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.

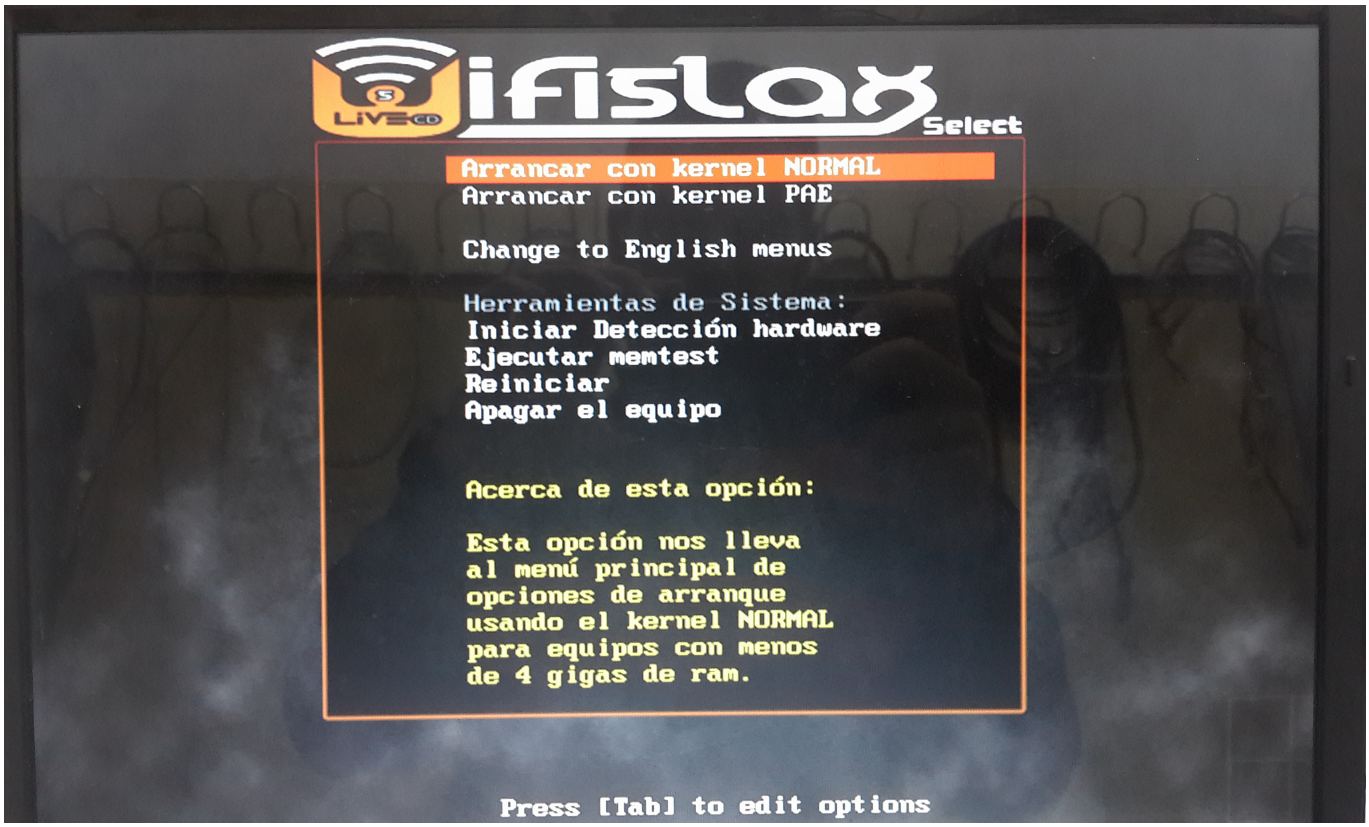


Manual router

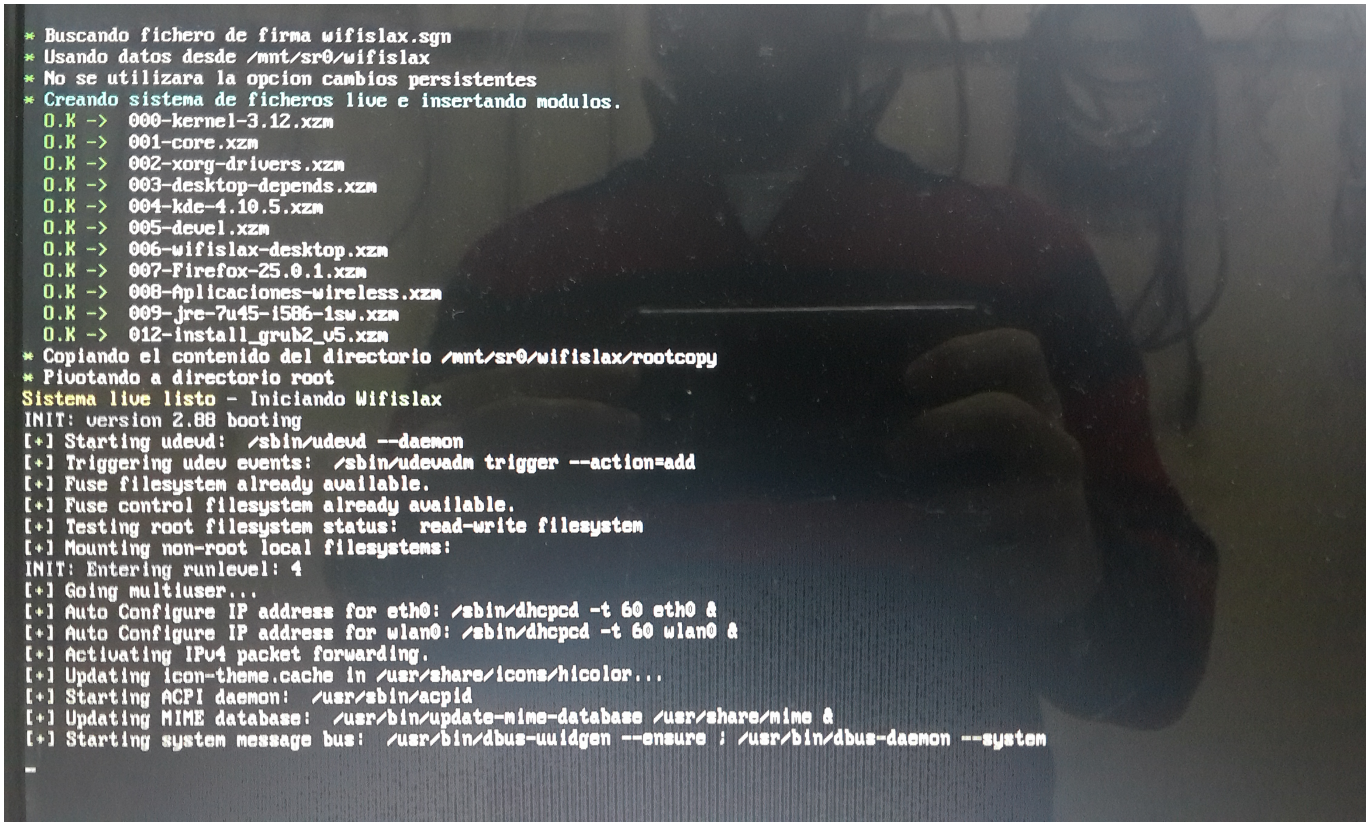
Arrancamos el CD LIVE

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”.







Acabada la instalación.



Escritorio de Wifislax

Este es el escritorio de nuestro programa.



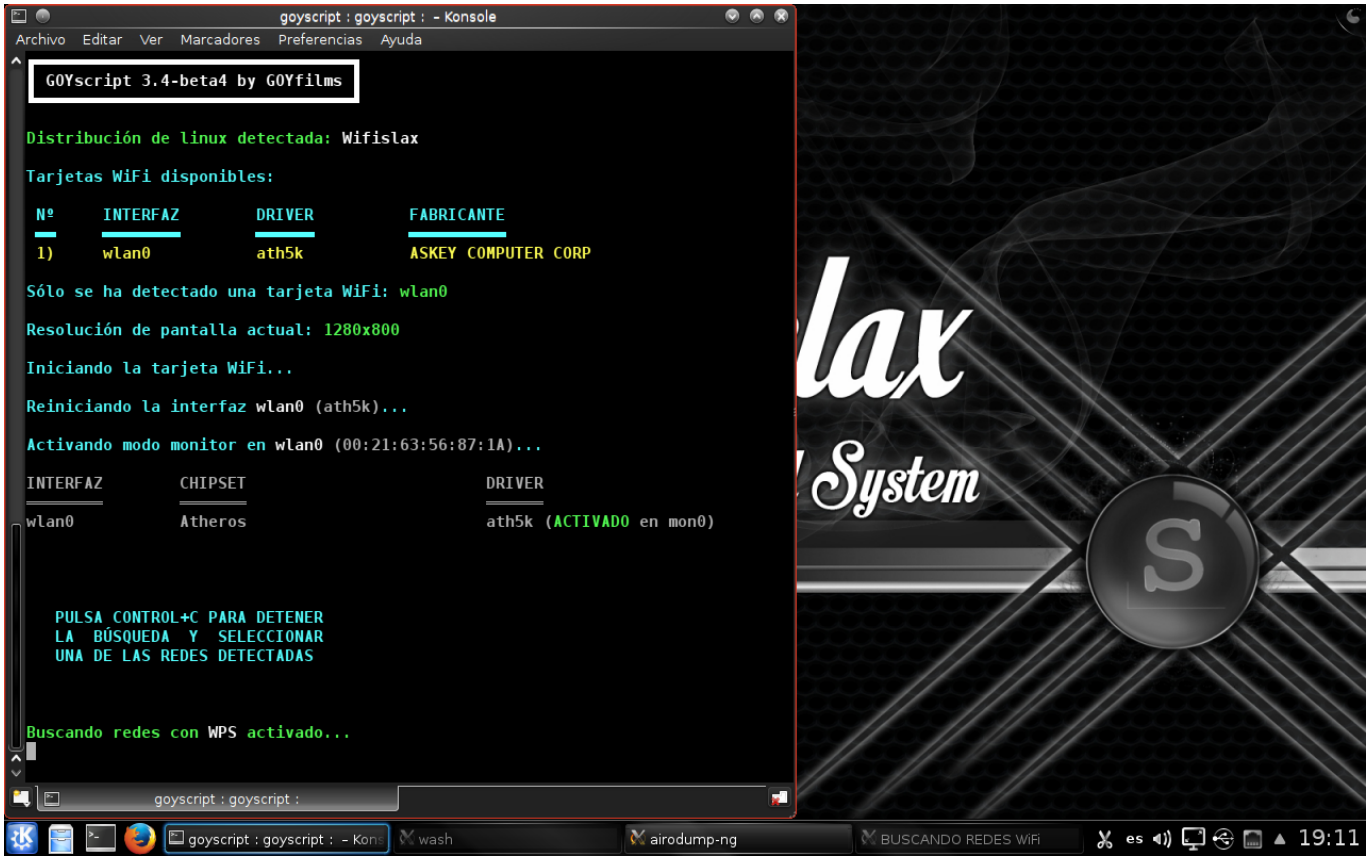
Pasos a seguir

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

