

## Especialización: Tecnologías de la Información

- CETI1: Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.
- CETI2: Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.
- CETI3: Capacidad para emplear metodologías centradas en el usuario y la organización para el desarrollo, evaluación y gestión de aplicaciones y sistemas basados en tecnologías de la información que aseguren la accesibilidad, ergonomía y usabilidad de los sistemas.
- CETI4: Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.
- CETI5: Capacidad para seleccionar, desplegar, integrar y gestionar sistemas de información que satisfagan las necesidades de la organización, con los criterios de coste y calidad identificados.
- CETI6: Capacidad de concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación móvil.
- CETI7: Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

## Actividad: Pasos para obtener la clave WiFi de un router

Esta actividad nos servirá por ejemplo, para comprobar la fiabilidad de nuestro router o en el caso de no poder acceder a él, poder abrir una “puerta” para hacerlo.

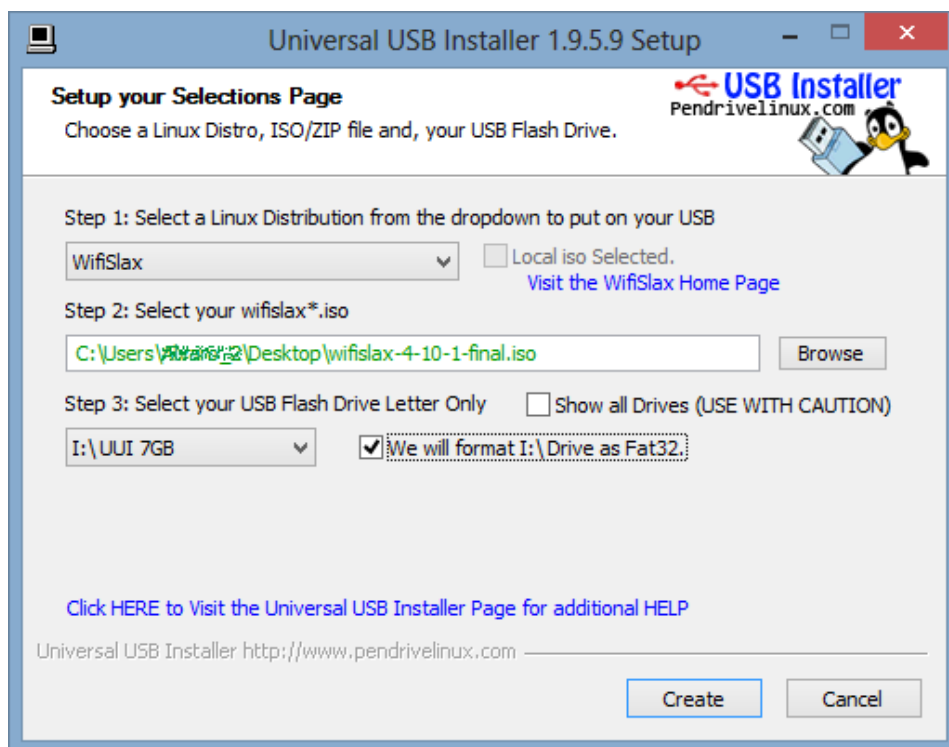
### 1. Descargar WifiSlax

Lo primero que vamos a hacer es [descargar Wifislax desde este enlace](#), son 1,97 Gb.

Lo que has descargado ha sido una imagen ISO. Esta imagen tendrás que cargarla en un Pendrive (Capacidad mínima 4 GB), otra forma de hacerlo con la cual te tendrías que saltar el Paso 2, sería descomprimiendo la imagen ISO en un DVD, y en vez de arrancar el PC desde el USB, lo tendrías que arrancar desde la unidad óptica de DVD.

### 2. Configurar pendrive para sacar contraseñas wifi

Para poder arrancar el pc desde el pendrive es necesario cargar la ISO correctamente en nuestro pendrive, para esto vamos a utilizar el programa [Universal USB Installer que podremos descargar desde este enlace](#). Este paso también sirve para instalar [Backtrack](#), [Beini](#) o [Wifiway](#) en un pendrive.



