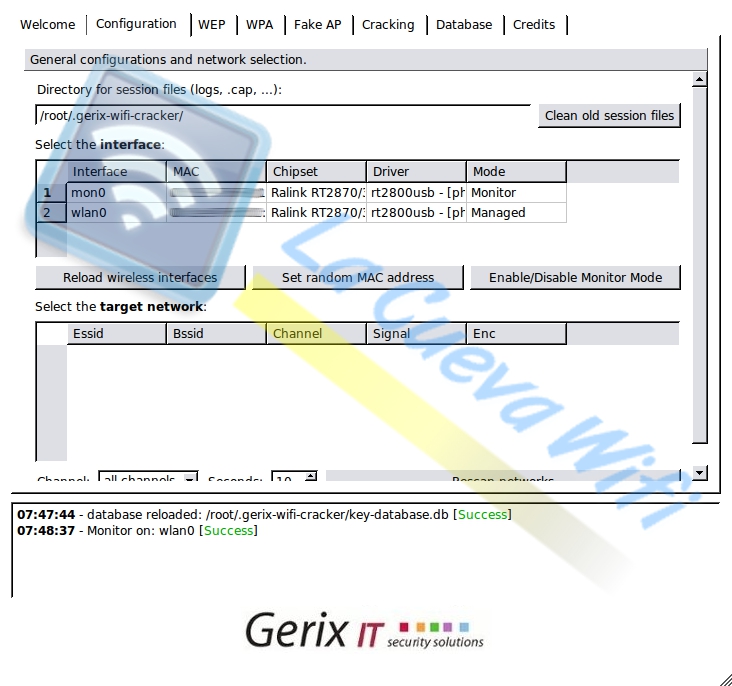
¡Comenzamos! Utilizaremos el programa llamado Gerix Wifi Cracker. El programa se encuentra en:**Applications → BackTrack → Exploitation Tools → Wireless Exploitation → WLAN Exploitation → gerix-wifi-cracker-ng.**

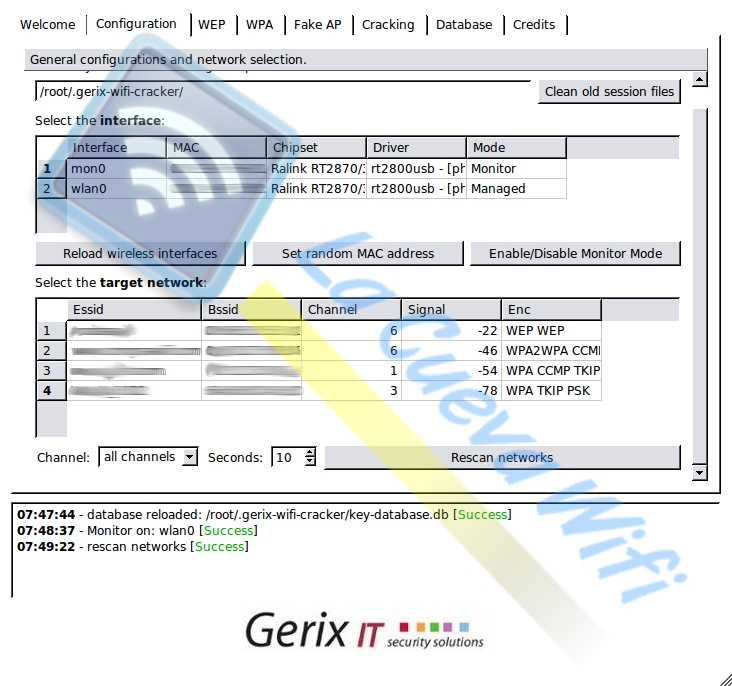
**[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa1.jpg)**

Esta es la pantalla principal del programa.

