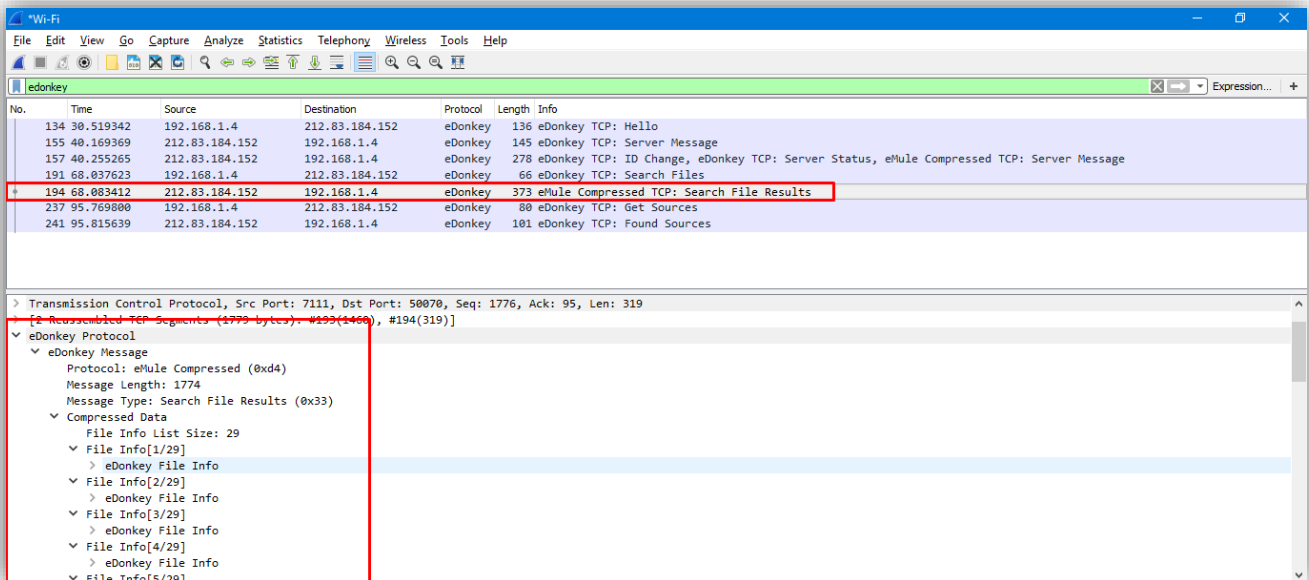
> Frame 155: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface 0  
 > Ethernet II, Src: CompalBr\_f2:2a:70 (dc:53:7c:f2:2a:70), Dst: HonHaiPr\_f0:1a:7b (08:3e:8e:f0:1a:7b)  
 > Internet Protocol Version 4, Src: 212.83.184.152, Dst: 192.168.1.4  
 > Transmission Control Protocol, Src Port: 7111, Dst Port: 50070, Seq: 1, Ack: 83, Len: 91  
 > eDonkey Protocol  
 > eDonkey Message  
 > Protocol: eDonkey (0xe3)  
 > Message Length: 86  
 > Message Type: Server Message (0x38)  
 > String Length: 83  
 > String: WARNING : You have a lowid. Please review your network config and/or your settings.

Vemos ahora la respuesta del servidor que le da a la máquina virtual, donde le da un aviso que también lo podíamos ver en la imagen del aMule cuando nos conectamos al servidor.