Una vez abierto hacemos lo siguiente:

- **Step 1** (Paso 1) → Seleccionaremos “WifiSlax” al igual que puedes ver en la imagen.
- **Step 2** → Pulsar Browse y seleccionar la ISO que acabais de descargar.
- **Step 3** → Seleccionar la unidad de vuestro Pendrive y marcar la casilla “We will format I:\ Drive as Fat32” para asegurarnos que el Pendrive tendrá el formato correcto (**esta opción borrará toda la información de vuestro Pendrive**)

Una vez hecho esto solo tendrás que pulsar el botón “Create” y esperar unos minutos. Cuando se haya creado la imagen deberemos reiniciar nuestro PC con el pendrive conectado. Y arrancar el Pc desde nuestro pendrive para comenzar a descifrar las claves wifi.

### 3. Arrancar WifiSlax

Una vez arrancado nuestro PC desde el pendrive aparecerán un par de pantallas como la siguiente:



Deberemos pulsar un par de veces INTRO para elegir la primera opción. Y en un minuto ya tendremos cargado WifiSlax.

Si te pide **usuario y contraseña al iniciar WifiSlax**, los datos de acceso son:

Usuario -> **root**

Contraseña -> **toor**

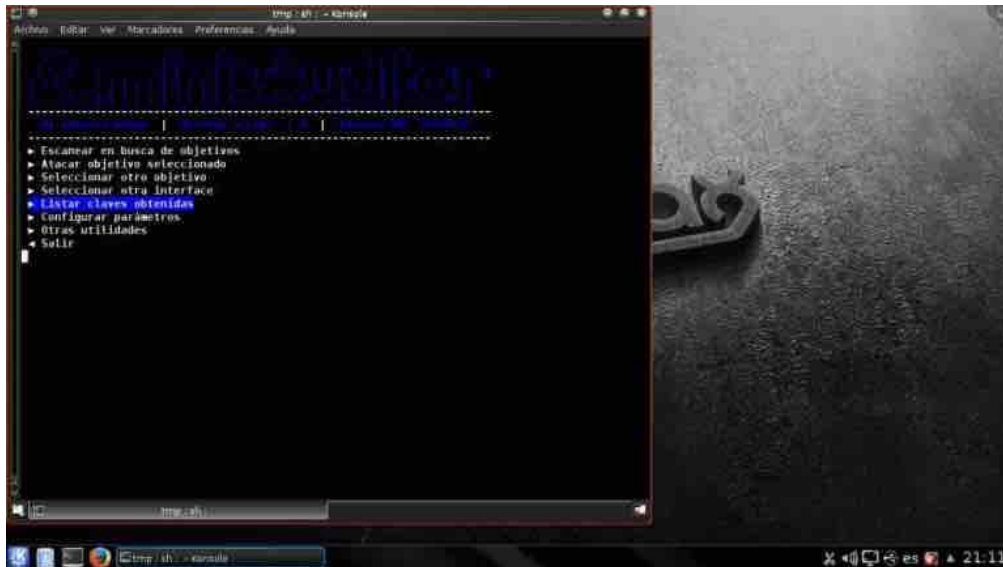
Y nos aparecerá esto:



## 4. Geminis Auditor

Una vez abierto WifiSlax, para conseguir nuestra clave wifi, vamos a utilizar una herramienta que es muy fácil de usar, se llama **Geminis Auditor**. Para abrirla debemos pulsar en el icono azul de la esquina inferior izquierda (es como si fuera el botón de inicio de Windows) y al igual que podéis ver en la imagen superior deberéis ir a WifiSlax -> Wireless -> Geminis Auditor (Todo en uno).

Una vez abierto nos encontraremos con la siguiente ventana:



Moviéndote con las flechas arriba y abajo del teclado, tendrás que seleccionar la primera Opción “Escanear en busca de objetivos” con la tecla INTRO para intentar descifrar tu contraseña wifi.