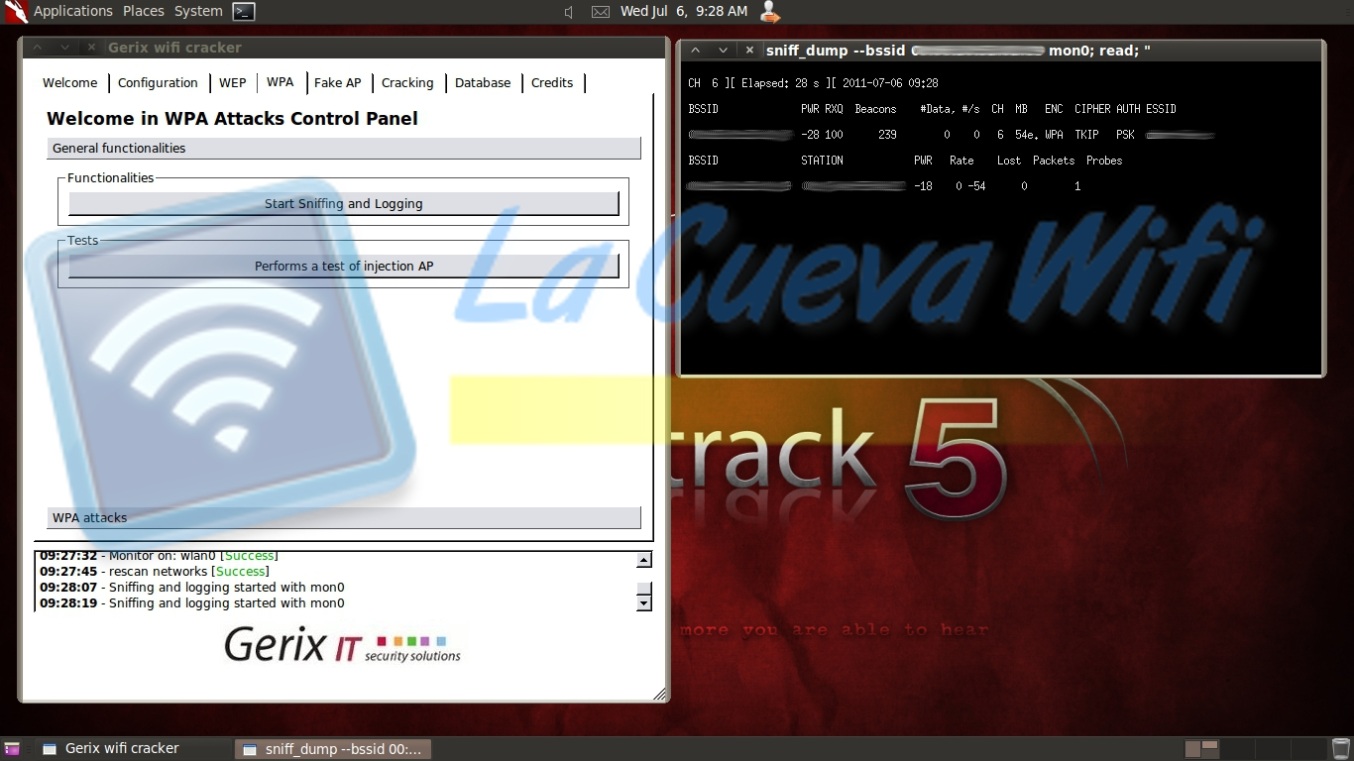
[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa2.jpg)

Ahora tenemos que pinchar en Configuration. En esta pantalla lo primero que vamos  a hacer es habilitar el modo monitor, para eso pulsamos en **Enable/Disable Monitor Mode,** observamos que nos aparece otra interfaz llamada mon0, ese es el modo monitor.

[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa3.jpg)El siguiente paso es escanear las redes que nos rodean. Para eso pulsamos en **Rescan networks.** Nos aparecerán las redes disponibles, seleccionamos la red objetivo.