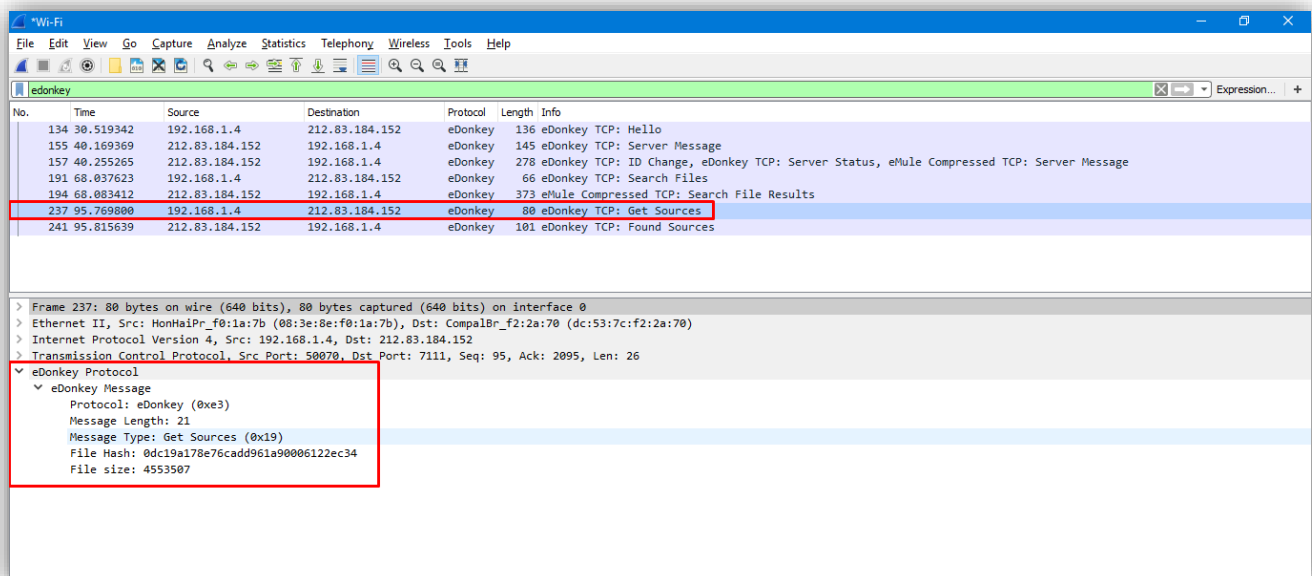
No.	Time	Source	Destination	Protocol	Length	Info
134	30.519342	192.168.1.4	212.83.184.152	eDonkey	136	eDonkey TCP: Hello
155	40.169369	212.83.184.152	192.168.1.4	eDonkey	145	eDonkey TCP: Server Message
157	40.255265	212.83.184.152	192.168.1.4	eDonkey	278	eDonkey TCP: ID Change, eDonkey TCP: Server Status, eMule Compressed TCP: Server Message
191	68.037623	192.168.1.4	212.83.184.152	eDonkey	66	eDonkey TCP: Search Files
194	68.083412	212.83.184.152	192.168.1.4	eDonkey	373	eMule Compressed TCP: Search File Results
237	95.769800	192.168.1.4	212.83.184.152	eDonkey	80	eDonkey TCP: Get Sources
241	95.815639	212.83.184.152	192.168.1.4	eDonkey	101	eDonkey TCP: Found Sources

> Ethernet II, Src: HonHaiPr\_f0:1a:7b (08:3e:8e:f0:1a:7b), Dst: CompalBr\_f2:2a:70 (dc:53:7c:f2:2a:70)  
 > Internet Protocol Version 4, Src: 192.168.1.4, Dst: 212.83.184.152  
 > Transmission Control Protocol, Src Port: 50070, Dst Port: 7111, Seq: 83, Ack: 316, Len: 12  
 > eDonkey Protocol  
 > eDonkey Message  
 > Protocol: eDonkey (0xe3)  
 > Message Length: 7  
 > Message Type: Search Files (0x16)  
 > Search Type: Name (1)  
 > String Length: 3  
 > String: pop

