

INDICE

1. Agradecimientos

2. Como Funciona

2.1 Funcionamiento para el tipo D-LINK

2.2 Funcionamiento para el tipo ADSL_XX

2.3 Funcionamiento para el tipo ADSLXXXX

2.3.1 Como crear el diccionario

2.3.2 Como recuperar el passphrase usando una clave

2.3.3 Como recuperar la clave a partir del passphrase

2.3.4 Como usar este diccionario

2.4 Funcionamiento para el tipo SPEEDTOUCH

Agradecimientos

Quería agradecer a todos los que colaboraron con este proyecto y muy especialmente a los creadores de los fuentes de los cuales obtuve gran parte del código necesario para mi aplicación:

Kevin Devine → Creador del fuente para el **SpeedTouch**

ska1ix → Creador del fuente para el **adslXXXX Decsagem 0.1**

Nilp0inteR y ***dudux** → Creadores del fuente del **wlandecrypter**

Buckynet → Creador del fuente del **JazztelDecrypter**

Pianista y **hodgar** → Creadores del fuente para linux del **dlinkdecrypter**

Y a mis amigos **Guan de Dio** que me ayudó muchísimo con todos los problemas y dudas que se me presentaron y **Shaddy** que también me aclaró dudas que se me presentaron.

Creo que no me dejo a nadie atrás pero si es así espero que me perdone jejeje.

Como Funciona

Al arrancar el programa vemos esto:



Si le damos a la lista desplegable veremos 3 opciones a elegir (para los diferentes tipos de routers con los que trabaja este programa):



Para usar este programa lo primero es elegir un tipo de los de la lista.

Funcionamiento para el tipo D-LINK

Simplemente elegimos ese tipo en la lista desplegable y escribimos el BSSID como se muestra en la imagen y hacemos clic en el botón “Sacar WEP”:



Y, como vemos, nos muestra abajo las 3 posibles claves para ese BSSID. Sólo quedaría ver cual de las 3 es, siempre y cuando no haya sido cambiada la que trae por defecto.

Funcionamiento para el tipo ADSL_XX

Esta función sirve para obtener por diccionario la clave WEP de los ESSID tipo ADSL_XX con los siguientes tipos de BSSID:

MODELO	PATRONES DE INICIOS DE MACS			
Comtrend_2008	00:19:15			
Comtrend 535	00:03:C9			
Comtrend_536+	00:16:38	00:1D:20	00:30:DA	
Comtrend_DSL	00:1A:2B			
P-660HW-D1	00:13:49			
Xavi 7768r	00:01:38			
Z-com	00:60:B3			
ZyGate	00:02:CF			
Zyxel 650HW/660HW	00:A0:C5			
Zyxel_660hw	00:19:CB			

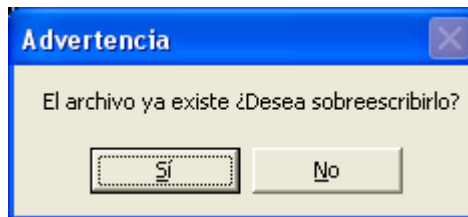
Si el BSSID no comienza como ninguno de los que están en la tabla no nos servirá este programa y veremos este mensaje que nos avisa de ello:



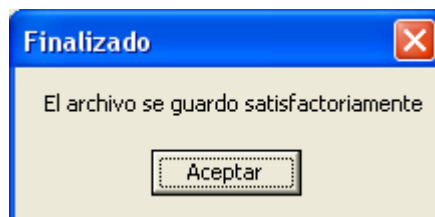
Simplemente metemos el BSSID y el ESSID correctamente y elegimos el nombre de archivo donde se guardará el diccionario que se creará y hacemos clic en el botón Crear diccionario.



Si el archivo existe nos preguntará si deseamos sobrescribirlo:



Y si no existe y todo salió bien nos dirá esto:



Y veremos algo así en la ventana del programa:



Una vez tenemos el diccionario creado, para obtener la clave correcta necesitamos capturar paquetes con el airodump y obtener al menos 5 IVS.

Ahora hay que usar estos dos comandos en Wifislax:

```
airodump-ng -w captura -c canal wlan0  
aircrack-ng -b BSSID -w diccionario.txt capturacon5ivs.ivs
```

Ejemplo:

```
airodump-ng -w captura -c 6 wlan0  
aircrack-ng -b 00:1A:2B:33:44:55 -w Diccionario.txt captura.cap
```

Ahora solo queda esperar a que el aircrack nos diga cual es la clave correcta.