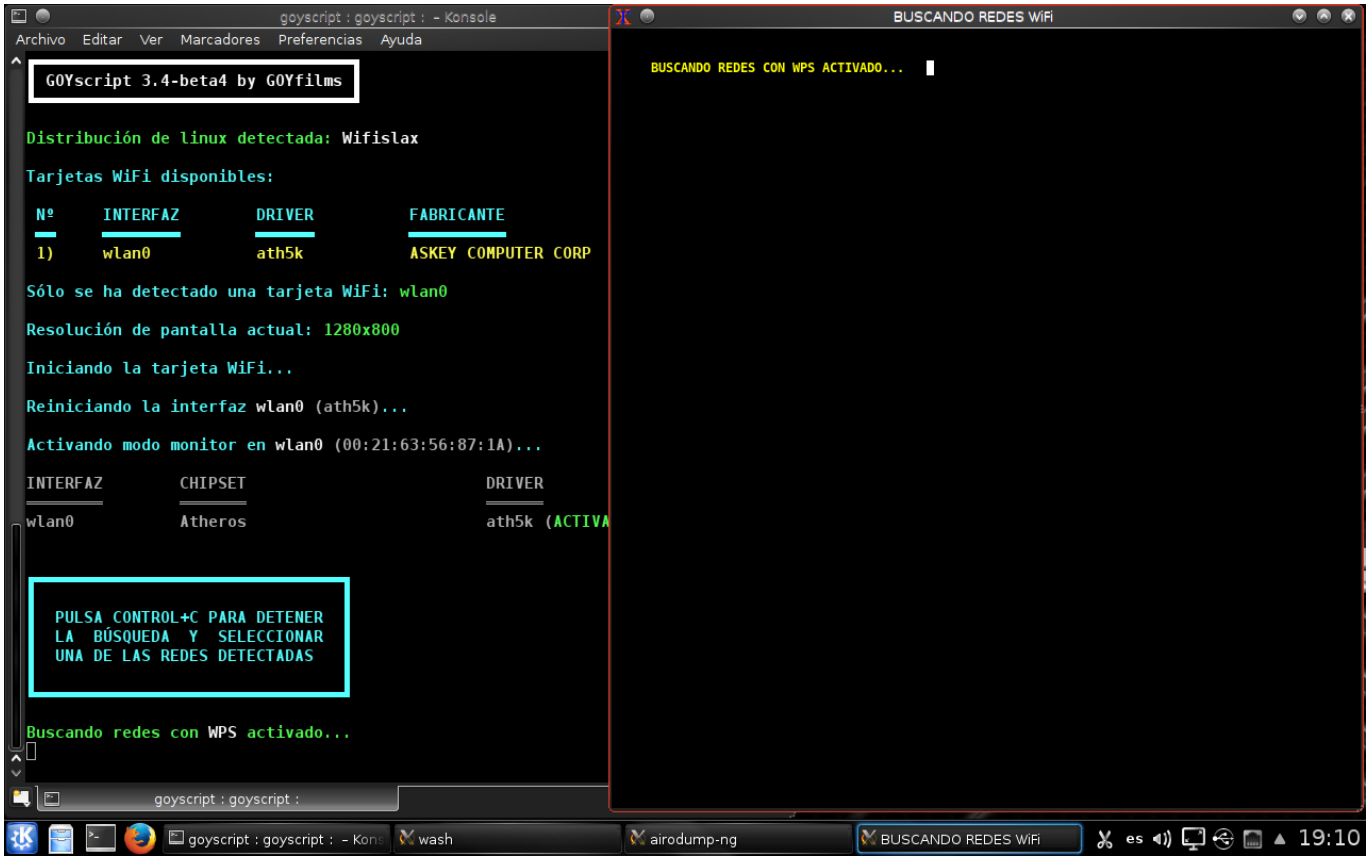


Preparando el ataque