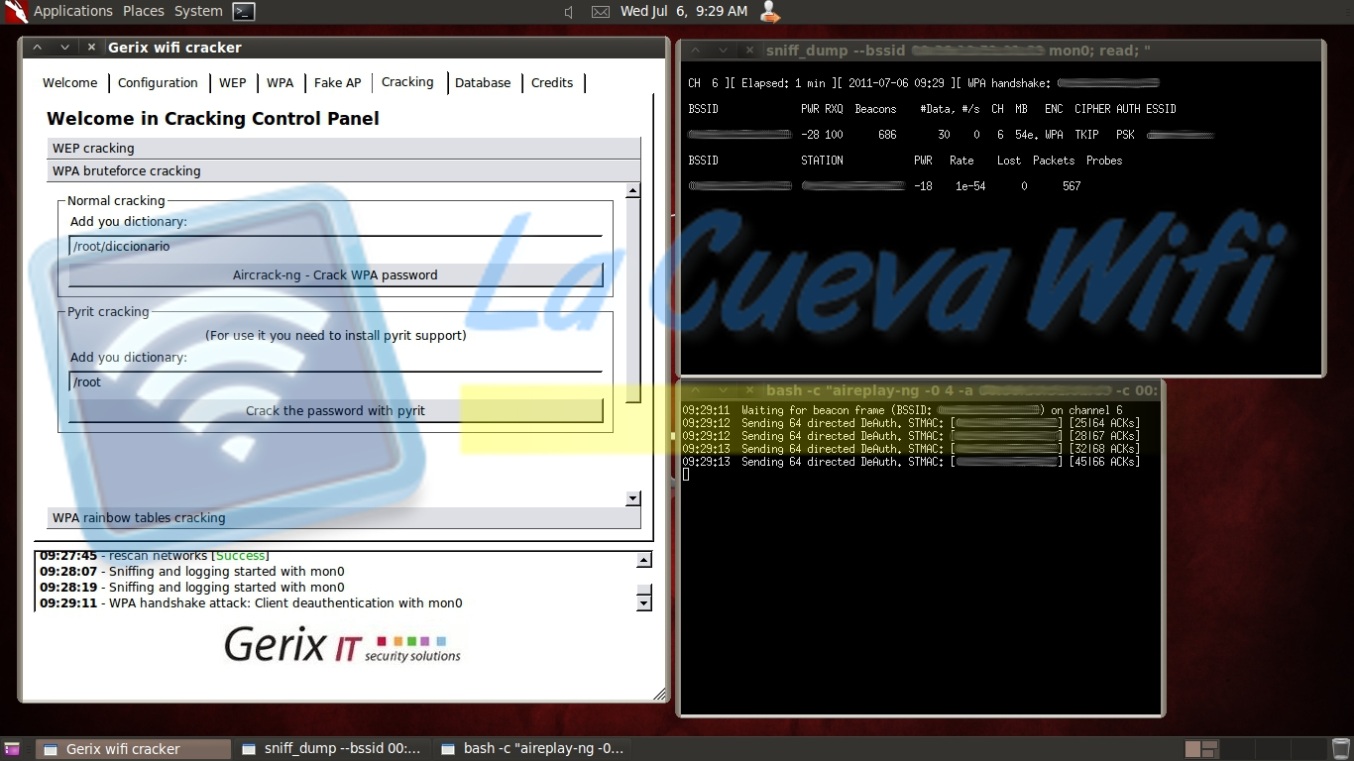
[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa4.jpg)

Una vez tengamos la red seleccionada nos dirigimos a la pestaña **WPA.**

[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa5.jpg)

