

Desencriptar clave WPA con Wifislax



Hello everybody! A continuación nos disponemos a desencriptar una clave WPA con [Wifislax](#).

Es importante saber el tipo de antena de nuestro PC, en nuestro caso es [Qualcomm Atheros AR242x / AR542x](#).

El tipo de antena y su alcance es crucial para hacer un ataque eficiente.

El router que hemos utilizado para esta prueba es de Telefónica fibra óptica Comtrend 5813.

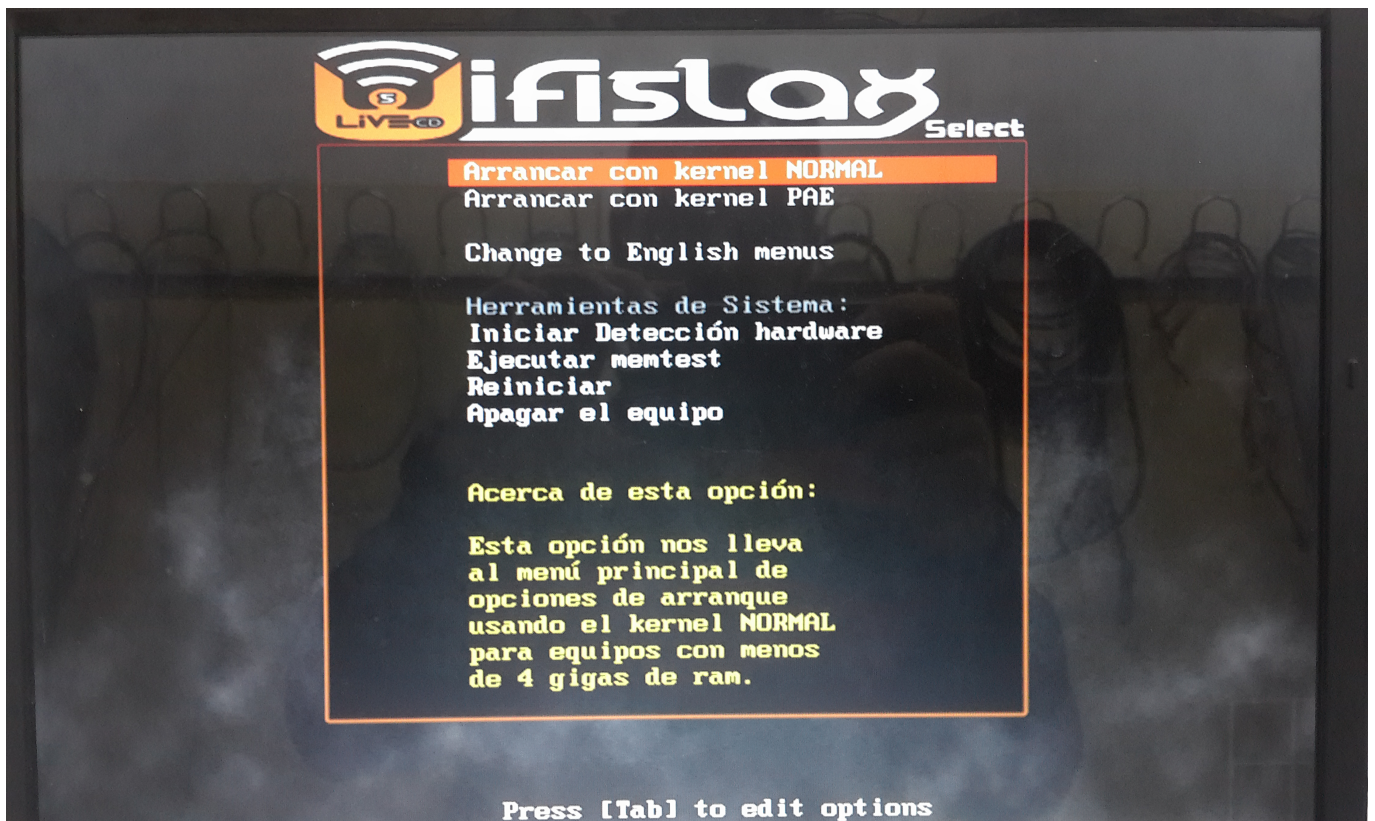


[Manual router](#)

Arrancamos el CD LIVE

Primero insertamos el CD, (la BIOS tiene que estar configurada para que el ordenador arranque desde un CD).

En el primer menú elegimos la primera opción, "arrancar con Kernel NORMAL".



```
* Buscando fichero de firma wifislax.sgn
* Usando datos desde /mnt/sr0/wifislax
* No se utilizara la opcion cambios persistentes
* Creando sistema de ficheros live e insertando modulos.
O.K -> 000-kernel-3.12.xzm
O.K -> 001-core.xzm
O.K -> 002-xorg-drivers.xzm
O.K -> 003-desktop-depends.xzm
O.K -> 004-kde-4.10.5.xzm
O.K -> 005-devel.xzm
O.K -> 006-wifislax-desktop.xzm
O.K -> 007-Firefox-25.0.1.xzm
O.K -> 008-aplicaciones-wireless.xzm
O.K -> 009-jre-7u45-1586-1sw.xzm
O.K -> 012-install_grub2_v5.xzm
* Copiando el contenido del directorio /mnt/sr0/wifislax/rootcopy
* Pivotando a directorio root
Sistema live listo - Iniciando Wifislax
INIT: version 2.88 booting
[+] Starting udevd: /sbin/udev --daemon
[+] Triggering udev events: /sbin/udevadm trigger --action=add
[+] Fuse filesystem already available.
[+] Fuse control filesystem already available.
[+] Testing root filesystem status: read-write filesystem
[+] Mounting non-root local filesystems:
INIT: Entering runlevel: 4
[+] Going multiuser...
[+] Auto Configure IP address for eth0: /sbin/dhccpd -t 60 eth0 &
[+] Auto Configure IP address for wlan0: /sbin/dhccpd -t 60 wlan0 &
[+] Activating IPv4 packet forwarding.
[+] Updating icon-theme.cache in /usr/share/icons/hicolor...
[+] Starting ACPI daemon: /usr/sbin/acpid
[+] Updating MIME database: /usr/bin/update-mime-database /usr/share/mime &
[+] Starting system message bus: /usr/bin/dbus-uuidgen --ensure ; /usr/bin/dbus-daemon --system
```

Acabada la instalación.



Escritorio de Wifislax

Este es el escritorio de nuestro programa.



Pasos a seguir

Damos a inicio, wifislax > wpa wps > Goscript WPS.



Preparando el ataque

1. La tarjeta interfaces de tu PC se activa en modo monitor.



```
goyscript : goyscript : - Konsola
GOYscript 3.4-beta4 by GOYfilms

Distribución de linux detectada: Wifislax
Tarjetas WiFi disponibles:

Nº   INTERFAZ   DRIVER   FABRICANTE
1)   wlan0      ath5k    ASKEY COMPUTER CORP

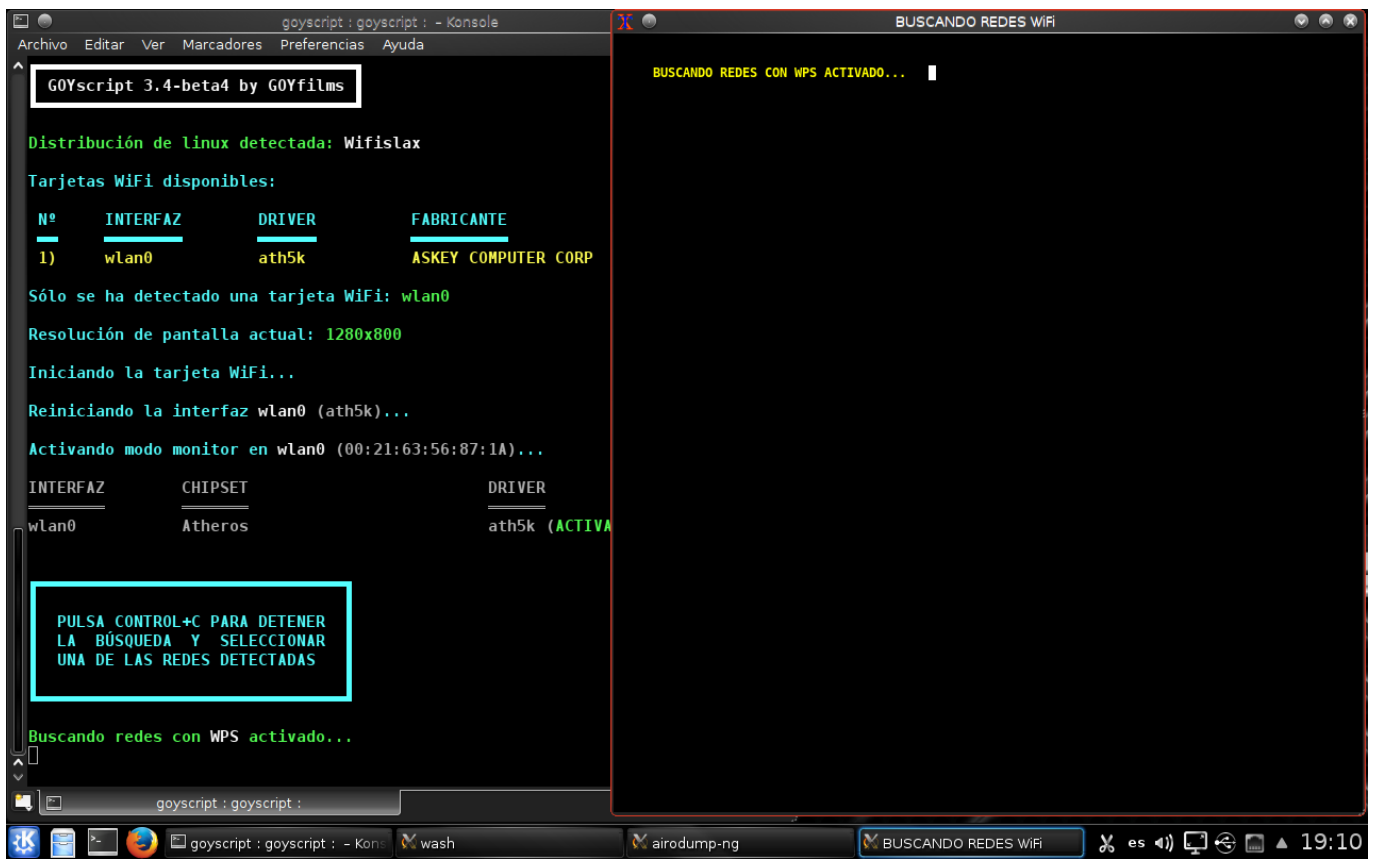
Sólo se ha detectado una tarjeta WiFi: wlan0
Resolución de pantalla actual: 1280x800
Iniciando la tarjeta WiFi...
Reiniciando la interfaz wlan0 (ath5k)...
Activando modo monitor en wlan0 (00:21:63:56:87:1A)...

INTERFAZ   CHIPSET   DRIVER
wlan0      Atheros   ath5k (ACTIVADO en mon0)

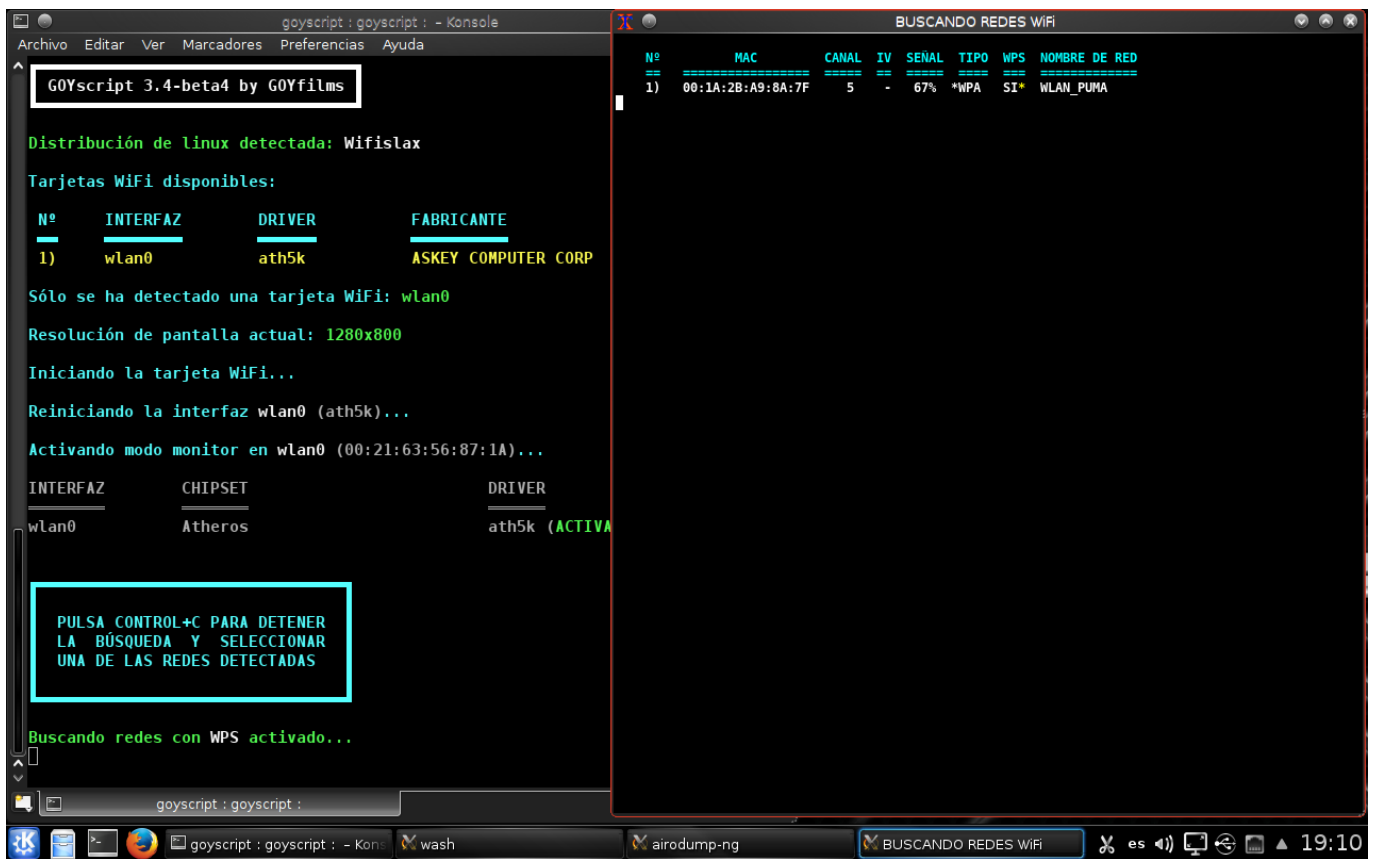
PULSA CONTROL+C PARA DETENER
LA BÚSQUEDA Y SELECCIONAR
UNA DE LAS REDES DETECTADAS

Buscando redes con WPS activado...
```

2. Automáticamente se abre una ventana paralela buscando las redes wifi con contraseña WPS.



3. Sale un lista con las redes a nuestro alcance con clave WPS.



Al ataque!!

Control +c para cerrar la ventana paralela y te sale un listado con los routers a romper, en nuestro caso solamente encuentra una y automáticamente lanza el ataque.



```
goyscript : goyscript : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

  N#      MAC          CANAL  IV  SEÑAL  TIPO  WPS  NOMBRE DE RED
  ---  -
  1)  00:1A:2B:A9:8A:7F    5     -   67%   *WPA  SI*   WLAN_PUMA

RESUMEN

INTERFAZ:
Nombre.....: wlan0
Modo monitor...: mon0
MAC.....: 00:21:63:56:87:1A
Fabricante.....: ASKEY COMPUTER CORP

PUNTO DE ACCESO:
Nombre.....: WLAN_PUMA
MAC.....: 00:1A:2B:A9:8A:7F
Canal.....: 5
Encriptación...: WPA-CCMP (WPS activado)
Fabricante.....: Ayecom Technology Co., Ltd.

GOYscriptWPS 3.4-beta4 by GOYfilms

Atacando la red WLAN_PUMA...
Iniciando ataques con pin específico...
Probando pin 11110392 generado por WPSPinGeneratorMOD... []

Atacando la red "WLAN_PUMA"
[+] Fijando mon0 en el canal 5
[+] Esperando beacon de 00:1A:2B:A9:8A:7F
[+] Asociado con 00:1A:2B:A9:8A:7F (ESSID: WLAN_PUMA)
[+] Probando pin 11110392
[+] Enviando solicitud WPS [EAPOL_START]
[+] Recibida solicitud de identidad
[+] Enviando respuesta de identidad
```

Resultado del ataque

En este caso lanza un ataque con tres pin conocidos en la base de datos, el primer pin da fallo o pin incorrecto y el segundo vemos que nos da la contraseña.



Vídeo demostrativo del ataque

<html> <head>

```
<meta charset="utf-8" />  
<title>Vídeo demostrativo del ataque</title>
```

</head> <body>

```
<h2>Video demostrativo del ataque</h2>  
<video controls>  
  <source  
src="http://www.mediafire.com/download/skdn0dovp4m2725/Video_ataque_Wifislax  
.mp4">  
  <track label="Subtítulos en español" kind="subtitles" srclang="es"  
src="sintel_es.vtt" default>  
</video>
```

</body> </html>

Publicado por:

Hugo Machado y Alfonso Araque alumnos de STI1, con la ayuda de J.C. Ballesteros.

From:
<http://server-jk.ddns.net/dokuwiki/> - IES Palomeras-Vallecas Dep. Electronica

Permanent link:
http://server-jk.ddns.net/dokuwiki/doku.php?id=aula:redes:haking:como_desencriptar_una_clave_wpa2_con_wifislax

Last update: 2025/01/22 02:02