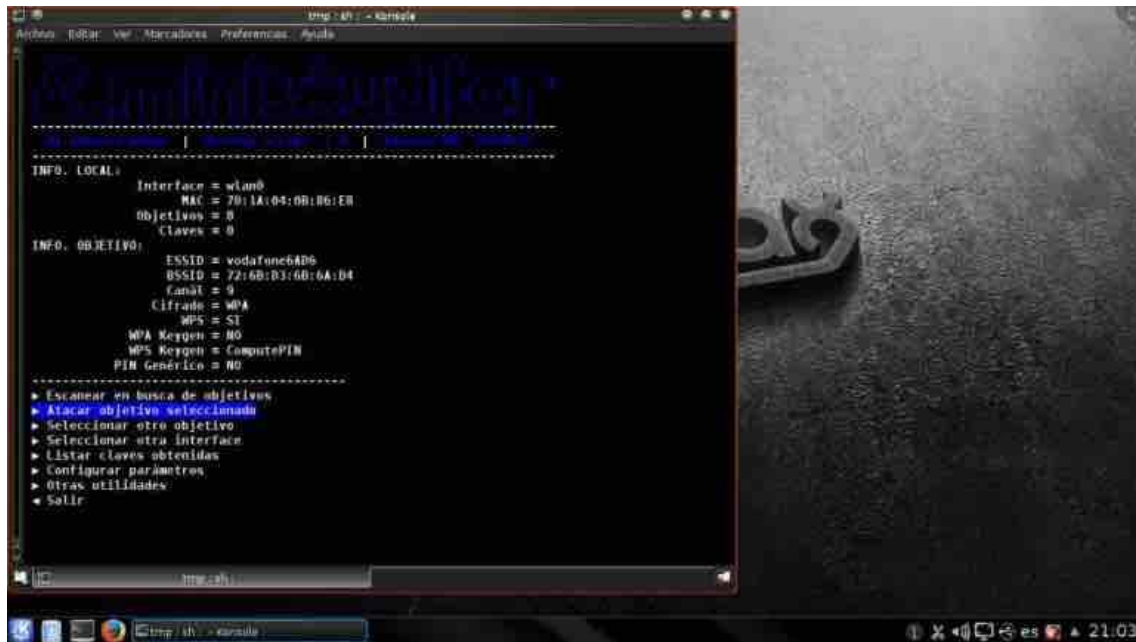
El escaneo tarda 30 segundos en comprobar la seguridad de las redes.

**Sigamos**, una vez escaneado las redes, os saldrá una pantalla similar a esta:



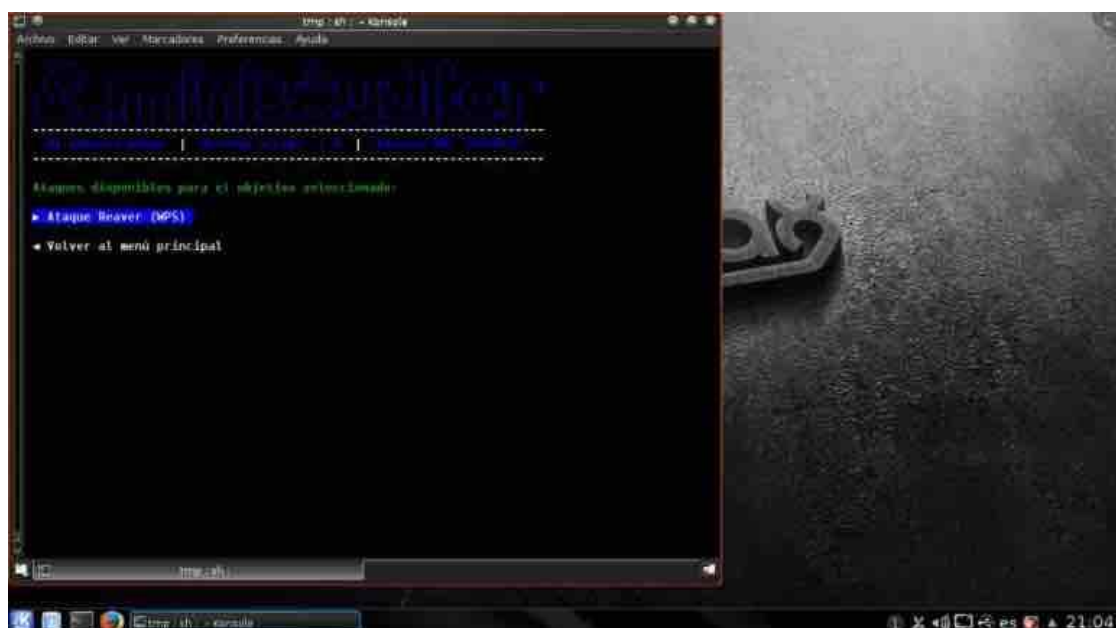
En lo que tenemos que fijarnos es en el color VERDE, en mi red que es la de Vodafone6AD6 si que aparece el color verde, esto quiere decir que la seguridad de mi red es una auténtica porquería y que en menos de 1 minuto cualquier persona que use una herramienta similar a Wifislax va a poder robarme la señal Wifi.