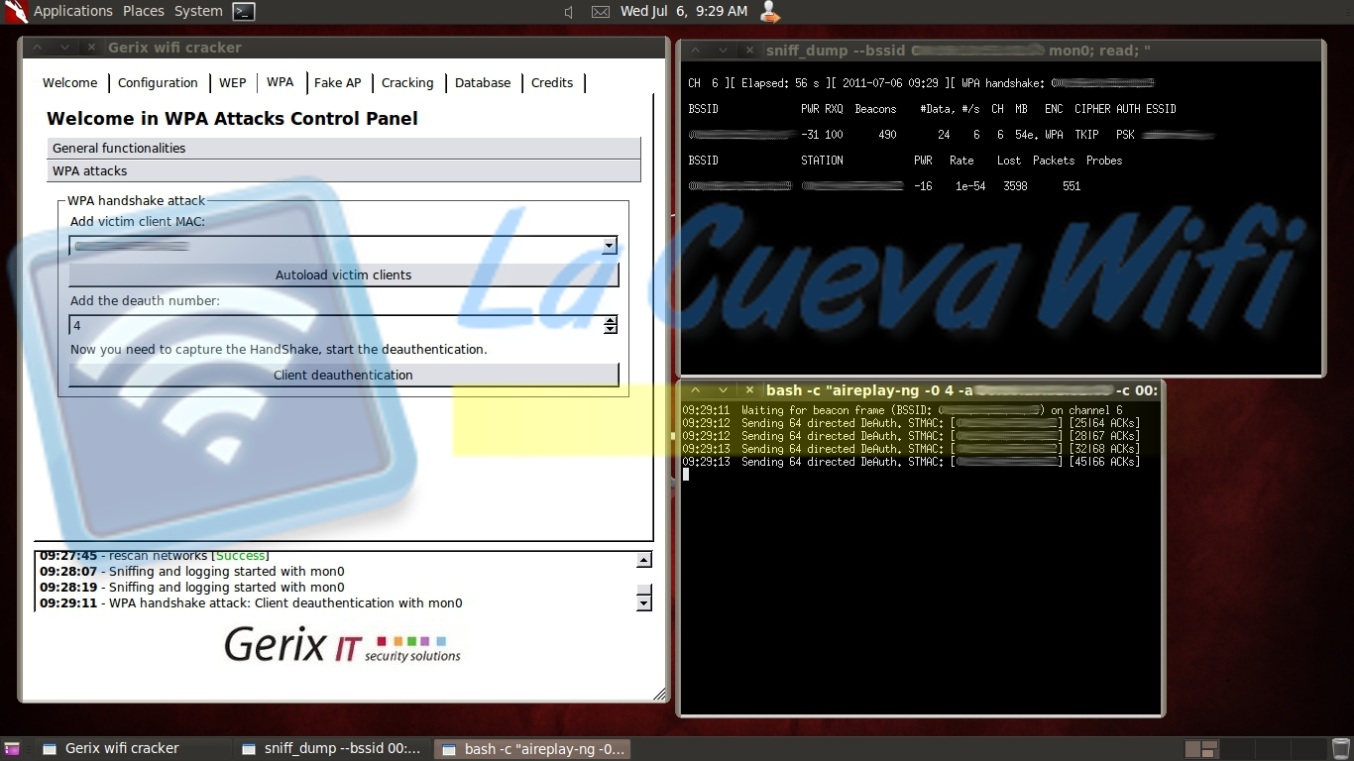
En el apartado **General functionalities** pulsamos en **Start sniffing and Login.** Se nos abrirá una consola como la de la izquierda en la imagen. Esta terminal nos ofrece información sobre la red que escogimos, los clientes conectados, etc.

El siguiente paso es ir al apartado **WPA Attacks.**

[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa6.jpg)

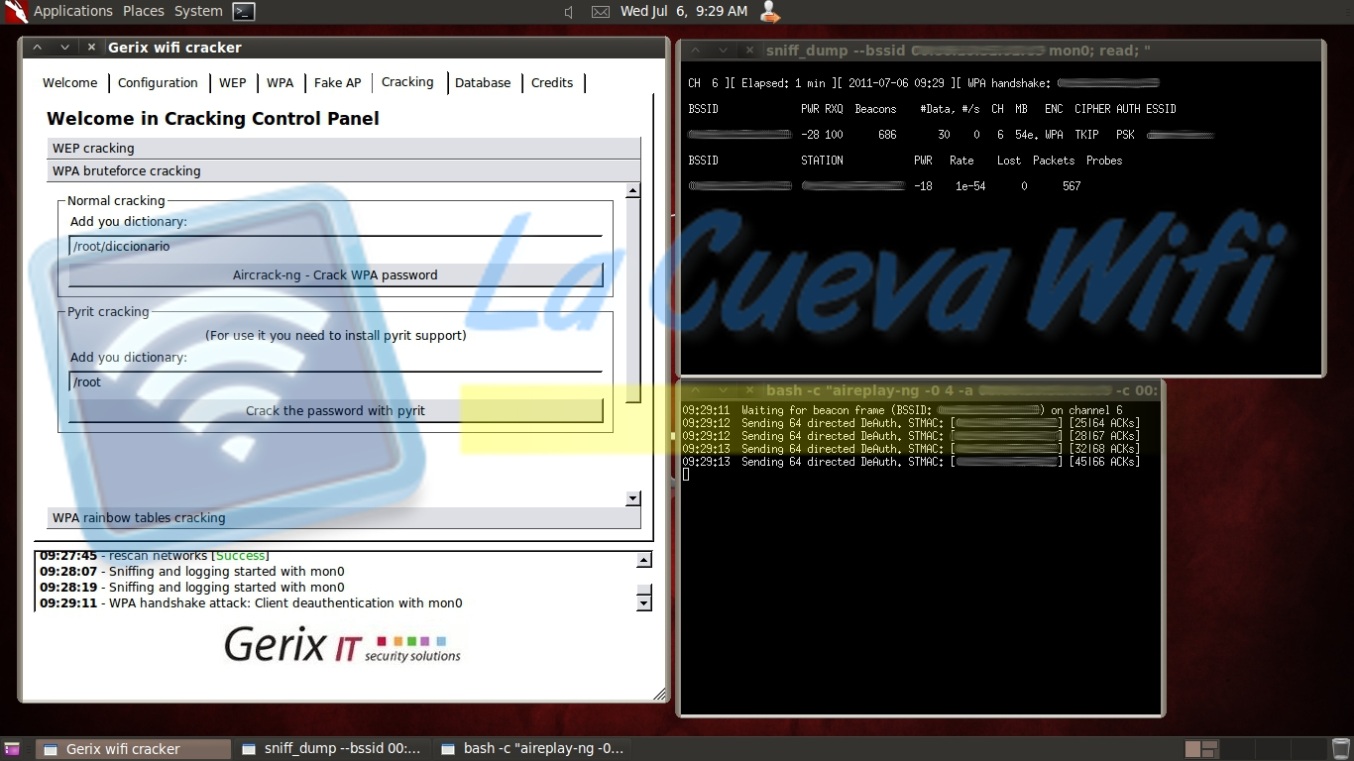
Ahora vamos a obtener un paquete llamado **handshake** que es fundamental para sacar la clave. Para conseguirlo pulsamos en **Autoload victim clients**. Si tenemos un cliente asociado al punto de acceso nos saldrá su MAC en este cuadro. Es imprescindible tener un cliente conectado para obtener el handshake.

Ahora vamos a desautenticar al cliente que está conectado para obtener el handshake. Pulsamos en **client desauthentication**. Se nos abrirá otro terminal que muestra como inyecta paquetes para desautenticar al cliente.

