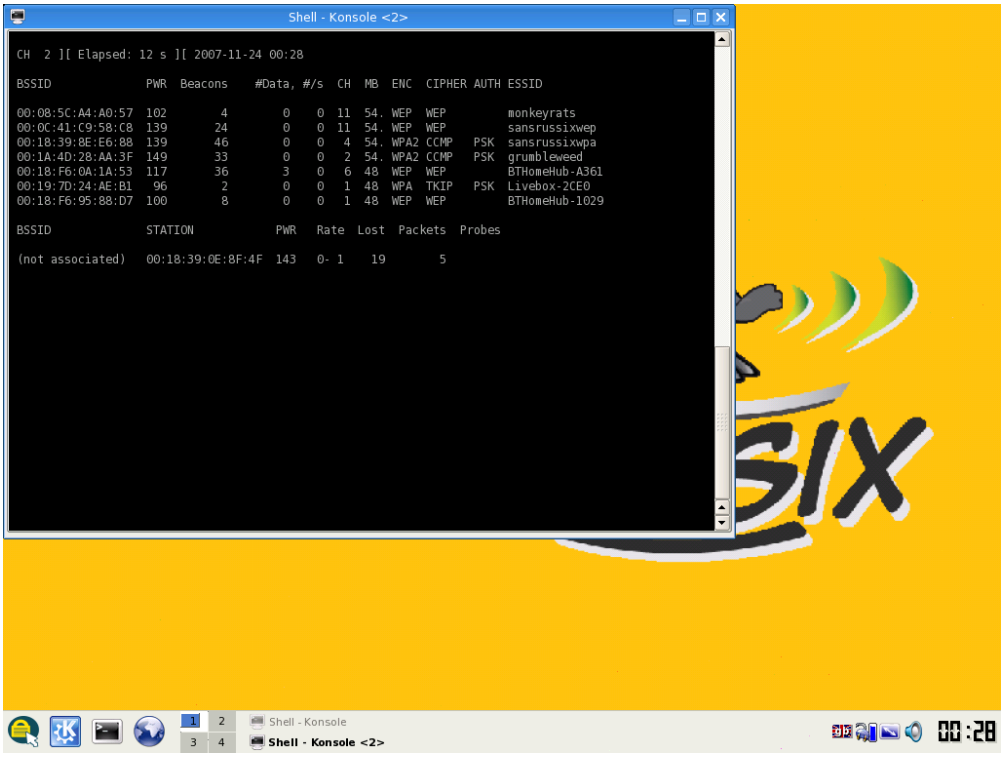
WPA CRACKING WITH RUSSIX

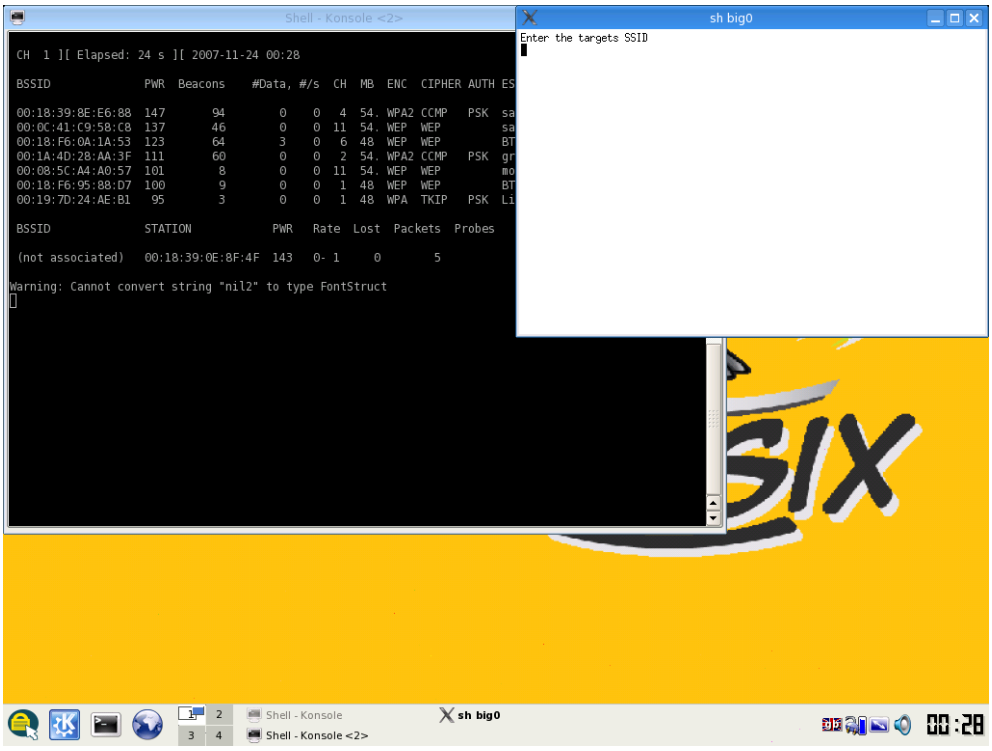
You can start WPA cracking by either selecting "athx (WEP/WPA)" from the menu or by opening a terminal window and typing 0 if you want to use ath0 or 1 if you want to use ath1.

Airodump-ng will start up.

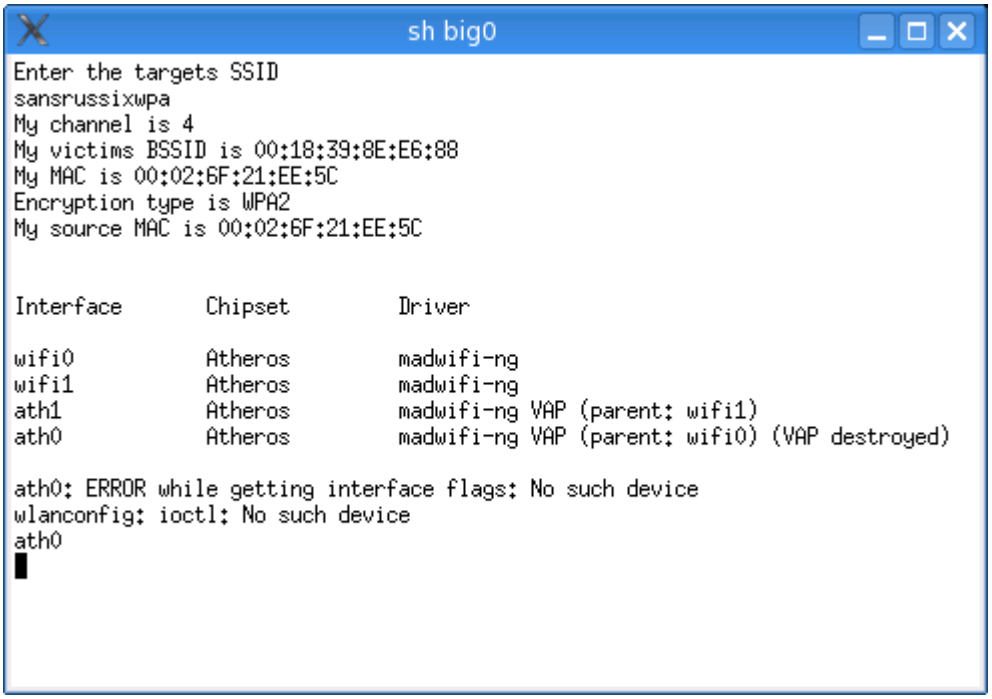


When you find a suitable WPA target hit <CTRL>-C

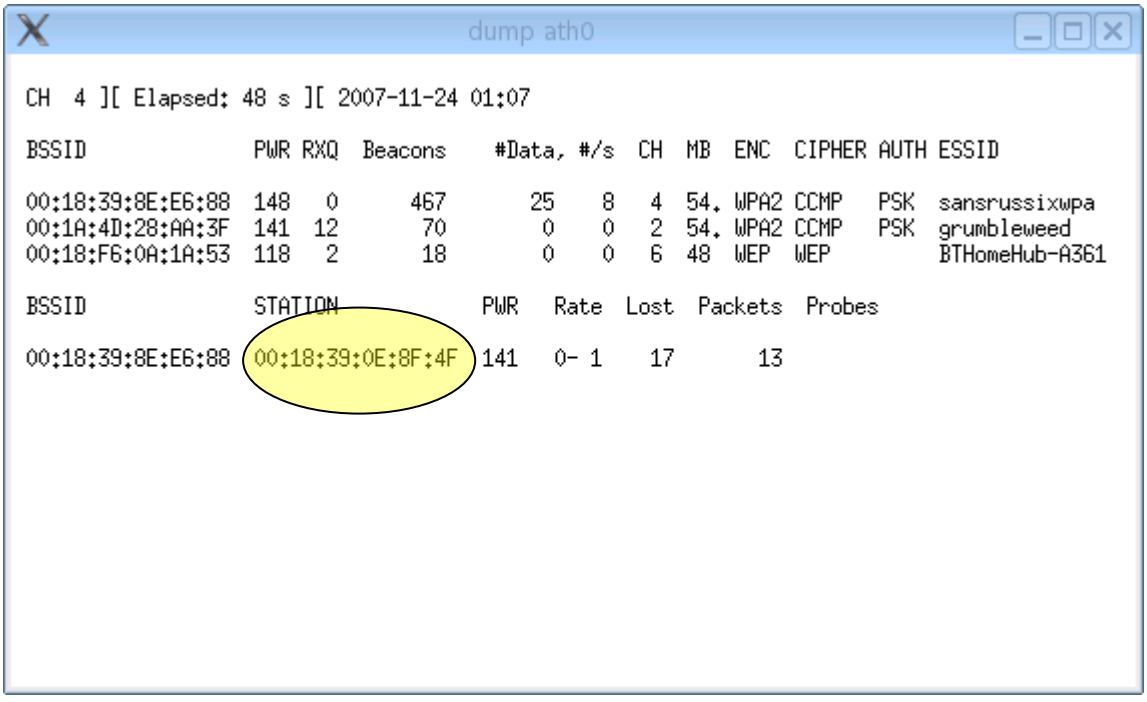
The WPA Cracking script will automatically start You can either cut and paste the SSID in or just type it into the xterm window.