Una vez elegida tu red, tendrás que volver al menú anterior como se ve en la siguiente imagen:

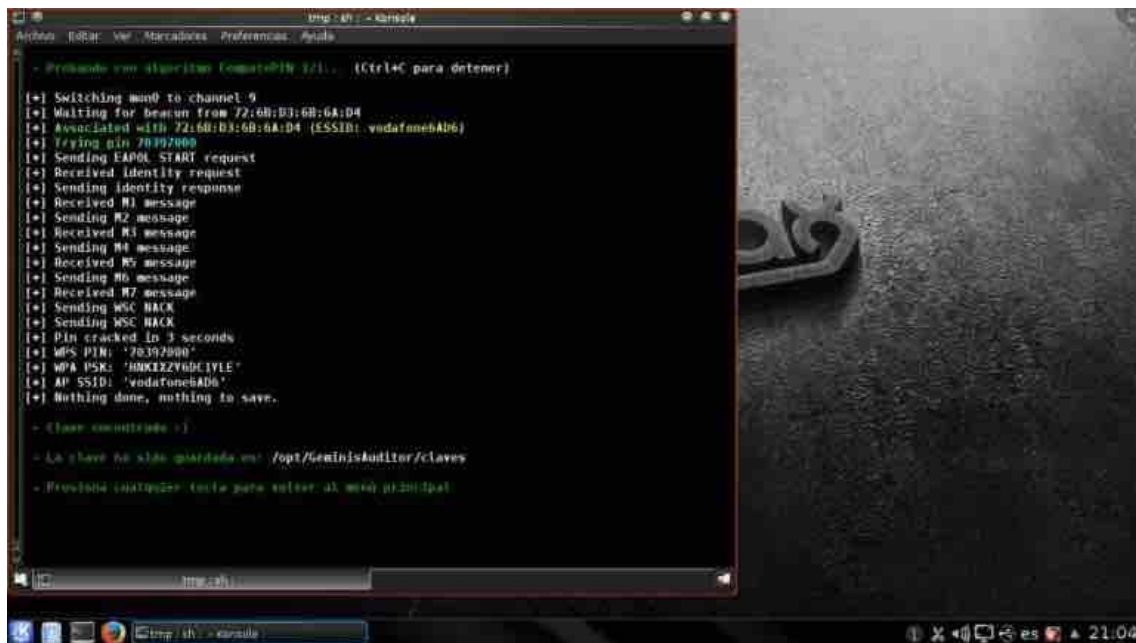


## 5. Ver clave WiFi

El siguiente paso para conseguir tus claves wifi será pulsar sobre la segunda opción: *"Atacar objetivo seleccionado"*, os va a salir otro submenú para que veas el tipo de ataque que se va a hacer. Pulsar intro y empezara a hacer la magia el software para descifrar la clave wifi.



Una vez seleccionada está opción será cuando el software intente descifrar la clave wifi.