[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa7.jpg)

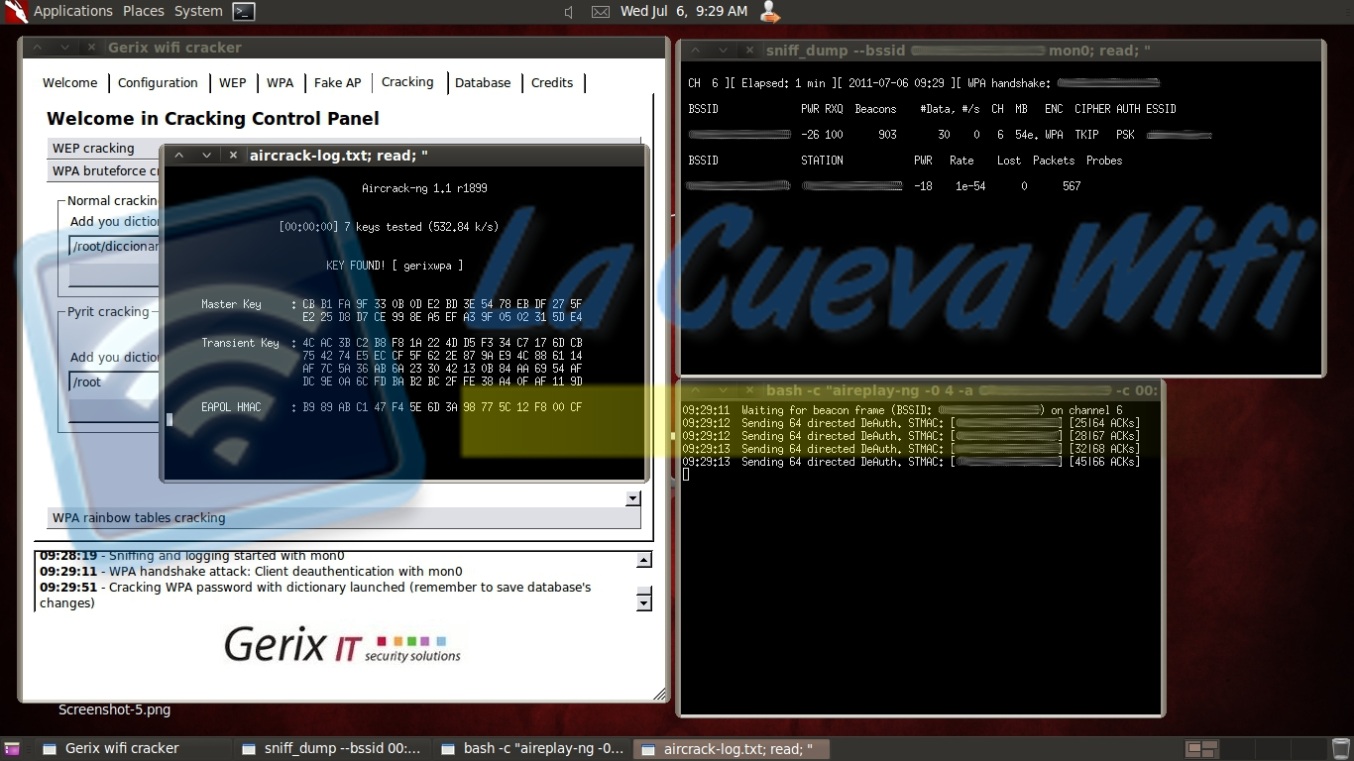
Para saber si hemos obtenido el handshake miramos el primer terminal, en la parte superior derecha tiene que aparecer WPA handshake y la MAC.

Para terminar nos dirigimos a la pestaña **cracking** y pulsamos en **WPA bruteforce cracking.**

[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa8.jpg)

Ahora tenemos que indicar la ruta del diccionario que usaremos para descifrar la clave. La ruta la ponemos en: **Add your dictionary**

Solo nos queda pinchar en **Aircrack-ng – Crack WPA Password**

[](http://www.lacuevawifi.com/wp-content/uploads/2011/07/gerixwpa9.jpg)

Si el ataque tiene éxito nos saldrá una tercera terminal con la clave.