

Actividades Seminario 2

por: Arturo Cortés Sánchez

Captura de una
búsqueda en
amule de ubuntu

eth1 [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.2.5	91.200.42.119	eDonkey	48	eDonkey UDP: Server Status Request
2	1.706246	10.0.2.5	192.168.1.1	DNS	76	Standard query A daisy.ubuntu.com
3	1.709173	192.168.1.1	10.0.2.5	DNS	108	Standard query response A 162.213.33.
4	2.708447	10.0.2.5	192.168.1.1	DNS	76	Standard query A daisy.ubuntu.com
5	2.711929	192.168.1.1	10.0.2.5	DNS	108	Standard query response A 162.213.33.
6	5.801863	10.0.2.5	213.163.71.135	eDonkey	48	eDonkey UDP: Server Status Request
7	7.585668	10.0.2.5	212.83.184.152	TCP	69	54947 > 7111 [PSH, ACK] Seq=1 Ack=1 W
8	7.599123	212.83.184.152	10.0.2.5	TCP	60	7111 > 54947 [ACK] Seq=1 Ack=16 Win=3
9	7.644056	212.83.184.152	10.0.2.5	TCP	393	7111 > 54947 [PSH, ACK] Seq=1 Ack=16
10	7.644075	10.0.2.5	212.83.184.152	TCP	54	54947 > 7111 [ACK] Seq=16 Ack=340 Win
11	11.371457	10.0.2.5	77.120.115.66	eDonkey	48	eDonkey UDP: Server Status Request

Frame 1: 48 bytes on wire (384 bits), 48 bytes captured (384 bits)

Ethernet II, Src: CadmusCo_4f:b6:46 (08:00:27:4f:b6:46), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)

Internet Protocol Version 4, Src: 10.0.2.5 (10.0.2.5), Dst: 91.200.42.119 (91.200.42.119)

User Datagram Protocol, Src Port: contclientms (4665), Dst Port: 9943 (9943)

eDonkey Protocol

0000 52 54 00 12 35 00 08 00 27 4f b6 46 08 00 45 00 RT..5... 'O.F..E.
0010 00 22 fc 9a 40 00 40 11 ab ec 0a 00 02 05 5b c8 .".@.@.[.
0020 2a 77 12 39 26 d7 00 0e 92 63 e3 96 9f 9a aa 55 *w.9&... .C.....U

File: "/tmp/wireshark_eth1_20171... Packets: 11 Displayed: 11 Marked: 0 Dropped: 0

eth1 [Wireshark 1.6.7] 18:36

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
7388	26.091532	163.172.50.154	10.0.2.5	TCP	1514	cp-cluster > 49040 [PSH, ACK] Seq=3558015 Ack=1278 Win=31491 Len=1460
7389	26.091556	10.0.2.5	163.172.50.154	TCP	54	49040 > cp-cluster [ACK] Seq=1278 Ack=3559475 Win=65535 Len=0
7390	26.091839	163.172.50.154	10.0.2.5	TCP	1490	cp-cluster > 49040 [PSH, ACK] Seq=3559475 Ack=1278 Win=31491 Len=1436
7391	26.093792	10.0.2.5	163.172.50.154	TCP	54	49040 > cp-cluster [ACK] Seq=1278 Ack=3560911 Win=65535 Len=0
7392	26.094063	163.172.50.154	10.0.2.5	TCP	1502	cp-cluster > 49040 [PSH, ACK] Seq=3560911 Ack=1278 Win=31491 Len=1448
7393	26.094632	10.0.2.5	163.172.50.154	TCP	54	49040 > cp-cluster [ACK] Seq=1278 Ack=3562359 Win=65535 Len=0
7394	26.095179	163.172.50.154	10.0.2.5	TCP	1502	cp-cluster > 49040 [PSH, ACK] Seq=3562359 Ack=1278 Win=31491 Len=1448
7395	26.099667	163.172.50.154	10.0.2.5	TCP	1514	cp-cluster > 49040 [PSH, ACK] Seq=3563807 Ack=1278 Win=31491 Len=1460
7396	26.099732	10.0.2.5	163.172.50.154	TCP	54	49040 > cp-cluster [ACK] Seq=1278 Ack=3565267 Win=65535 Len=0
7397	26.100024	163.172.50.154	10.0.2.5	TCP	1490	cp-cluster > 49040 [PSH, ACK] Seq=3565267 Ack=1278 Win=31491 Len=1436
7398	26.100374	10.0.2.5	163.172.50.154	TCP	54	49040 > cp-cluster [ACK] Seq=1278 Ack=3566703 Win=65535 Len=0
7399	26.101329	163.172.50.154	10.0.2.5	TCP	1502	cp-cluster > 49040 [PSH, ACK] Seq=3566703 Ack=1278 Win=31491 Len=1448
7400	26.102279	10.0.2.5	163.172.50.154	TCP	54	49040 > cp-cluster [ACK] Seq=1278 Ack=3568151 Win=65535 Len=0

Window size value: 31491
 [Calculated window size: 31491]
 [Window size scaling factor: -2 (no window scaling used)]
 ▶ Checksum: 0x1c8c [validation disabled]
 ▶ [SEQ/ACK analysis]

▼ Data (1448 bytes)
 Data: 1fd7a2ac896e343353a238b400915c1b614d0d6cae0dd4d2...
 [Length: 1448]

0000	08 00 27 4f b6 46 52 54 00 12 35 00 08 00 45 00	.. 'O.FRT ..5...E.
0010	05 d0 10 64 00 00 ff 06 c3 78 a3 ac 32 9a 0a 00	...d.... .x..2...
0020	02 05 1f b4 bf 90 00 36 7b 2d 0e 4b 3b 6a 50 186 {-K;jP.
0030	7b 03 1c 8c 00 00 1f d7 a2 ac 89 6e 34 33 53 a2	{..... ..n43S.

Frame (frame), 1502 bytes Packets: 7601 Displayed: 7601 Marked: 0 Dropped: 2 Profile: Default

Captura de una descarga de amule, en la parte inferior se puede apreciar el string de datos del paquete seleccionado