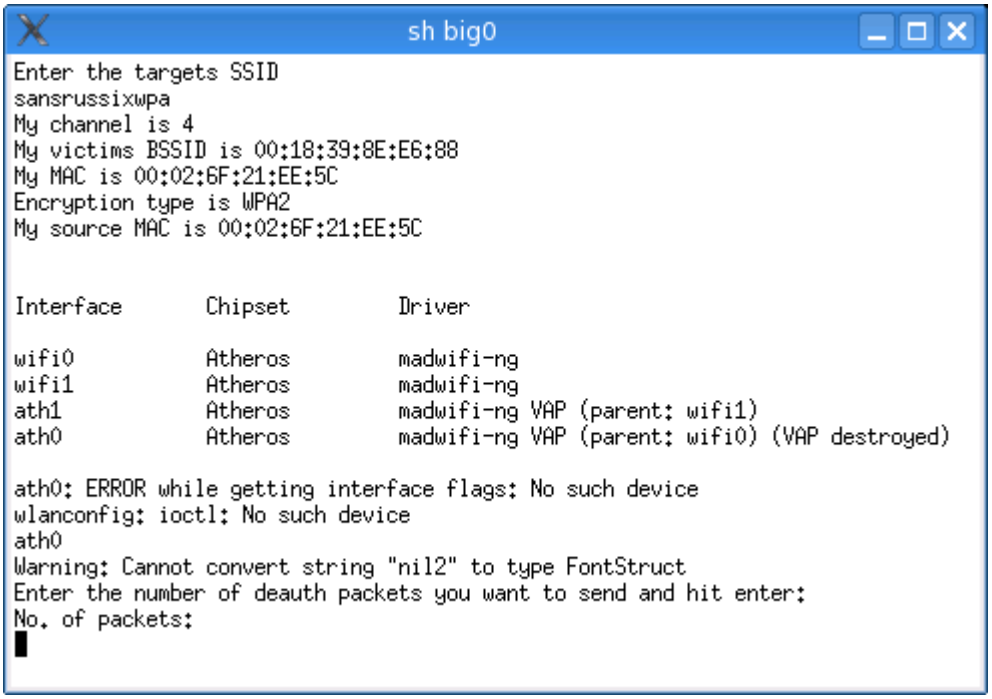
The script will pull all the necessary information from the airodump_ng dump file and reset the atheros card ready for aireplay_ng.



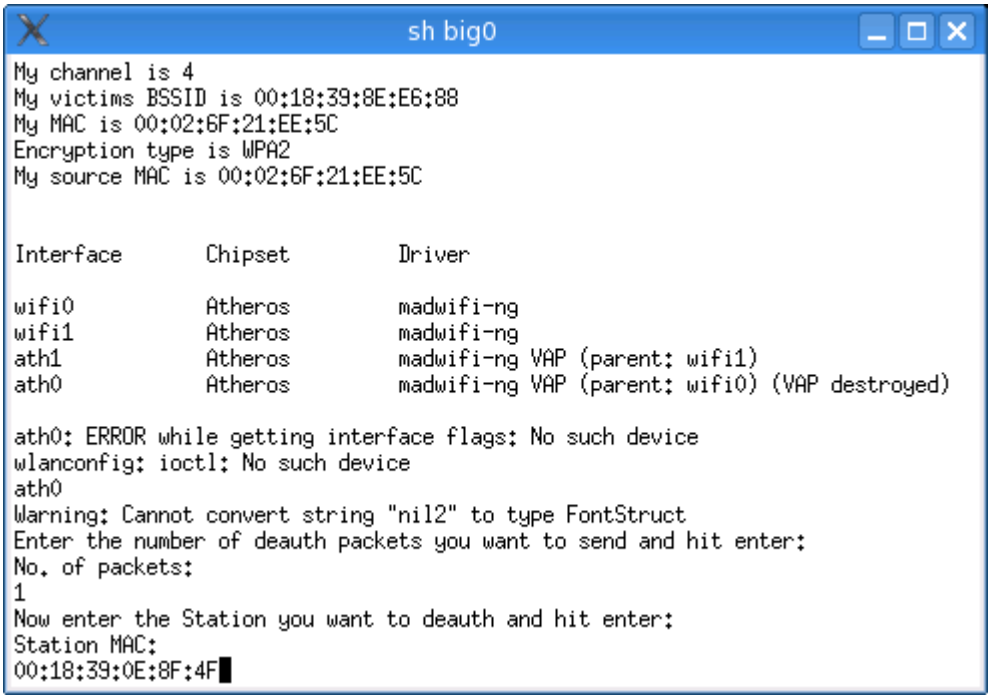
Once the card is ready airodump_ng will automatically start. You will need a client attached to an AP for this attack to work. When you see a suitable target you may proceed with the attack.



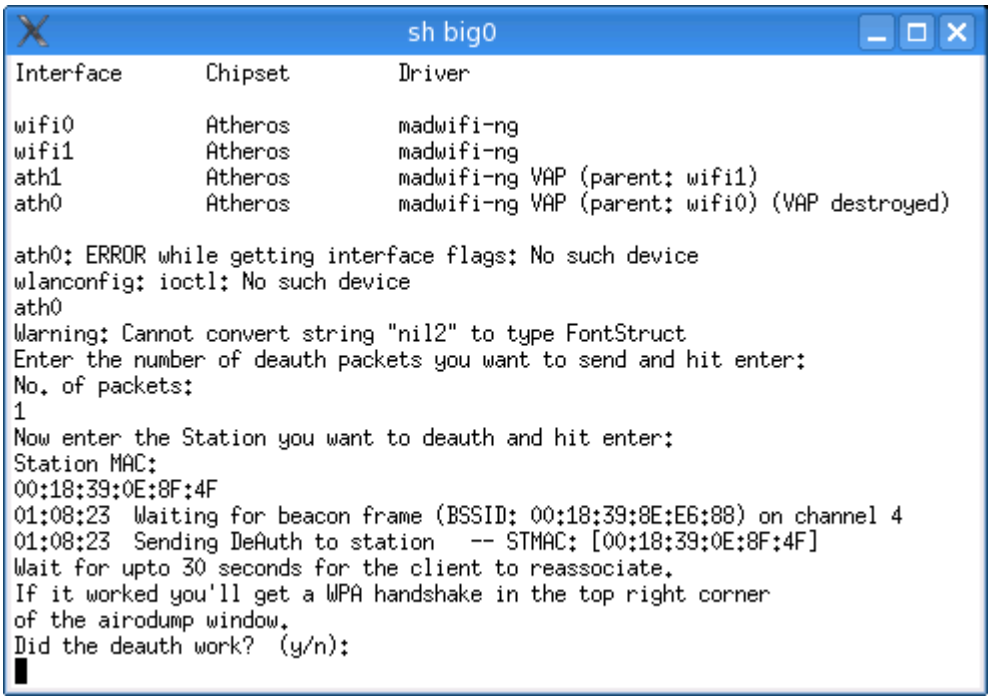
Enter the number of deauth packets you want to send – start at 1 and increase if you are unable to deauth the client.