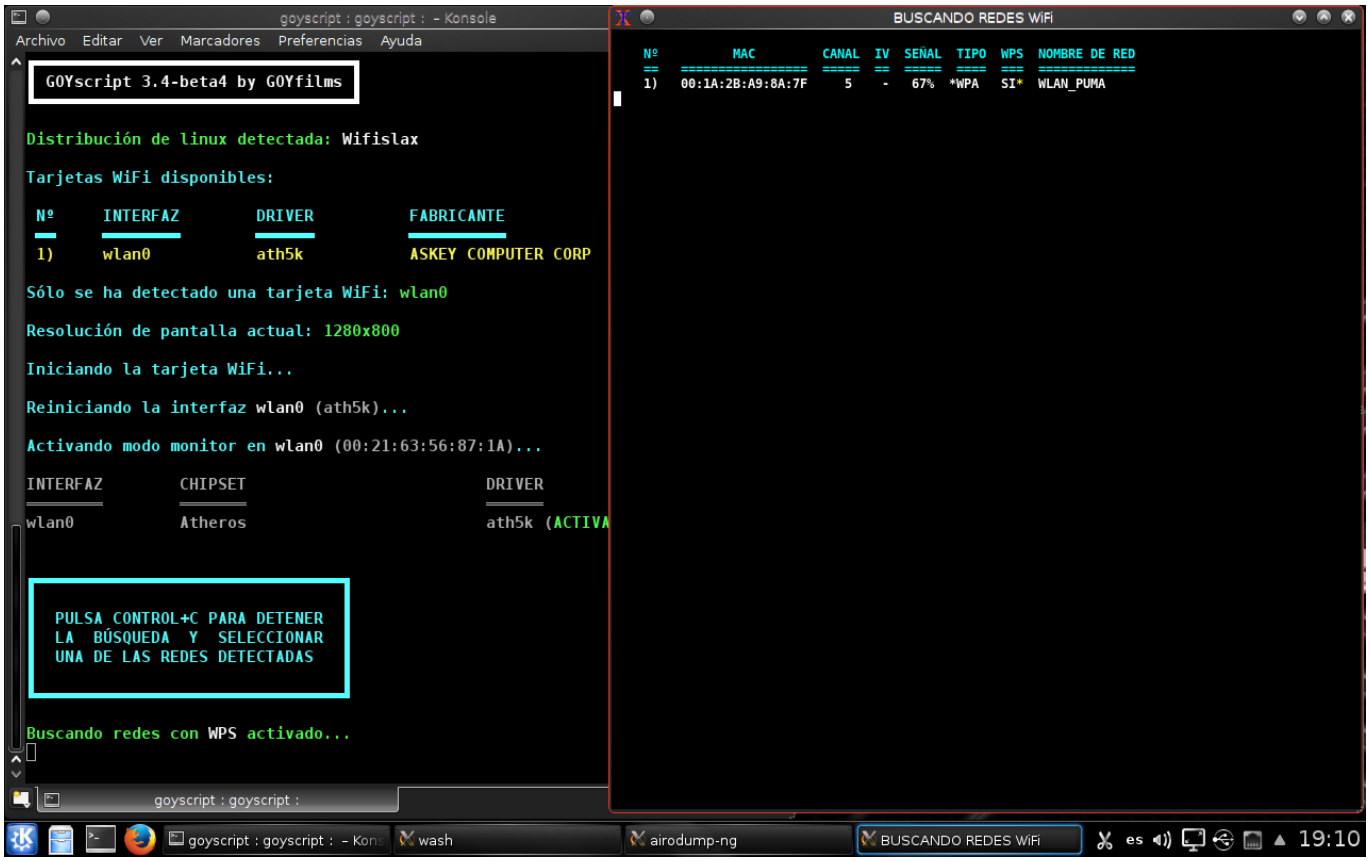
1. La tarjeta interfaces de tu PC se activa en modo monitor.