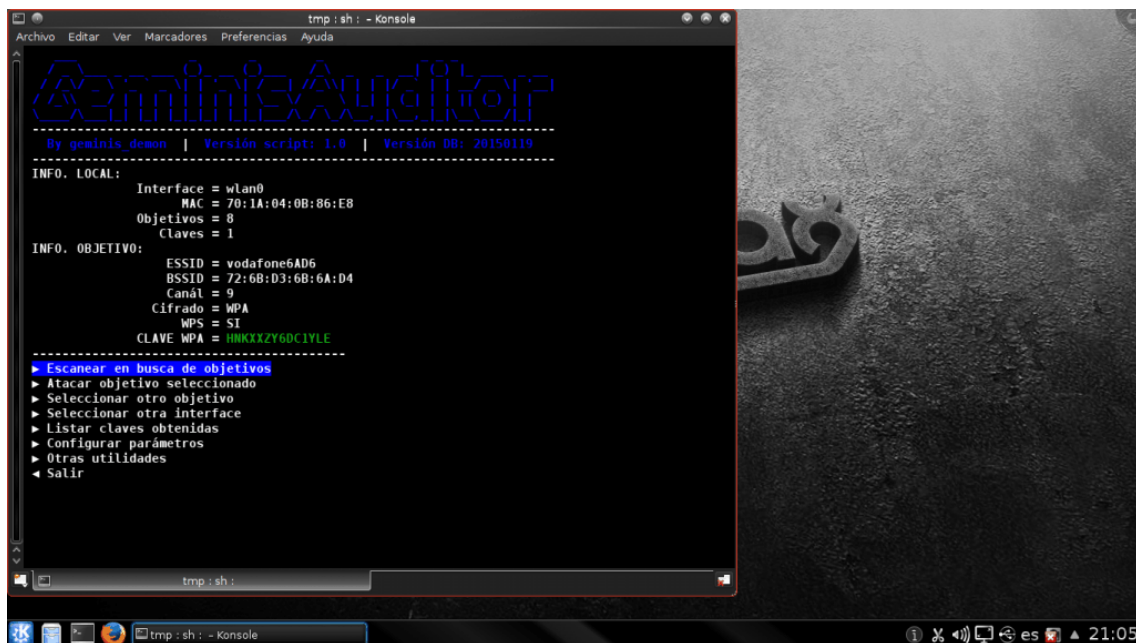
```
tmp: sh: - Konsole
- Probar con algoritmo (Formato PIN 121)... (Ctrl+C para detener)

[+] Switching mudo to channel 9
[+] Waiting for beacon from 72:6B:D3:6B:6A:D4
[+] Associated with 72:6B:D3:6B:6A:D4 (ESSID: vodafoneAD6)
[+] Trying pin 70397000
[+] Sending EAPOL START request
[+] Received Identity request
[+] Sending Identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC HACK
[+] Sending WSC HACK
[+] PIN cracked in 3 seconds
[+] WPS PIN: '70397000'
[+] WPA PSK: 'HNKXXZY6DC1YLE'
[+] AP SSID: 'vodafoneAD6'
[+] Nothing done, nothing to save.

- Cerrar consola: :)
- La clave ha sido guardada en: /opt/GeminisAuditor/claves
- Presiona cualquier tecla para volver al menú principal
```

En mi caso en menos de 30 segundos como puedes comprobar en la imagen anterior ha **descifrado la clave wifi**.

Ahora solo tendrás que presionar cualquier tecla y ya podrás ver la clave Wifi como en la siguiente imagen:



```
tmp: sh: - Konsole
GeminisAuditor
By geminis demon | Versión script: 1.0 | Versión DB: 20150119
-----
INFO. LOCAL:
Interface = wlan0
MAC = 70:1A:04:0B:86:E8
Objetivos = 0
Claves = 1
INFO. OBJETIVO:
ESSID = vodafoneAD6
BSSID = 72:6B:D3:6B:6A:D4
Canal = 9
Cifrado = WPA
WPS = SI
CLAVE WPA = HNKXXZY6DC1YLE
-----
► Escanear en busca de objetivos
► Atacar objetivo seleccionado
► Seleccionar otro objetivo
► Seleccionar otra interface
► Listar claves obtenidas
► Configurar parámetros
► Otras utilidades
◀ Salir
```

**Wifi Clave: HNKXXZY6DC1YLE**

Si también a ti te ha funcionado, deberías cambiar la contraseña del wifi INMEDIATAMENTE de tu Router Wifi.

## Bibliografía

[https://wifibit.com/como-robar-wifi-tutorial-wifislax/#Descargar\\_Version\\_mas\\_reciente\\_de\\_WifiSlax](https://wifibit.com/como-robar-wifi-tutorial-wifislax/#Descargar_Version_mas_reciente_de_WifiSlax)

<http://cvnet.cpd.ua.es/webcvnet/planestudio/planEstudioND.aspx?plan=C203&lengua=C#>