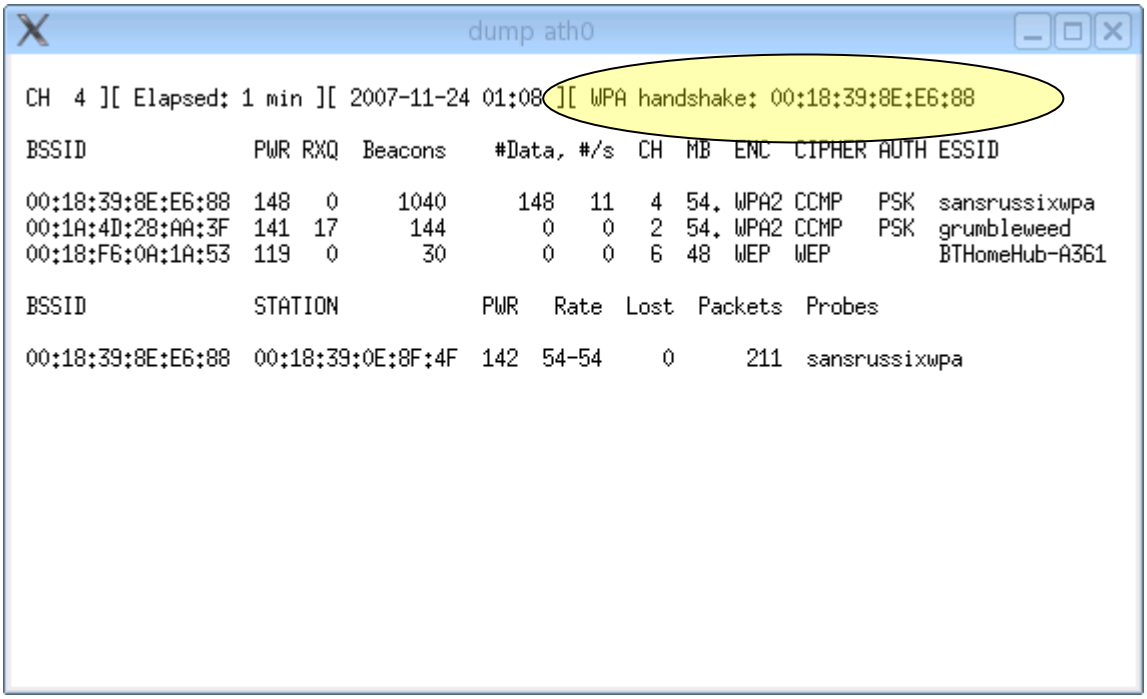
When prompted enter the Client Stations MAC address



You will then be asked if the deauth worked.

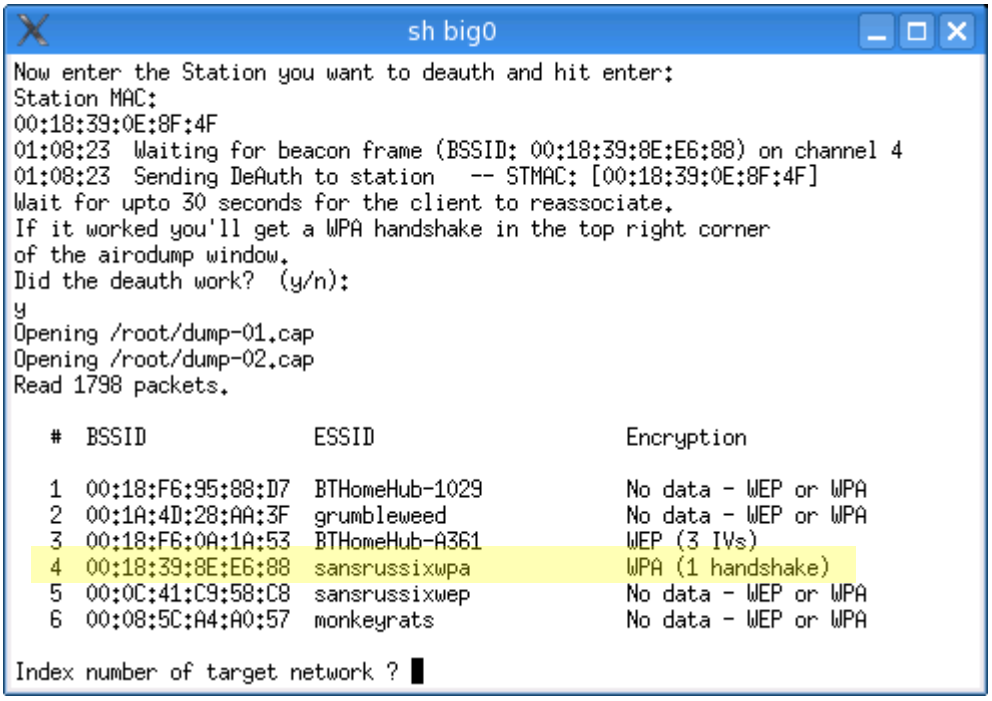


If you monitor the airodump_ng window if you receive a WPA handshake it worked NOTE: Give the client up to about 30 seconds to associate.



When you have a WPA handshake press y and <ENTER> in the required terminal.

You will be asked for the Index number of the target network – in this case 4.



Aircrack_ng will then start trying to brute force the PSK using a small dictionary file.