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

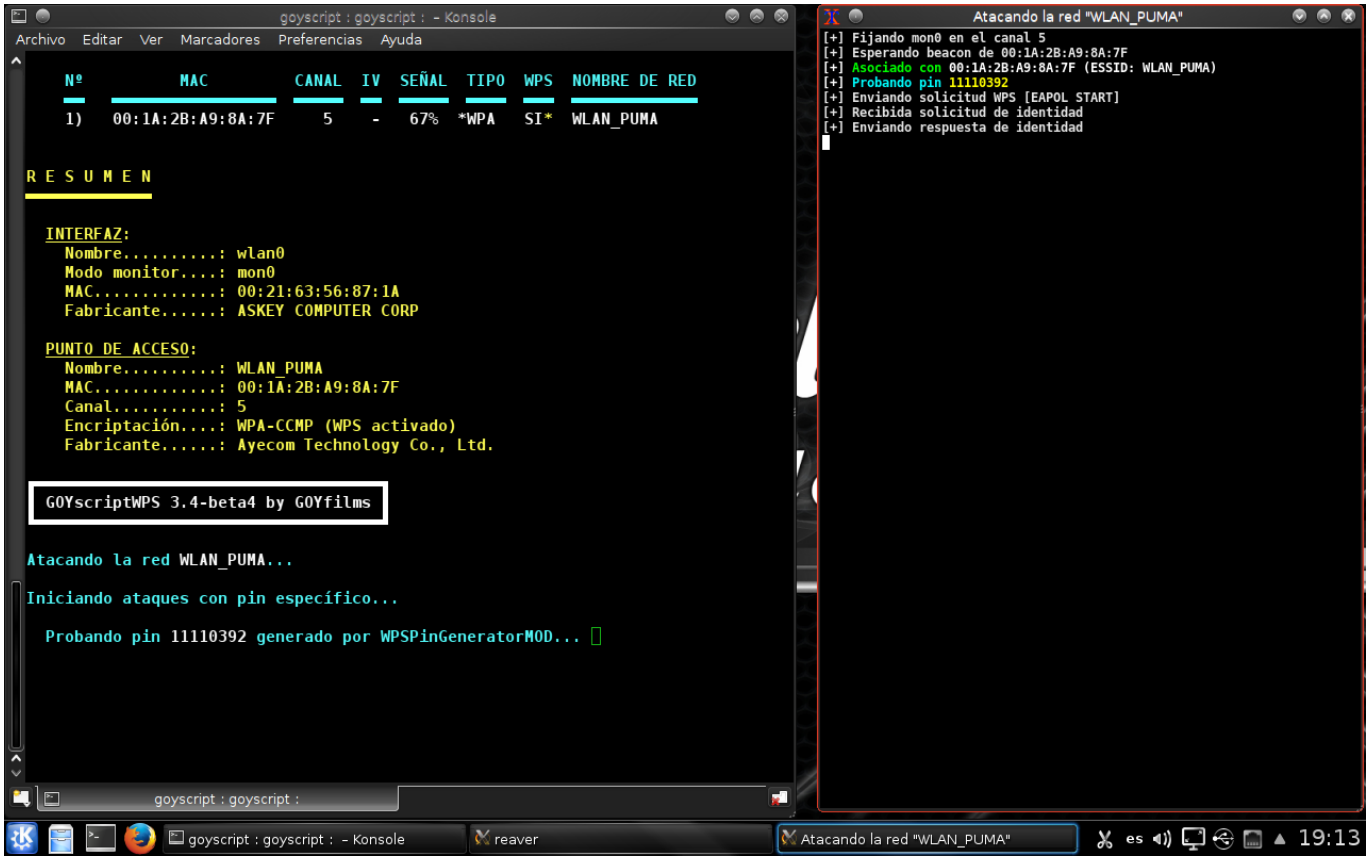


3. Sale un lista con las redes a nuestro alcance con clave WPS.



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.



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:
https://server-jk.ddns.net/dokuwiki/ - **IES Palomeras-Vallecas Dep. Electronica**

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

Last update: **2025/01/22 01:02**