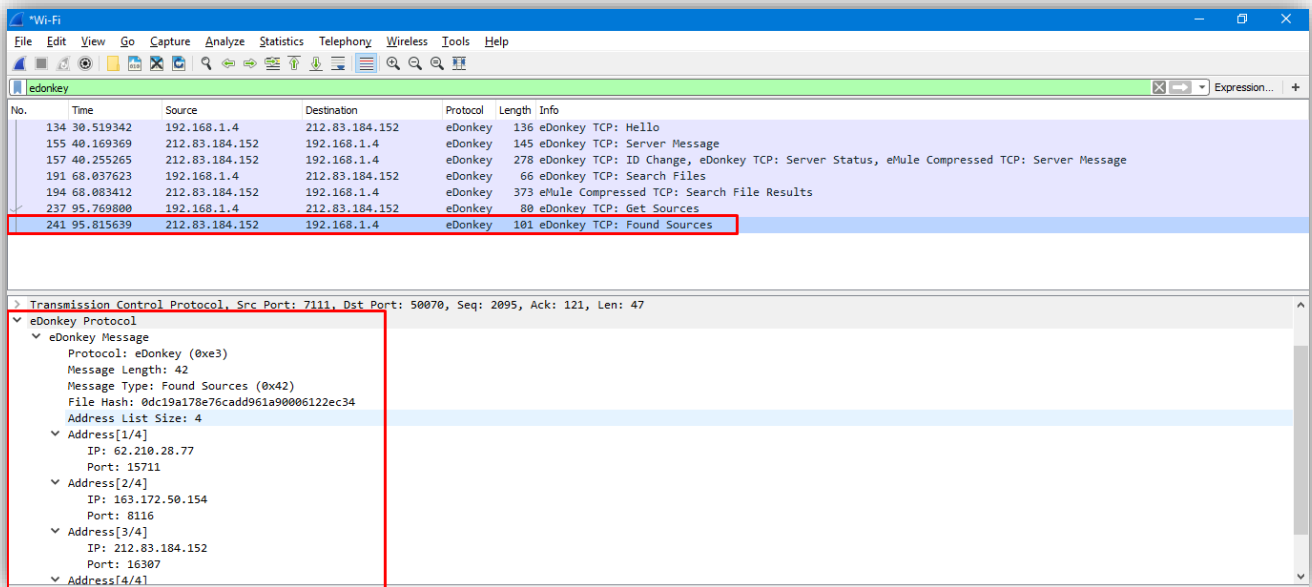
Aquí podemos ver el paquete que hemos obtenido al realizar la búsqueda de ficheros en el aMule y podemos ver que parámetros hemos escrito para enviárselos al servidor para que nos devuelva el resultado de la búsqueda.



Ahora vemos el resultado que nos ha devuelto el servidor cuando hemos buscado y podemos ver los diferentes ficheros que nos ha devuelto el servidor entre los que nosotros hemos escogido 1.



Ahora vemos como nuestra máquina virtual envía al servidor un mensaje para que nos muestre las distintas fuentes para comenzar la descarga.



No.	Time	Source	Destination	Protocol	Length	Info
134	30.519342	192.168.1.4	212.83.184.152	eDonkey	136	eDonkey TCP: Hello
155	40.169369	212.83.184.152	192.168.1.4	eDonkey	145	eDonkey TCP: Server Message
157	40.255265	212.83.184.152	192.168.1.4	eDonkey	278	eDonkey TCP: ID Change, eDonkey TCP: Server Status, eMule Compressed TCP: Server Message
191	68.037623	192.168.1.4	212.83.184.152	eDonkey	66	eDonkey TCP: Search Files
194	68.083412	212.83.184.152	192.168.1.4	eDonkey	373	eMule Compressed TCP: Search File Results
237	95.769800	192.168.1.4	212.83.184.152	eDonkey	80	eDonkey TCP: Get Sources
241	95.815639	212.83.184.152	192.168.1.4	eDonkey	101	eDonkey TCP: Found Sources

Transmission Control Protocol, Src Port: 7111, Dst Port: 50070, Seq: 2095, Ack: 121, Len: 47	
eDonkey Protocol	
eDonkey Message	
Protocol: eDonkey (0xe3)	
Message Length: 42	
Message Type: Found Sources (0x42)	
File Hash: 0dc19a178e76cadd961a90006122ec34	
Address List Size: 4	
Address[1/4]	
IP: 62.210.28.77	
Port: 15711	
Address[2/4]	
IP: 163.172.50.154	
Port: 8116	
Address[3/4]	
IP: 212.83.184.152	
Port: 16307	
Address[4/4]	

Por último, vemos como la descarga proviene de distintas fuentes distintas y finalmente termina la descarga.