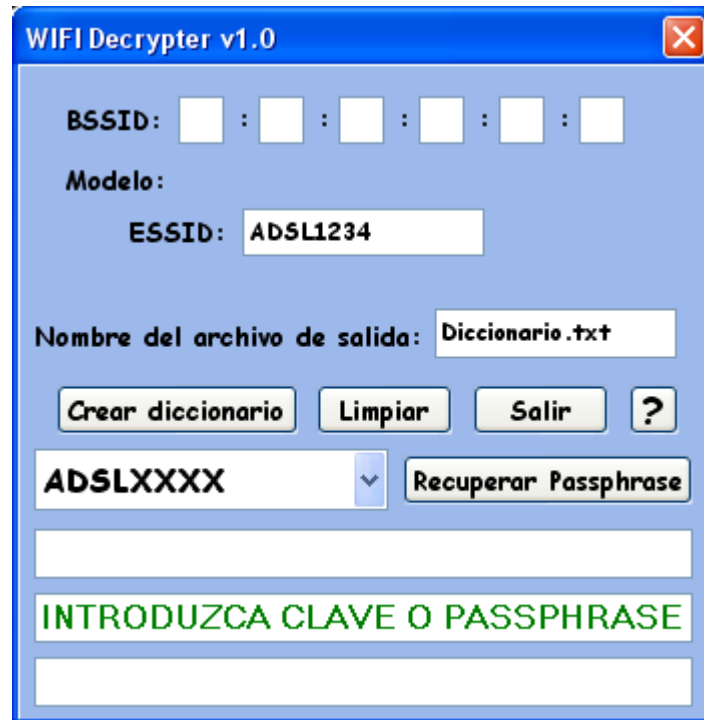
Funcionamiento para el tipo ADSLXXXX

Este es algo más lioso pero veréis que una vez explicado como funciona este apartado es muy fácil de usar. Al elegir ese tipo veremos esto:

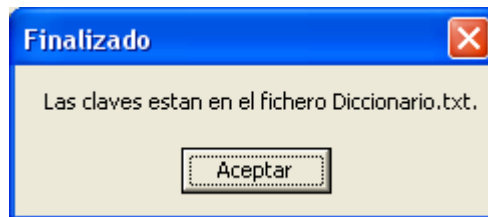


Como crear el diccionario

En este caso no necesitamos introducir el BSSID, solo el ESSID y el nombre del archivo donde se guardará el diccionario.



Hacemos clic en “Crear diccionario” y nos saldrá esto si todo salió bien:



Como recuperar el passphrase usando una clave

En este caso vamos a recuperar el passphrase desde el cual se obtuvo la clave que tenemos. Para ello necesitamos la clave y el ESSID.

Usare la clave: **F0:6B:B0:66:83:25:8F:57:FC:A2:6E:8B:D6**

Y el ESSID con el que obtuve esa clave que es ADSL1234.

Introducimos la clave en el lugar que vemos que nos la pide pero la introducimos sin los “:” como se muestra en la imagen:



Hacemos clic en el botón “Recuperar Passphrase” y veremos esto si todo salio bien:



Como recuperar la clave a partir del passphrase

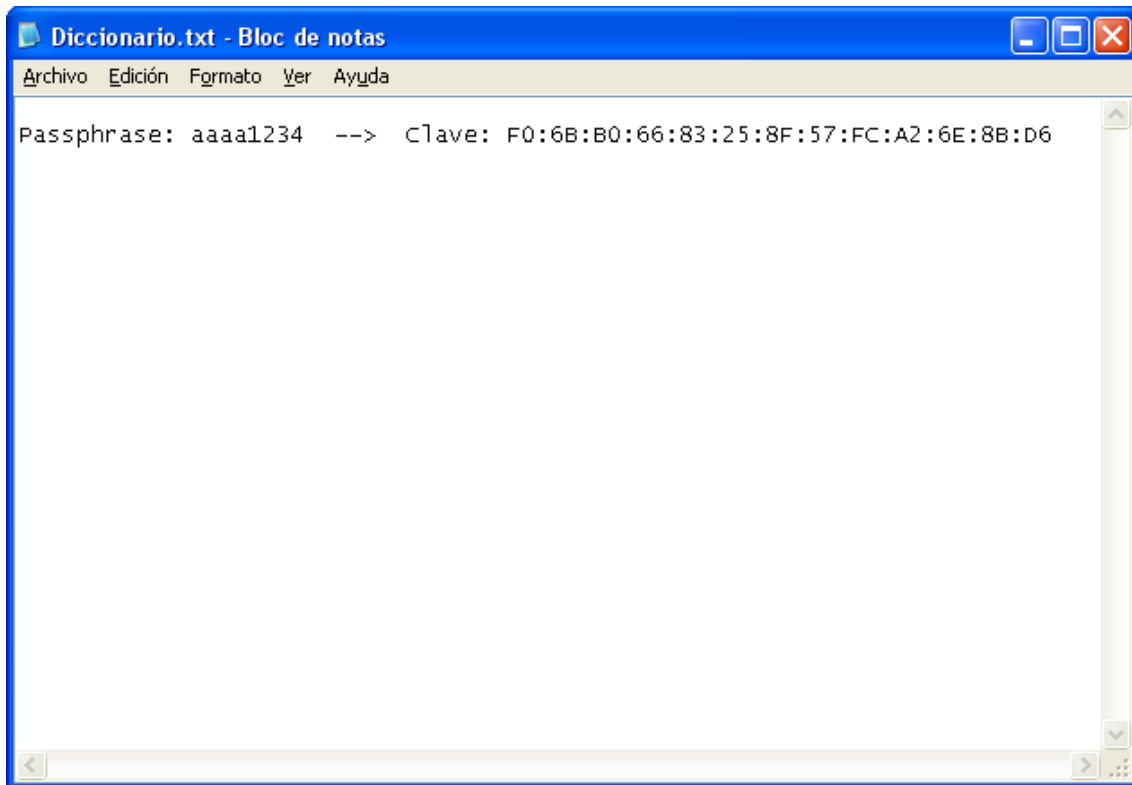
En este caso necesitaremos sólo el nombre de archivo donde se guardarán los datos y el passphrase del cual queremos saber la clave.



Hacemos clic en el botón “Recuperar Clave” y veremos esto si todo salió bien:



Ahora simplemente abrimos el archivo donde se guardó la clave, que en este caso sería “Diccionario.txt” y que está en el directorio del programa y veremos algo así:



Como usar este diccionario

Hay que usar estos dos comandos en Wifislax:

```
airodump-ng -w captura -c canal wlan0  
aircrack-ng -b BSSID -w diccionario.txt captura.ivs
```

Ejemplo:

```
airodump-ng -w captura -c 6 wlan0  
aircrack-ng -b 00:11:22:33:44:55 -w Diccionario.txt captura.cap
```

Ahora sólo queda esperar a que el aircrack nos diga cual es la clave correcta.

Funcionamiento para el tipo SPEEDTOUCH

Este apartado sirve para la recuperación de la clave WEP/WPA que traen por defecto los Routers Thomson modelos 580i y 585v6.

El funcionamiento del programa para este tipo es muy sencillo, simplemente tenemos que introducir el ESSID y dar a Obtener claves y nos guardará un diccionario con el nombre que le especifiquemos donde estarán todas las posibles claves para ese ESSID y también nos guardará un archivo llamado "posibles claves.txt" en el cual estarán las mismas claves pero con una breve descripción.

Veámoslo en funcionamiento:

Elegimos el tipo SPEEDTOUCH y veremos esta ventana:



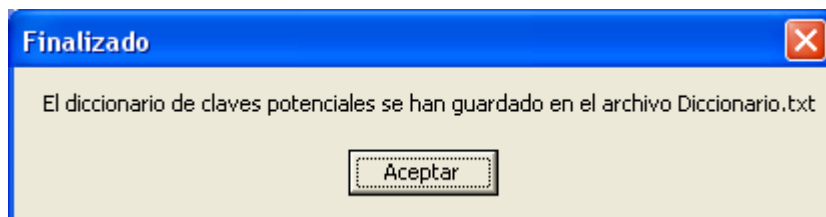
Introducimos el ESSID del cual queremos obtener las claves:



Por lo que he leído, este método sirve también para el tipo TomsonXXXX, TomsonXX, SpeedTouchXX y SpeedTouchXXXX así que si lo quieren usar para este tipo, si por ejemplo el ESSID es Tomson1234, tendréis que poner SPEEDTOUCH1234.

Este método sirve sólo para los ESSIDs con un largo de valores pares, es decir SPEEDTOUCH12, SPEEDTOUCH1234, SPEEDTOUCH123456, los de largo impar los he descartado porque de momento no conozco ningún ESSID que tenga esos caracteres impares y además si metiésemos uno impar el programa se volvería loco y empezaría a crear claves como un poseso. Este bug no es cosa mia, hagan la prueba en el que esta para consola y verán que pasa, así que mejor acabar con ese bug así ya que tampoco se como solucionarlo para que los admita sin volverse loco.

Una vez introducido el ESSID hacemos clic en el botón "Obtener Claves" y, pasados unos segundos (en mi caso unos 40 segundos), veremos esto:



Y esto:



Y si vemos los archivos que creó veremos esto:

