

¿En qué consiste el Wardriving? El término wardriving se deriva de su antecesor el wardialing, pero aplicado a redes inalámbricas. El hacker entabla una guerra inalámbrica desde las inmediaciones del objetivo, usualmente parqueado desde su auto con una laptop y una antena amplificadora de señal. El objetivo es detectar la presencia de redes inalámbricas pertenecientes al cliente e identificar vulnerabilidades que permitan el ingreso al hacker.

Las antenas amplificadoras de señal pueden construirse utilizando implementos tan simples como el clásico cilindro metálico de papitas fritas, también llamado “cantenna” - por la combinación de las palabras inglesas “can” (contenedor) y “antenna” (antena). Por supuesto, si no somos expertos soldadores siempre podremos recurrir a comprar antenas amplificadoras profesionales.

Es una práctica común entre los aficionados al wardriving, el utilizar dispositivos GPS para registrar en un mapa las coordenadas de las redes inalámbricas halladas y así poder volver luego a un punto específico o bien con fines estadísticos. El sitio web más popular que permite registrar estos hallazgos es Wigle (<https://www.wigle.net>). Hardware requerido Para poder efectuar un hacking inalámbrico necesitamos:

- Dispositivo de cómputo con capacidad inalámbrica (laptop, tablet, smartphone). ● Tarjeta de red inalámbrica con manejadores (drivers) compatibles con el sistema operativo de nuestro dispositivo.
- Software para WiFi hacking compatible con nuestro sistema operativo.
- Si la red inalámbrica objetivo está a una distancia corta de nuestra ubicación y la potencia de la señal que detectamos es buena, basta con la tarjeta WiFi integrada, caso contrario deberemos comprar una nueva tarjeta que se pueda conectar a una antena amplificadora de señal.

En lo personal, prefiero Linux como sistema operativo para efectuar pruebas de intrusión de cualquier tipo. La suite Kali Linux (antes Backtrack) y Backbox son mis distribuciones de seguridad informática favoritas. Luego, esto no impide que podamos realizar un hacking inalámbrico desde Windows u otro sistema operativo, siempre y cuando usemos el hardware y software adecuados. La suite Wifislax merece una especial mención ya que está dedicada al hacking de WiFi.

El dispositivo que utilicemos para realizar nuestro hacking inalámbrico dependerá del caso particular. Las laptops permiten conectar antenas de mayor potencia o amplificadoras de señal, pero cuando hay que moverse por tramos largos en sitios como un centro comercial o la vía pública, suelen llamar mucho la atención del personal de seguridad y de los delincuentes también. Así que, en estos casos, una tablet o inclusive un smartphone, pueden cumplir con la tarea de mejor manera. La desventaja de usar una tablet o un smartphone es la poca potencia que tienen las antenas integradas en estos dispositivos y la dificultad en mejorar esta potencia. No obstante, hay algunos tips que nos pueden ayudar en este sentido, como el viejo truco de recortar un envase de aluminio curvado y colocar el dispositivo dentro para ampliar la recepción o comprar una carcasa especial⁸ para amplificar la recepción de la señal.

Otro tema que hay que resolver es que las aplicaciones de wardriving para smartphones y tablets normalmente requieren que se “rootee” el dispositivo. Esto implica realizar una serie de pasos - que usualmente incluyen modificar el sistema operativo de fábrica con que viene el dispositivo - para otorgarnos privilegios de administrador (root). Un dispositivo que recientemente se ha ganado su espacio en el mundo del wardriving es el Raspberry Pi, gracias a su bajo costo y a la facilidad con que se le pueden agregar componentes e instalarle diversos sistemas operativos. De hecho, hay sitios de ecommerce que ofrecen versiones ya listas de Raspberry Pi con tarjetas y antenas para wardriving y Kali Linux preinstalado. Algunas aplicaciones móviles populares para análisis de WiFi son:

- Wifi Analyzer, para Android.
- NetHunter, la versión móvil de Kali Linux.

Tarjetas de red

La tarjeta de red que usemos será vital para efectuar un wardriving exitoso, por eso es importante tomar en cuenta los siguientes puntos:

- Tipo de tecnología inalámbrica soportada (802.11a, 802.11b/g, 802.11n, etc.). Debemos asegurarnos que la tecnología de nuestro adaptador de red sea compatible con las redes WiFi que vamos a auditar.
- Manejadores compatibles con el sistema operativo de nuestro dispositivo, que permitan colocar a la tarjeta en modo monitor.
- Puerto que permita conectar la tarjeta de red a una antena amplificadora de señal externa. Estas son algunas marcas de tarjetas inalámbricas populares: Alfa Networks, Belkin, Tp-Link, Panda, entre otras.

Antenas amplificadoras de señal Como su nombre lo indica, este tipo de antenas permiten mejorar una señal débil de una red inalámbrica distante. Si queremos una antena amplificadora de señal, la opción más simple consiste

consiste en comprarla en nuestra tienda de productos electrónicos local (Ej: RadioShack) o bien a través de una tienda online (Ej: Amazon, Mercado Libre, Best Buy, WalMart, etc). Hay puntos importantes que debemos considerar antes de comprar una antena amplificadora:

- Tipo de conector compatible con nuestra tarjeta inalámbrica externa o que venga una tarjeta WiFi en el paquete.
- Que incluya un cable extensor lo suficientemente largo para poder ubicar mejor la antena y aun así tener comodidad suficiente para maniobrar nuestro dispositivo.
- Precio acorde a nuestro bolsillo. Dependiendo del fabricante y los accesorios, los precios pueden variar desde unos modestos 40 hasta varios cientos de euros.

En la gráfica siguiente podemos ver una antena amplificadora conectada a través de un conector coaxial a una tarjeta inalámbrica externa, la que a su vez está conectada a un cable extensor USB. Un extra importante de resaltar es el trípode, mismo que resulta imprescindible al momento de brindar estabilidad para posicionar adecuadamente la antena. Por otro lado, en la imagen inferior observamos un amplificador de señal que se vende por separado, el cual requiere que poseamos una tarjeta inalámbrica compatible con el conector coaxial provisto.

Software requerido Los aplicativos que permiten detectar routers o puntos de acceso inalámbricos cercanos y recopilar información detallada sobre los mismos como: nombre de la red (SSID), dirección física (BSSID), protocolo de autenticación y cifrado (OPEN, WEP, WPA/WPA2), intensidad de la señal, etc., se denominan detectores, en inglés: *stumblers*. Aquel software que además permite capturar los paquetes transmitidos en las redes (no sólo inalámbricas), se denominan capturadores o *sniffers*. Software de WiFi hacking para Windows Si bien Windows no es la plataforma preferida por los hackers, hay que admitir que es el sistema operativo más popular a nivel de equipos de escritorio. Y esta popularidad se la ha ganado en su mayor parte por su facilidad de uso, está de más decir que ejecutar y usar una aplicación en Windows en la mayoría de los casos apenas requiere que el usuario haga clicks con el mouse.

Lo anterior se contrapone a las herramientas de WiFi hacking para Linux, las cuales son habitualmente ejecutadas desde la interfaz de comandos. Cuando el auditor maneja bien Linux, ejecutar comandos es como nadar en el agua; más para los usuarios neófitos podría conllevar a errores y posterior frustración. Por este motivo consideramos importante incluir una sección sobre herramientas de WiFi hacking para Windows.

Algunos detectores para Windows son:

- **Vistumbler**, aplicación amigable y de código abierto, por consiguiente, gratuita.
- **NetStumbler**, conocida también como Network Stumbler, es gratuita y fácil de usar.

Ejemplos de sniffers:

- **CommView for WiFi**, es un analizador profesional (detector y capturador a la vez) desarrollado por la empresa Tamos Software como software comercial.
- **Acrylic WiFi Professional**, una suite desarrollada por Tarlogic Security SL que agrega drivers a Windows que permiten inyectar paquetes en tarjetas de red compatibles. ● **Wireshark**, es la nueva versión del clásico *Ethereal* y es software libre, cuenta con una interfaz gráfica amigable y está disponible tanto para Windows como para Linux. Un punto a resaltar de

Wireshark son los extensos tutoriales disponibles en la página web del proyecto.

Adicionalmente la suite de código abierto para hacking inalámbrico, **Aircrack-ng**, ha sido portada a Windows.

Nota importante: Si bien en teoría podemos usar Aircrack bajo Windows para hackear redes WiFi, en la práctica no es posible hacerlo si no contamos además con drivers que permitan colocar nuestra tarjeta inalámbrica en modo monitor y, por ende, tener la capacidad de inyectar paquetes en la red. Un adaptador inalámbrico popular que permite capturar e

inyectar paquetes bajo Windows es AirPcap, desarrollado por Riverbed, disponible en varios modelos de acuerdo a los protocolos 802.11

En consecuencia, si el lector desea realizar bajo Windows los laboratorios que involucran la suite Aircrack-ng, deberá invertir en tarjetas como AirPcap o comprar herramientas que provean drivers para inyectar paquetes como Acrylic Professional. Debido a lo anterior y dado que la inyección de paquetes en Linux es posible con una amplia gama de tarjetas inalámbricas integradas y externas de bajo costo, hemos decidido limitar los laboratorios bajo Windows a aquellos que no requieran colocar nuestra tarjeta en modo monitor; en todos los demás usaremos como plataforma principal Linux.

Software de WiFi hacking para Linux

Linux es un sistema operativo estable, escalable y de buen rendimiento, además de ser software libre y por ende gratuito. Todo esto - sumado a la adición de interfaces gráficas amigables - ha logrado que Linux transcienda la barrera de haber sido encasillado como un sistema para servidores y de exclusivo uso empresarial, para ubicarse como uno de los sistemas de escritorio favoritos a nivel mundial. Por el hecho de ser software libre, miles de desarrolladores han contribuido para crear diversas variaciones - denominadas distribuciones o distros - que incluyen software adicional que cumple propósitos específicos, pero siempre conservando como base la parte modular que hace que Linux sea Linux. A esta parte central o software común se le denomina el núcleo o kernel. Algunos ejemplos de distribuciones conocidas son: Ubuntu, Fedora, SuSe, Mandriva, Mint, CentOS, etc. Y por supuesto, las necesidades de los consultores, ingenieros y demás entusiastas de la Seguridad Informática llevaron a la creación de

distribuciones especializadas en hacking como Kali Linux, Backbox, Wifislax, Samurai Linux, Knoppix, entre otras. KISMET Kismet es un sniffer popular que suelen incluir las diversas distros Linux de Seguridad Informática. Para ejecutar Kismet basta con escribir el nombre de la aplicación (en minúsculas) en una ventana de terminal. Dado que necesitamos acceder a la tarjeta inalámbrica y cambiar su configuración, deberemos efectuar esto con privilegios administrativos (directamente como el usuario root o utilizando sudo). Ej: # kismet AIRCRACK-NG La suite aircrack-ng es un conjunto de aplicativos ejecutables desde la interfaz de línea de comandos (CLI) de Linux, que en conjunto permiten detectar redes inalámbricas, capturar paquetes de datos transmitidos y realizar ataques de claves. Puesto que requerimos privilegios administrativos también deberemos ejecutar estos comandos como el usuario root o bien otro usuario con un rol que nos permita manipular nuestras tarjetas inalámbricas.

Software para efectuar ataques de claves

Dependiendo del tipo de protocolo de seguridad al que nos enfrentemos en la red inalámbrica objetivo, es posible que necesitemos efectuar un ataque de claves. Aunque hay una gran diversidad de software para realizar ataques de claves, las siguientes son herramientas especializadas que se destacan por su efectividad:

- Aircrack-ng, la popular suite de comandos para WiFi disponible en Windows y Linux. Se ejecuta desde una línea de comandos CMD.
- Crunch, comando incluido con Kali Linux. Permite generar diccionarios personalizados para luego usarlos en un ataque de claves.
- Ophcrack, disponible tanto para Windows como para Linux. Utiliza una tecnología basada en tablas-rainbow, lo que lo hace una herramienta rápida si se cuenta con el respectivo diccionario de claves.
- Cain&Abel, herramienta de cracking y también sniffing disponible sólo para Windows, bastante popular.
- Wifite, herramienta de cracking para WEP/WPA/WPA2 incluida con Kali Linux.
- Hydra, excelente herramienta para cracking de claves desarrollada por los buenos amigos de The Hackers Choice, mejor conocidos como THC. Aunque fue desarrollada inicialmente sólo para Linux, ha sido portada exitosamente a Windows.

Recursos útiles

- Artículo: Alternativa a airpcap - Emulación de tarjetas Airpcap con Acrylic. (2017). Acrylic WiFi. Recuperado en 2017, de <https://www.acrylicwifi.com/blog/tarjetas-wifi-usb-alternativas-a-airpcap/>.
- Website: Wardriving.com. Recuperado en 2016, de <http://www.wardriving.com>.
- Website: Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution. (2016). Recuperado de <https://www.kali.org>.
- Paper: Rahul Pal, Randheer Kr. Das & R. Raj Anand. (2014). Rooting of Android Devices and Customized Firmware Installation and its Calibre. International Journal of Scientific Engineering and Technology. Volume No.3 Issue No.5, pp: 553-556. Recuperado de http://ijset.com/ijset/publication/v3s5/IJSET_2014_522.pdf.
- Paper: Justin Phelps. (2012). How to Set Up a Wireless Router. Recuperado de http://www.pcworld.com/article/249185/how_to_set_up_a_wireless_router.html.

FASE 1: RECONOCIMIENTO O MAPEO INALÁMBRICO Durante esta fase el hacker utiliza su dispositivo de wardriving favorito equipado con el hardware requerido y software detector (stumbler), para identificar las redes inalámbricas presentes en el área. Una vez identificadas las WLANs, el hacker procede a escoger su objetivo y determinar el tipo de autenticación, encripción y el cipher utilizado por la WLAN en cuestión. Esta información le servirá al hacker para escoger el tipo de ataque que efectuará para ganar acceso a la WLAN en el siguiente paso.

FASE 2: GANAR ACCESO A LA RED INALÁMBRICA Dependiendo de la información levantada en la fase previa, aquí el hacker escogerá el tipo de ataque a efectuar para ganar acceso a la red inalámbrica objetivo. Este ataque puede ser: al protocolo de encripción, al sistema de autenticación, a un cliente inalámbrico, una combinación de lo anterior, etc.

FASE 3: MANTENER ACCESO A LA RED INALÁMBRICA Durante esta fase, asumiendo que se tuvo éxito en la fase previa, el hacker ya puede conectarse a la red inalámbrica objetivo; por lo tanto, su siguiente movimiento será efectuar un reconocimiento de los equipos y redes conectadas a la WLAN con el fin de identificar nuevos objetivos y tratar de adentrarse en la LAN de la víctima. Esto nos lleva de nuevo al reconocimiento y al resto de fases del Círculo del Hacking. Mapeo Inalámbrico Ahora vamos a ver cómo efectuar un mapeo inalámbrico en Windows, Linux y Android con la ayuda de capturadores populares (stumblers).

Para ello es importante aclarar un par de conceptos. Todo mapeo inalámbrico inicia con un escaneo, el objetivo del escaneo es encontrar redes inalámbricas (WLANs) a los que un cliente pueda conectarse.

Dicho escaneo se puede efectuar de dos formas:

- Escaneo Activo
- Escaneo Pasivo

El escaneo es activo cuando para hallar un AP el cliente inalámbrico transmite un probe request y espera a recibir una respuesta. Por otro lado, el escaneo se considera pasivo¹⁰ cuando el cliente escucha en un canal por un cierto tiempo y durante ese lapso trata de “escuchar” unas tramas especiales denominadas beacons¹¹. Por este motivo un AP transmite beacons con información de cada una de sus WLANs de forma periódica, así los clientes inalámbricos conocen de la presencia de una WLAN en particular, para luego asociarse a ella. Dicho esto, hay ventajas y desventajas entre efectuar un escaneo pasivo vs hacer un escaneo activo. En un escaneo pasivo el cliente inalámbrico descubre WLANs sin necesidad de delatar su presencia ante un AP, pero si escucha muy poco tiempo en un canal podría perderse la presencia de un beacon y no detectar una WLAN. Por el contrario, durante un escaneo activo el cliente interactúa enviando tramas de tipo probe request, revelando su presencia a los posibles APs presentes en un canal, pero detectando rápidamente rápidamente las WLANs presentes. Este último inconveniente podría salvarse fácilmente escondiendo la verdadera MAC de nuestro adaptador de red, lo cual es bastante sencillo tal y como veremos en uno de los laboratorios más adelante.

La suite Aircrack-ng

La suite Aircrack-ng (<http://aircrack-ng.org/>) es un conjunto de herramientas de código abierto que permiten efectuar tareas como escaneo, mapeo, captura de tramas, inyección de paquetes y cracking de claves, en redes inalámbricas. Aunque fue desarrollada inicialmente para Linux está también disponible en otras plataformas como MacOS y Windows. Por sus muchas prestaciones, viene usualmente preinstalada en todas las distros Linux de Seguridad Informática, entre ellas Kali. Estos son de forma breve los comandos más utilizados de la suite Aircrack-ng:

- airmon-ng: usado para habilitar el modo monitor en un adaptador de red inalámbrico.
- aireplay-ng: se usa para inyectar paquetes en una wlan.
- airodump-ng: sirve para efectuar capturas de paquetes en una wlan.
- aircrack-ng: su propósito es realizar cracking de claves de los protocolos WEP y WPA/WPA2.

Usaremos esta suite y sus comandos en muchos de los laboratorios más adelante, por lo tanto vale la pena que el lector le dedique unos minutos a revisar la Wiki del proyecto ubicada en <http://aircrack-ng.org/doku.php>.

Lab: Escaneo pasivo con Linux

Recursos:

Estación hacker: Computador con sistema operativo Linux (en este ejemplo usamos Ubuntu). Software: Suite Aircrack y wireless-tools. Hardware: Tarjeta de red inalámbrica compatible con Linux y con la suite Aircrack-ng Notas:

- Si en su versión de Linux no viene preinstalada la suite Aircrack, puede instalarla desde un repositorio o compilando el código fuente previamente descargado desde la página del proyecto en <https://www.aircrack-ng.org/>.
- La mayoría de comandos usados en este laboratorio requieren privilegios de root, para ello puede cambiarse de rol con el comando su, o bien puede anteponer sudo a los comandos.

Pasos a seguir:

Empezaremos verificando el nombre de su tarjeta inalámbrica. Para ello usaremos el comando: ifconfig.

1.- Deberemos buscar el nombre de nuestro adaptador inalámbrico (usualmente se llama wlanX, en donde X es el número del adaptador: 0 si es el primero, 1 si es el segundo y así sucesivamente). En mi caso particular aparte de la tarjeta integrada denominada wlan0, he conectado una tarjeta externa y el sistema la identifica como “wlx...”, por ello verán este nombre de adaptador en las imágenes ejemplo.

2.- Una vez identificado nuestro adaptador deberemos desconectarlo de cualquier WLAN a la que hubiere sido conectado (seleccionar ícono de la red inalámbrica en la barra de estado, click en “Disconnect” bajo el nombre de la WLAN).

3.- Ahora usaremos el comando iwconfig para ver los parámetros de nuestra interfaz. Ej: iwconfig wlan0.

4.- Si la tarjeta lo permite podemos subir la potencia de transmisión usando la opción txpower. Este parámetro es en dBm. Si el valor de potencia está en Watts, la fórmula de conversión es $P(\text{dBm}) = 30 + 10 \times \log(W)$. Ej: sudo iwconfig wlan0 txpower 60. Para que esto sea posible la interfaz debe estar arriba (up).

5.- Ahora colocaremos nuestra tarjeta de red inalámbrica en modo monitor. Esto lo haremos usando el comando airmon-ng.

Baje su interfaz inalámbrica usando el comando ifconfig. Sintaxis: ifconfig nombre_adaptador_wifi down Ej: ifconfig wlan0 down

Coloque la interfaz wlan0 en modo monitor y súbala nuevamente:

Sintaxis: airmon-ng start nombre_adaptador_wifi Ej:airmon-ng start wlan0

Sintaxis: ifconfig nombre_adaptador_wifi up Ej: ifconfig wlan0 up

Nota: Si el comando airmon-ng le mostrara un mensaje de error al ejecutarlo, indicando que hay procesos que le causan conflicto, proceda a detener dichos procesos y ejecute airmon-ng nuevamente. Ej: airmon-ng check kill.

Luego usaremos el comando iw para efectuar un escaneo pasivo de las redes inalámbricas cercanas.

Sintaxis: iw dev nombre_adaptador_wifi scan passive | grep SSID Ej: iw dev wlan0 scan passive | grep SSID

Lab: Escaneo activo con Linux

Recursos:

1. **Estación hacker:** Computador con sistema operativo Linux (en este lab usamos Ubuntu).
2. **Software:** Suite Aircrack y wireless-tools.
3. **Hardware:** Tarjeta de red inalámbrica compatible con Linux y con la suite Aircrack-ng.

Pasos a seguir:

1. Identifique su tarjeta de red inalámbrica.
2. Baje la interfaz inalámbrica usando el comando ifconfig.
3. Coloque la interfaz en modo monitor con airmon-ng y súbala nuevamente. Observe que además del adaptador físico se crean interfaces lógicas de tipo monitor (monX).

4. Luego usaremos el comando iwlist para efectuar un escaneo activo de las redes inalámbricas cercanas.

Sintaxis: `iwlist nombre_adaptador_wifi scan | grep SSID`

Ej: `iwlist wlan0 scan | grep SSID`

5. La figura siguiente muestra un posible resultado.

```
root@Trantor:/home/karina
wlx784476b445e5 Link encap:Ethernet HWaddr 78:44:76:b4:45:e5
      UP BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:3573 errors:0 dropped:3573 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:1081477 (1.0 MB) TX bytes:0 (0.0 B)

root@Trantor:/home/karina# ifconfig wlx784476b445e5 down
root@Trantor:/home/karina# airmon-ng start wlx784476b445e5

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
19791    NetworkManager
19810    wpa_supplicant
19817    dhclient
Process with PID 19817 (dhclient) is running on interface wlan0

Interface      Chipset      Driver
mon2          Ralink RT2870/3070   rt2800usb - [phy1]
wlx784476b445e5      Ralink RT2870/3070   rt2800usb - [phy1]
                           (monitor mode enabled on mon6)
mon1          Ralink RT2870/3070   rt2800usb - [phy1]
wlan0         Broadcom wl - [phy0]
mon8          Ralink RT2870/3070   rt2800usb - [phy1]
mon5          Ralink RT2870/3070   rt2800usb - [phy1]
mon3          Ralink RT2870/3070   rt2800usb - [phy1]
mon4          Ralink RT2870/3070   rt2800usb - [phy1]

root@Trantor:/home/karina# ifconfig wlx784476b445e5 up
root@Trantor:/home/karina# iwlist wlx784476b445e5 scan | grep SSID
        ESSID:"ELX [REDACTED]"
        ESSID:"INV [REDACTED]"
        ESSID:"INTE [REDACTED] T"
        ESSID:"CNT [REDACTED] "
        ESSID:"7E [REDACTED]"
        ESSID:"Claro [REDACTED] "
        ESSID:""
        ESSID:"Claro [REDACTED] "
root@Trantor:/home/karina#
```

Lab: Mapeando WLANs con Windows

Recursos:

1. **Estación hacker:** Computador con sistema operativo Windows.
2. **Software:** Comando netsh incluido con Windows.
3. **Hardware:** Adaptador inalámbrico compatible con Windows.

Pasos a seguir:

1. Abra una línea de comandos cmd y ejecute el siguiente comando:

```
netsh wlan show networks mode=ssid
```

```
C:\Windows\system32\cmd.exe
C:\Users\Karina>netsh wlan show networks mode=ssid
Nombre de interfaz : Conexión de red inalámbrica
Actualmente hay 6 redes visibles.

SSID 1 : Claro_
    Tipo de red      : Infraestructura
    Autenticación   : Abierta
    Cifrado          : WEP

SSID 2 : Claro_
    Tipo de red      : Infraestructura
    Autenticación   : Abierta
    Cifrado          : WEP

SSID 3 : Android_
    Tipo de red      : Infraestructura
    Autenticación   : WPA2-Personal
    Cifrado          : CCMP

SSID 4 :
    Tipo de red      : Infraestructura
    Autenticación   : WPA2-Personal
    Cifrado          : CCMP

SSID 5 : 799414
    Tipo de red      : Infraestructura
    Autenticación   : WPA2-Personal
    Cifrado          : CCMP

SSID 6 : 20331
    Tipo de red      : Infraestructura
    Autenticación   : Abierta
    Cifrado          : WEP

C:\Users\Karina>
```

2. El comando netsh tiene más opciones las cuales podemos revisar con la ayuda (/?) luego de cualquiera de los parámetros. Veamos un ejemplo:

```
C:\Windows\system32\cmd.exe
C:\Users\Karina>netsh wlan show networks /?
Uso: show networks [[interface=<cadena>] [[mode=ssid/bssid]]
Parámetros:
Etiqueta      Valor
interface    - Nombre de la interfaz que tiene este perfil configurado.
node         - Obtiene información bssid detallada.
Notas:
Muestra las redes disponibles para el sistema.
Los parámetros interface y bssid son opcionales.
Si se proporciona un nombre de interfaz, sólo se enumerarán las redes de
la interfaz dada. Si no se da un nombre, se enumerarán todas las redes
visibles para el sistema.
Si se especifica mode=bssid, también aparecerán los bssid visibles para
cada ssid. De lo contrario, sólo aparecerán los ssid.
Ejemplos:
show networks interface="Conexión de red inalámbrica"
show networks mode=Bssid
show networks

C:\Users\Karina>
```

3. Como podemos observar en la ayuda, si deseáramos mapear las WLANs previamente escaneadas bastaría con cambiar el modo a bssid.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.
C:\Users\Karina>netsh wlan show networks mode=bssid
```

```
C:\Windows\system32\cmd.exe
Otras velocidades (Mbps): 6 9 12 18 24 36 48 54
SSID 3 : Claro_ [REDACTED]
    Tipo de red      : Infraestructura
    Autenticación   : Abierta
    Cifrado          : WEP
    BSSID 1          : 4c:[REDACTED]
        Señal         : 70%
        Tipo de radio : 802.11n
        Canal          : 3
    Velocidades básicas (Mbps): 1 2 5.5 11
    Otras velocidades (Mbps): 6 9 12 18 24 36 48 54
SSID 4 : Claro_ [REDACTED]
    Tipo de red      : Infraestructura
    Autenticación   : Abierta
    Cifrado          : WEP
    BSSID 1          : 68:[REDACTED]:1c
        Señal         : 10%
        Tipo de radio : 802.11n
        Canal          : 8
    Velocidades básicas (Mbps): 1 2 5.5 11
    Otras velocidades (Mbps): 6 9 12 18 24 36 48 54
SSID 5 : [REDACTED]
    Tipo de red      : Infraestructura
    Autenticación   : WPA2-Personal
    Cifrado          : CCMP
    BSSID 1          : [REDACTED]:27
        Señal         : 44%
        Tipo de radio : 802.11n
        Canal          : 9
    Velocidades básicas (Mbps): 1 2 5.5 11
    Otras velocidades (Mbps): 6 9 12 18 24 36 48 54
SSID 6 : Android [REDACTED]
    Tipo de red      : Infraestructura
    Autenticación   : WPA2-Personal
    Cifrado          : CCMP
    BSSID 1          : 38:d4:[REDACTED]
        Señal         : 12%
        Tipo de radio : 802.11n
        Canal          : 11
    Velocidades básicas (Mbps): 1 2 5.5 11
    Otras velocidades (Mbps): 6 9 12 18 24 36 48 54
C:\Users\Karina>
```

Lab: Mapeando WLANs desde Linux

Recursos:

- **Estación hacker:** Computador con sistema operativo Linux (en este lab usamos Ubuntu).
- **Software:** Suite Aircrack y wireless-tools.

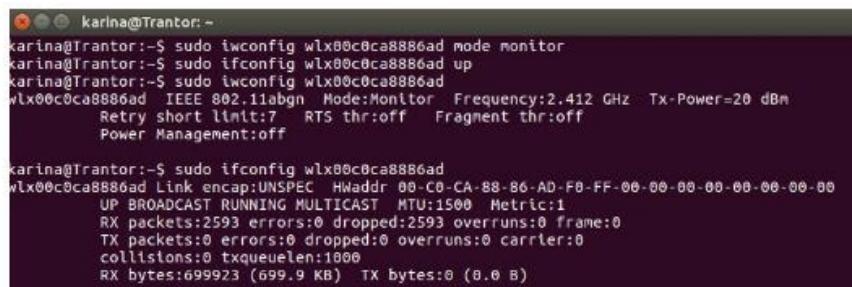
- **Hardware:** Tarjeta de red inalámbrica compatible con Linux y con la suite Aircrack-ng.

Pasos a seguir:

1. Habiendo identificado previamente nuestra interfaz de red inalámbrica, la colocaremos en modo monitor. En esta ocasión usaremos iwconfig (aunque bien podríamos usar airmon-ng).

Ej:

```
sudo ifconfig wlan0 down  
sudo iwconfig wlan0 mode monitor  
sudo ifconfig wlan0 up
```



```
karina@Trantor:~  
karina@Trantor:~$ sudo iwconfig wlx00c0ca8886ad mode monitor  
karina@Trantor:~$ sudo ifconfig wlx00c0ca8886ad up  
karina@Trantor:~$ sudo iwconfig wlx00c0ca8886ad  
wlx00c0ca8886ad IEEE 802.11abgn Mode:Monitor Frequency:2.412 GHz Tx-Power=20 dBm  
Retry short limit:7 RTS thr:off Fragment thr:off  
Power Management:off  
  
karina@Trantor:~$ sudo ifconfig wlx00c0ca8886ad  
wlx00c0ca8886ad Link encap:UNSPEC Hwaddr 00-C0-CA-88-B6-AD  
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
      RX packets:2593 errors:0 dropped:2593 overruns:0 frame:0  
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
      collisions:0 txqueuelen:1000  
      RX bytes:699923 (699.9 KB) TX bytes:0 (0.0 B)
```

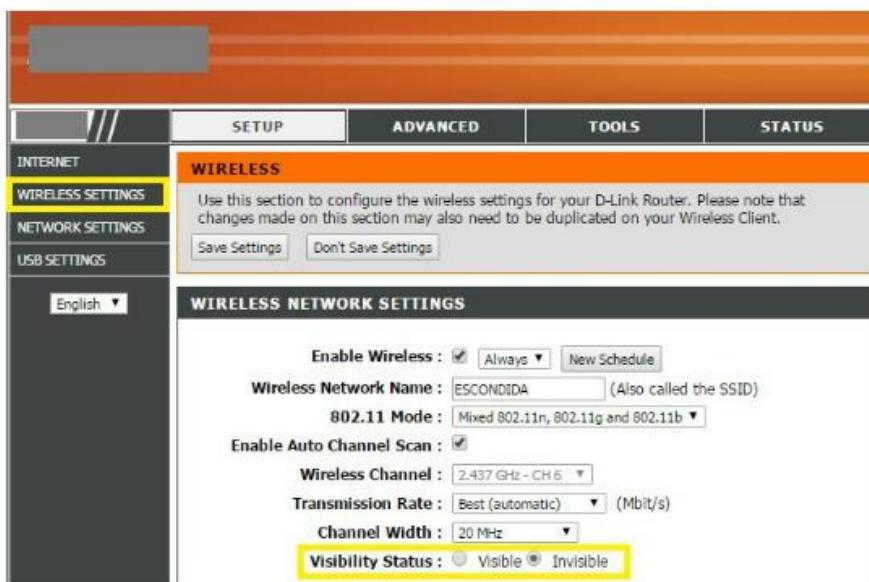
2. Finalmente estamos listos para mapear las redes inalámbricas cercanas. Para ello haremos un escaneo activo con el comando airodump-ng. Ej: sudo airodump-ng wlan0 (con mi tarjeta externa sería: sudo airodump-ng wlx00c0ca8886ad).
3. Como se puede observar ya podemos ver las distintas WLANs y sus parámetros. Sin embargo, se puede ver en el gráfico adjunto que hay una WLAN cuyo nombre está oculto (es la que dice “<length: 0>” en el campo ESSID (Extended Service Set Identifier)).

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
BC:66:41:	-48	16	0 0 7	54e	WPA2 CCMP	PSK	INT		
9C:D6:43:	-49	11	0 0 6	54e	WPA2 CCMP	PSK	<length: 0>		
9C:D6:43:	-51	12	0 0 6	54e	WPA2 CCMP	PSK	INV		
9C:D6:43:	-50	11	0 0 6	54e	WPA2 CCMP	PSK	ELX		
3B:4C:90:	-45	16	0 0 11	54e	WPA2 CCMP	PSK	Cla		
3B:68:23:	-58	7	0 0 11	54e	WEP WEP	PSK	Cla		
5C:D9:98:	-68	5	0 0 2	54e	WPA2 CCMP	PSK	dli		
3B:4C:90:	-71	4	0 0 1	54e	WPA2 CCMP	PSK	Cla		
EB:D6:27:	-74	6	0 0 9	54e	WPA2 CCMP	PSK	CHAI		
B4:A1:51:	-77	7	0 0 2	54e	WPA2 CCMP	PSK	Fan		
02:E6:60:	-77	5	0 0 1	54e	WPA2 CCMP	PSK	or		
EC:55:F9:	-78	7	0 0 1	54e	WEP WEP	PSK	Cla		
BB:9A:CD:	-78	6	0 0 11	54e	WPA2 CCMP	PSK	CN		
5B:B6:33:	-79	2	0 0 6	54e	WPA2 CCMP	PSK	Telc		
AC:EC:80:	-80	7	0 0 1	54e	WPA2 CCMP	PSK	Clar		
00:39:B3:	-80	5	0 0 1	54e	WEP WEP	PSK	clar		
AC:EC:80:	-81	6	0 0 11	54e	WEP WEP	PSK	Clar		
0C:B4:DC:	-92	5	0 0 11	54e	WEP WEP	PSK	Clar		
BSSID	STATION	PWR	Rate	Lost	Frames	Probe			
(not associated)	9C:2A:83:	-78	0 - 1	8	2				

¿Qué quiere decir que una WLAN está oculta?

Cuando configuramos una WLAN en un AP, como administradores tenemos la potestad de decidir si vamos a publicar la existencia de la misma; esto usualmente se puede hacer muy fácilmente desde la interfaz de administración del AP en la sección de redes inalámbricas con tan solo activar/desactivar una opción de “visibilidad”.

La siguiente figura muestra cómo se activa/desactiva la opción de visibilidad en un AP.



Ahora, ¿qué significa esto en términos del estándar 802.11? Pues entre los tipos de tramas usadas por una red WiFi hay un tipo especial denominado “beacon”.

Un beacon frame contiene información sobre la WLAN como el Service Set Identifier (SSID) el cual conocemos como “el nombre de la WLAN” y otros parámetros, estos beacons son transmitidos por el AP de forma periódica de modo que los clientes inalámbricos puedan asociarse a la WLAN.

Cuando un administrador configura a la WLAN en modo “invisible” lo que ocurre es que el campo SSID dentro del beacon se envía vacío, debido a lo cual, el cliente inalámbrico deberá conocer con antelación el nombre de la WLAN para poder asociarse a la misma.

En la siguiente gráfica observamos como al escanear WLANs desde Kali Linux¹³ tanto en modo pasivo como activo hay una red de la cual no nos aparece el SSID, por lo consiguiente, deducimos que el administrador ha ocultado la red.

```
root@kali:~# iwconfig wlan0
wlan0    IEEE 802.11bgn  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

root@kali:~# iw dev wlan0 scan passive | grep SSID
SSID: Claro [REDACTED]
SSID: M [REDACTED]
SSID: [REDACTED]
SSID: Claro [REDACTED]
SSID: TVCABLE [REDACTED]
SSID: RED [REDACTED]
root@kali:~# iwlist wlan0 scan | grep SSID
ESSID:"Claro" [REDACTED]
ESSID:"M" [REDACTED]
ESSID:""
ESSID:"Claro" [REDACTED]
ESSID:"TVCABLE" [REDACTED]
ESSID:"RED" [REDACTED]
ESSID:"Tvcable" [REDACTED]

root@kali:~#
```

Empero, esto es tan sólo un leve contra-tiempo, en el siguiente laboratorio veremos cómo podemos mapear una WLAN que tiene su SSID oculto.

Lab: Mapeando WLANs ocultas desde Linux

Recursos:

- **Estación hacker:** Computador con sistema operativo Linux (en este lab usamos Kali).
- **Software:** Suite Aircrack y wireless-tools.
- **Hardware:** Tarjeta de red inalámbrica compatible con Linux y con la suite Aircrack-ng.

Pasos a seguir:

1. Primero colocamos nuestra tarjeta WiFi en modo monitor y luego capturaremos paquetes con airodump-ng.

Ej: airodump-ng wlan0

CH 13][Elapsed: 48 s][2017-02-05 01:43										
BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:1C:F0:F1:51:54	-49	35	11 0 7 54 .	OPEN					<length: 0>	
38:	-72	16	35 0 1 54e	WPA2	CCMP	PSK			Lta	
4C:	-78	15	45 0 3 54e	WEP	WEP				Cla	
C0:	-86	14	4 0 9 54e	WPA2	CCMP	PSK				
F4:	-90	15	58 0 11 54e	WPA2	CCMP	PSK			RED	
E4:	-92	29	0 0 2 54e	WPA2	CCMP	PSK			TVC	
04:	-94	7	0 0 11 54e	WPA2	CCMP	PSK			Tvc	
38:	-95	3	0 0 6 54e	WPA2	CCMP	PSK			And	
BSSID	STATION	PWR	Rate	Lost	Frames	Probe				
(not associated)	30:	-50	0 - 1	0		7	wifi-kcer			
(not associated)	24:	-96	0 - 1	11		3				
00:1C:F0:F1:51:54	74:DE:2B:88:35:B6	-38	0 - 8e	0		6				
38:	00:	-1	0e- 0	0		13				

2. Como se puede ver hay una red abierta (OPEN), pero que está oculta. Esto lo sabemos porque en lugar del nombre de la WLAN aparece el texto “<length: 0>”.
3. Para conocer el nombre de esta WLAN oculta usaremos un truco sencillo, haremos que uno de los clientes conectados a dicha red se vuelva a autenticar. ¿Cómo? Pues des autenticándolo¹⁴ con el comando aireplay-ng.

- Corte la captura con airodump-ng y esta vez vuelva a efectuarla, pero restringiéndola al AP de interés. Para ello necesitaremos la información del campo BSSID, es decir la dirección MAC del AP víctima y el canal que usa para la comunicación.

Sintaxis: airodump-ng --channel #canal_de-l_AP —bssid *MAC_AP_victima nombre_adaptador_wifi*

Ej: airodump-ng --channel 7 --bssid
00:1C:F0:F1:51:54 wlan0

4. Ahora abra otro terminal y en él ejecute aireplay-ng.

Sintaxis: aireplay-ng -0*cantidad_paquetes_deauth* -a *dirección_MAC_del_AP_victima* -c *dirección_MAC_del_cliente nombre_adaptador_wifi*

Ejemplo: aireplay-ng -020 -a
00:1C:F0:F1:51:54 -c 74:DE:2B:08:35:B6 wlan0

```
CH 7 ][ Elapsed: 42 s ][ 2017-02-05 02:06
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:1C:F0:F1:51:54   0 100     163    28   0   7 54e. OPEN           ESCRITO
BSSID          STATION PWR Rate Lost Frames Probe
00:1C:F0:F1:51:54 74:DE:2B:08:35:B6   0    0 - 1e    2    1048 ESCRITO

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# clear
root@kali:~# aireplay-ng -020 -a 00:1C:F0:F1:51:54 -c 74:DE:2B:08:35:B6 wlan0
02:06:37 Waiting for beacon frame (BSSID: 00:1C:F0:F1:51:54) on channel 7
02:06:38 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 3|28 ACKs]
02:06:39 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 5|33 ACKs]
02:06:40 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|29 ACKs]
02:06:40 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|30 ACKs]
02:06:41 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|24 ACKs]
02:06:42 Sending 64 directed DeAuth. STMAC: [74:DE:2B:08:35:B6] [ 0|34 ACKs]
```

5. Como podemos ver, al efectuar el ataque con aireplay-ng el cliente se vuelve a autenticar, revelándonos el nombre de la WLAN. En este ejemplo nuestra WLAN oculta tiene por nombre “ESCONDIDA”.

*Lab: Mapeando WLANs en Windows
con Vistumbler*

Recursos:

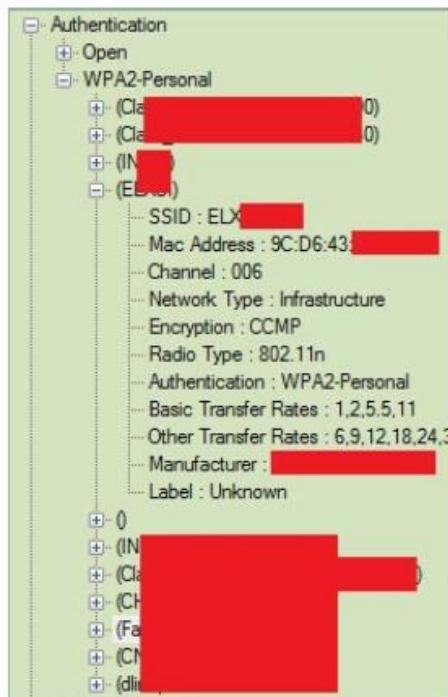
- **Estación hacker:** Computador con sistema operativo Microsoft Windows.
- **Software:** Vistumbler para Windows, descargable desde <https://www.vistumbler.net/>.
- **Hardware:** Adaptador inalámbrico compatible con Windows.

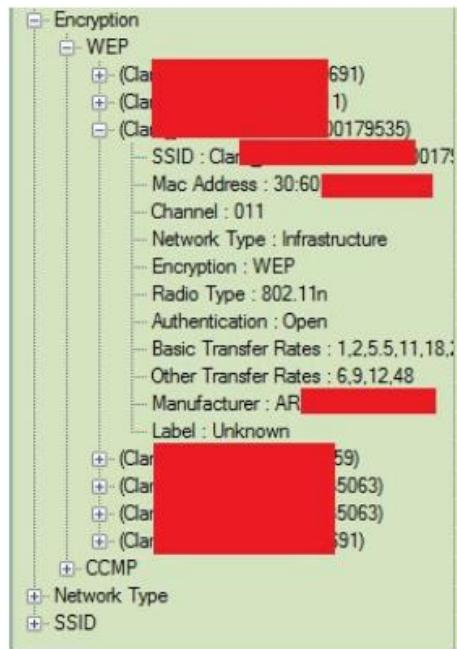
Pasos a seguir:

1. Descargar e instalar Vistumbler en su computador, siga los pasos indicados por el programa instalador.
2. Abrir Vistumbler y hacer click sobre el botón “Scan APs”. Aquí deberá ver un listado con los puntos de acceso inalámbricos cercanos e información útil como el nombre de la WLAN (SSID), niveles de señal, autenticación, encripción, etc.

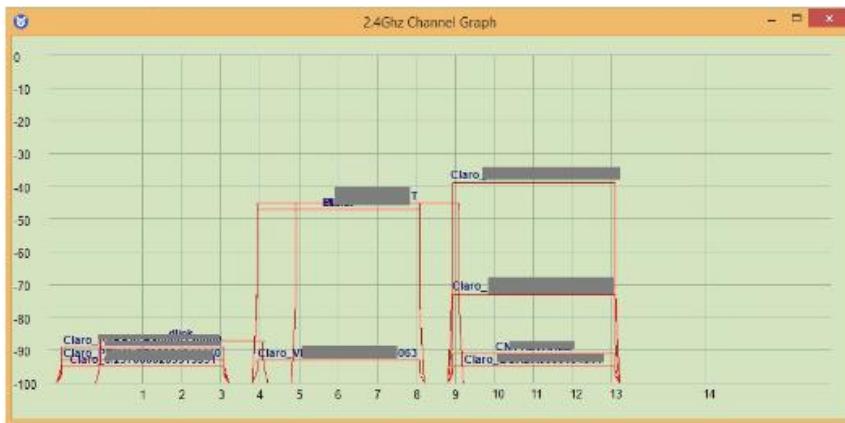
Wifimble v1.0.6.4 Beta 3 - By Andrew Cutcliff - 05/03/2016 - (2016-11-28 17-07-46.mdb)											
Stop		Link GUI		Active Atheros 12 / 14		WIFDB		Help		Support/Feedback	
Graph 1		Graph 2		Active Interf. 12/24m		Active N 0000.0000		Active P 0000.0000			
Authentication	#	Active	Mac Address	SSID	Signal	High Signal	BSST	High BSST	Chans	Authentication	Protocol
Channel	1	Active	00:0C:D6:43	00:0C:D6:43	-27	-47	-45 dBm	-45 dBm	1	Open	WEP
Encryption	2	Active	00:0C:D6:43	00:0C:D6:43	-22	-34	-45 dBm	-45 dBm	1	WPA2-Personal	CCMP
Network Type	3	Active	00:0C:D6:43	00:0C:D6:43	-6	-18	-10 dBm	-10 dBm	1	WPA2-Personal	CCMP
SSID	4	Active	00:0C:D6:43	00:0C:D6:43	-107	-107	-47 dBm	-45 dBm	6	WPA2-Personal	CCMP
	5	Active	00:0C:D6:43	00:0C:D6:43	-107	-107	-47 dBm	-45 dBm	6	WPA2-Personal	CCMP
	6	Active	00:0C:D6:43	00:0C:D6:43	-107	-107	-47 dBm	-45 dBm	6	WPA2-Personal	CCMP
	7	Active	00:0C:D6:43	00:0C:D6:43	-14	-18	-55 dBm	-51 dBm	11	Open	WEP
	8	Active	00:0C:D6:43	00:0C:D6:43	-82	-82	-69 dBm	-69 dBm	11	Open	WEP
	9	Active	00:0C:D6:43	00:0C:D6:43	-129	-107	-45 dBm	-41 dBm	7	WPA2-Personal	CCMP
	10	Active	00:0C:D6:43	00:0C:D6:43	-107	-107	-43 dBm	-39 dBm	11	WPA2-Personal	CCMP
	11	Active	00:0C:D6:43	00:0C:D6:43	-8	-18	-100 dBm	-91 dBm	1	Open	WEP
	12	Active	00:0C:D6:43	00:0C:D6:43	-1	-18	-95 dBm	-91 dBm	9	WPA2-Personal	CCMP
	13	Active	00:0C:D6:43	00:0C:D6:43	-14	-22	-93 dBm	-89 dBm	2	WPA2-Personal	CCMP
	14	Active	00:0C:D6:43	00:0C:D6:43	-10	-14	-95 dBm	-93 dBm	1	WPA2-Personal	CCMP

3. Sobre el lado izquierdo verá un conjunto de opciones tipo árbol. Al hacer click en el símbolo más (+) de una de las opciones podrá ver mayores detalles sobre una WLAN en particular.

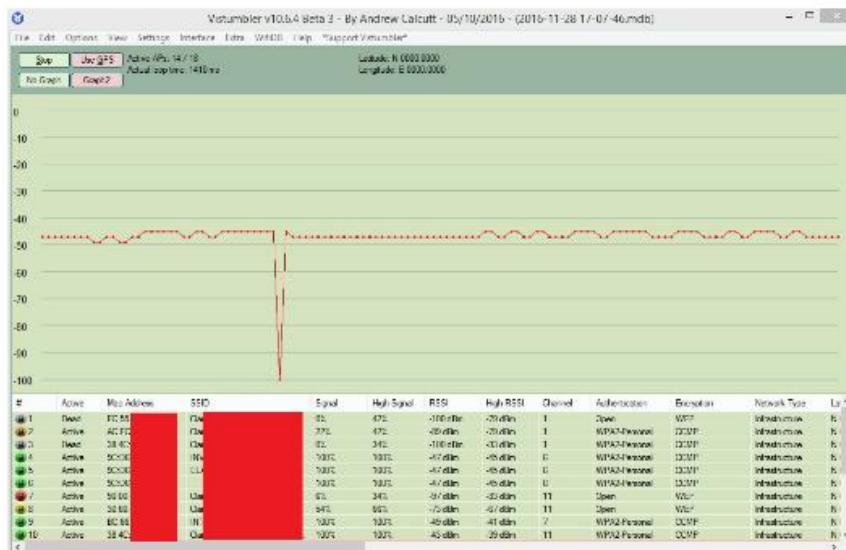




4. Si da click sobre los botones “Graph 1” o “Graph 2” podrá ver el gráfico de potencia de la señal de la WLAN que escoja. Para desactivar el gráfico haga click sobre el botón respectivo “No Graph”.

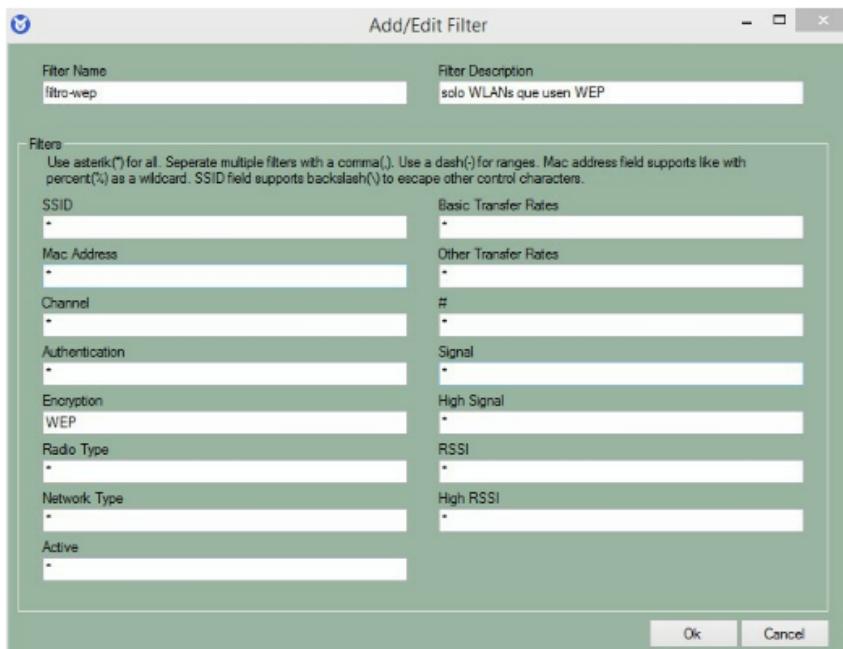


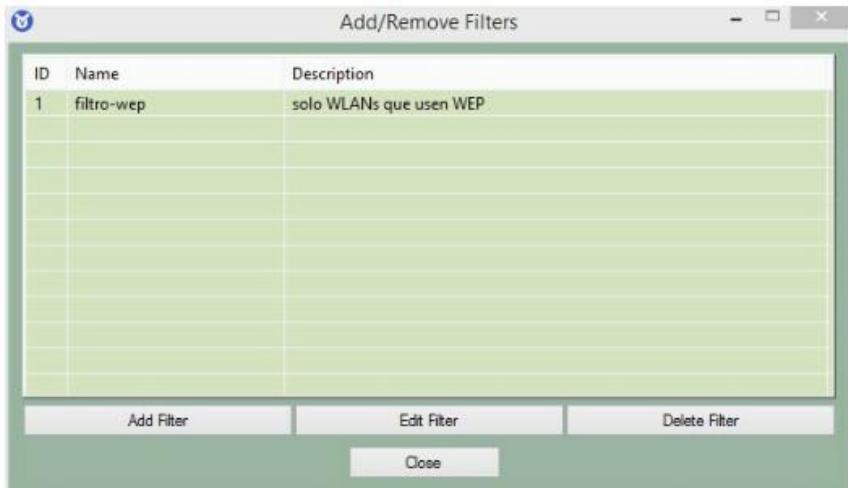
5. Una forma alternativa para comparar los niveles de potencia de los puntos inalámbricos cercanos es escogiendo el menú “Extras -> 2.4Ghz Channel Graph” o el equivalente para 5Ghz, dependiendo de nuestra antena.



6. Si queremos enfocarnos en una característica particular o en una WLAN, podemos usar la característica de filtros que incluye Vistumbler. Para ello seleccione “View -> Filters -> Add/Remove Filters”. Luego haga click en el botón “Add Filter”. Esto abrirá una ventana en la que podremos agregar la característica en la que queremos centrarnos. Por ejemplo, imaginemos que sólo queremos ver las WLANs que usen como encripción WEP. En este caso

particular le daremos un nombre apropiado al filtro (Ej: filtro-wep) y escribiremos “WEP” en la caja de texto correspondiente a “Encryption” y daremos click en el botón “OK”.

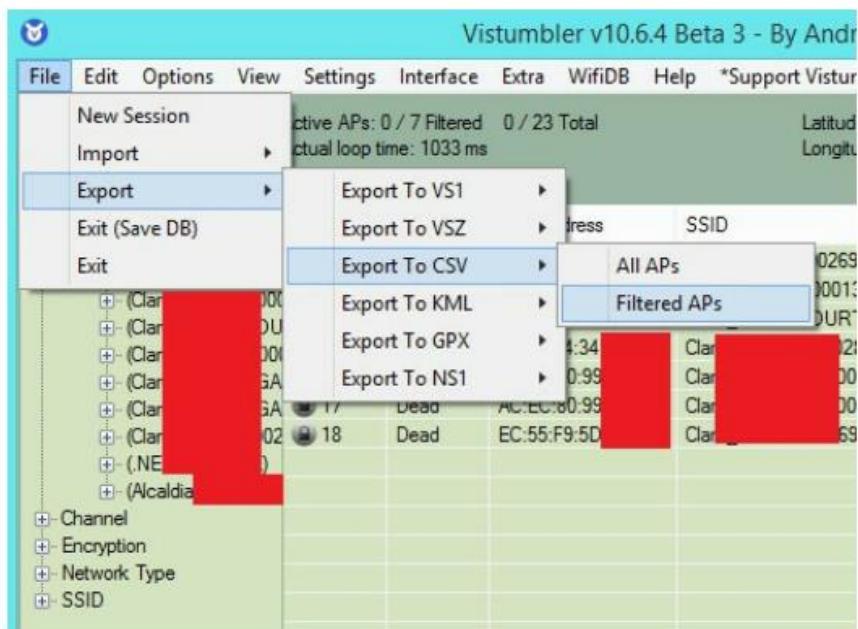




7. Ahora que ya tenemos creado nuestro filtro, simplemente lo escogeremos dentro del menú “View -> Filters -> filtro-wep” y observaremos el resultado.



8. El resultado de nuestro mapeo podemos exportarlo en diferentes formatos para posterior análisis. En este ejemplo hemos escogido exportar en formato csv los APs filtrados.



9. Como se puede observar, Vistumbler es un detector muy fácil de usar y realmente útil para mapear WLANs.

Lab: Mapeando WLANs desde Android

Recursos:

- **Dispositivo hacker:** Smartphone o tablet con sistema operativo Android.
- **Software:** Wifi Analyzer disponible sin costo desde Google Play.
- **Hardware:** Adaptador inalámbrico integrado en su smartphone/tablet.

Pasos a seguir:

1. Ingresar a Google Play, buscar “Wifi Analyzer” e instalarlo. Luego buscar “Wifi Connecter Library” e instalarla también.
2. Este aplicativo no requiere que desconectemos nuestro dispositivo de una WLAN para mapear, así que da lo mismo tanto si estamos conectados o no.
3. Abrir Wifi Analyzer. En la pantalla principal aparecerán todas las WLANs dentro del alcance de la tarjeta inalámbrica de su dispositivo. La información provista incluye: SSID (nombre de la WLAN), BSSID (dirección MAC del AP), marca del AP, niveles de potencia.

Wifi Analyzer



:

⚠️ No conectado!

INV [REDACTED] (9c:d6:43: [REDACTED])

WiFi Canal 6 2437 MHz D-LINK INTERNATIONAL
2448-2426=22 MHz -68 dBm

WPA2

INTER [REDACTED] (bc:66:41: [REDACTED])

WiFi Canal 7 2442 MHz IEEE REGISTRATION A...
2453-2431=22 MHz -50 dBm

WPA2

ARR [REDACTED] (38:4c:90: [REDACTED])

WiFi Canal 1 2412 MHz ARRIS GROUP, INC
2423-2401=22 MHz -52 dBm

WPA2

? (9c:d6:43: [REDACTED])

WiFi Canal 6 2437 MHz D-LINK INTERNATIONAL
2448-2426=22 MHz -69 dBm

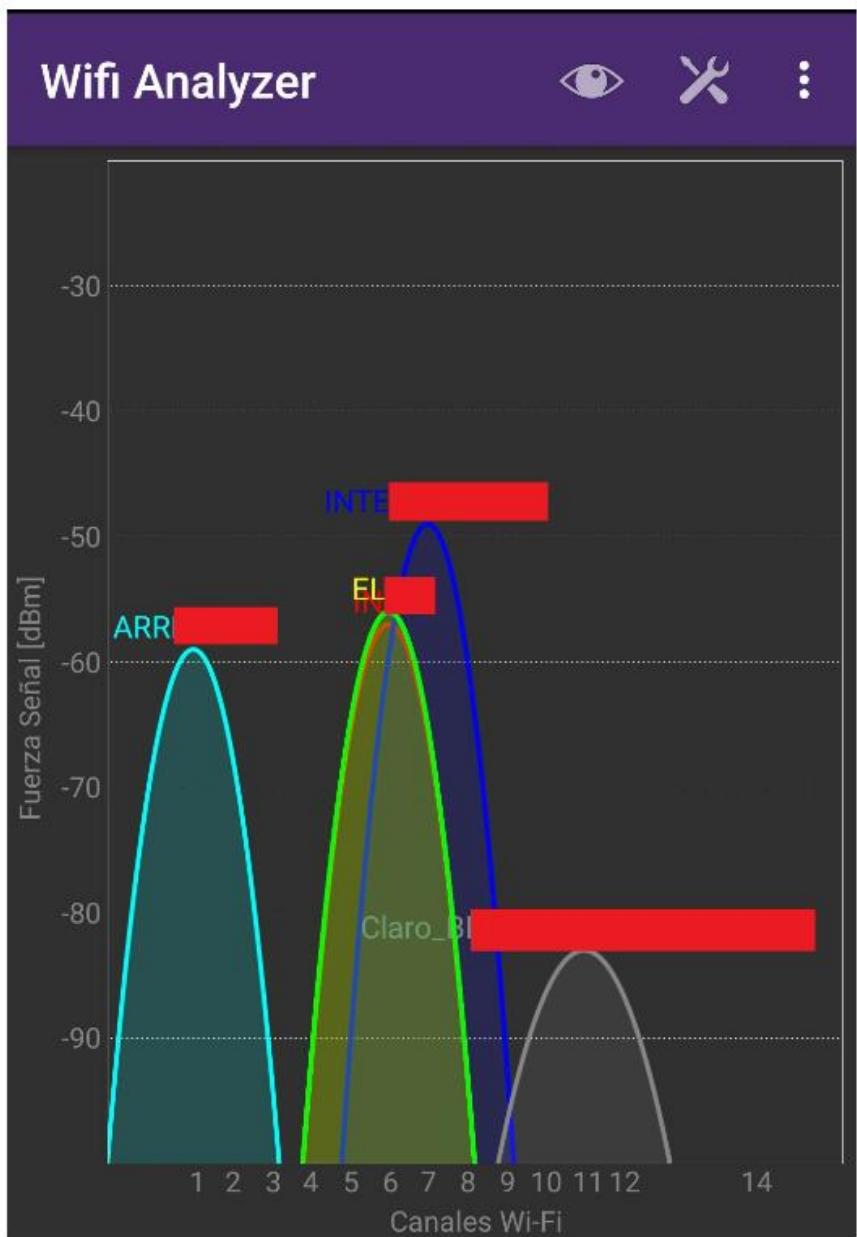
WPA2

ELX [REDACTED] (9c:d6:43: [REDACTED])

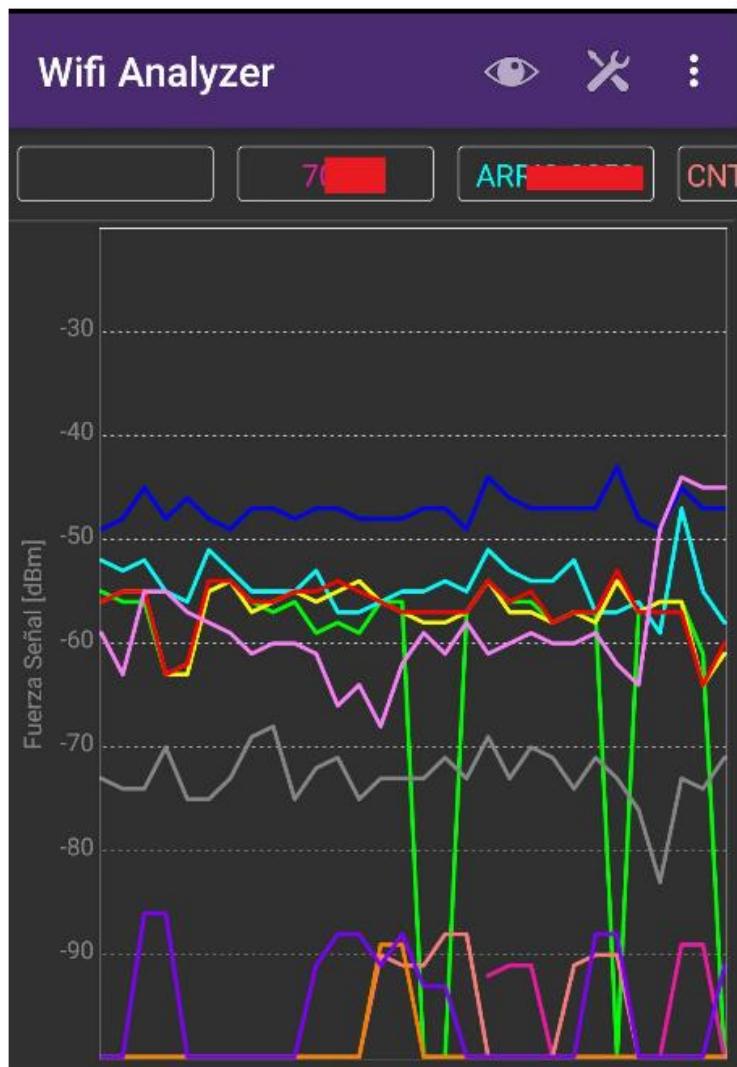
WiFi 2437 MHz D-LINK INTERNATIONAL

4. En la parte superior hay un ícono que representa un ojo. Si seleccionamos dicho ícono nos permitirá cambiar la vista a: gráfico de canales, gráfico de tiempo, puntuación de canales, lista de APs (la actual), medidor de señal. Vamos a escoger primero “Gráfico de canales”.





5. Luego escogeremos “Gráfico de tiempo”.



6. En la vista de “Puntuación de canales” nos pedirá seleccionar nuestro AP actual si estuviésemos conectados a una WLAN.
7. De igual forma en la vista de “Medidor de señal” necesitaremos escoger el AP al que estemos conectados para ver los niveles de potencia en tiempo real. Recordemos que esta es una aplicación de tipo “stumbler”, es decir que es sólo un detector, no sirve para hackear WLANs, sólo para mapearlas. Podremos comprobar cómo el nivel de potencia aumenta cuando caminamos en dirección al AP y disminuye si nos alejamos.

Wifi Analyzer



⚠ INV [redacted] (9c:d6:43: [redacted])

Canal actual: 6 Puntuacion: ★★★★★★★★★★★

Mejores canales: 12, 13, 14

Canal ▾

Canal 3 ★★★★★★★★★★

Canal 4 ★★★★★★★★★★

Canal 5 ★★★★★★★★★★

Canal 6 ★★★★★★★★★★

Canal 7 ★★★★★★★★★★

Canal 8 ★★★★★★★★★★

Canal 9 ★★★★★★★★★★

Canal 10 ★★★★★★★★★★

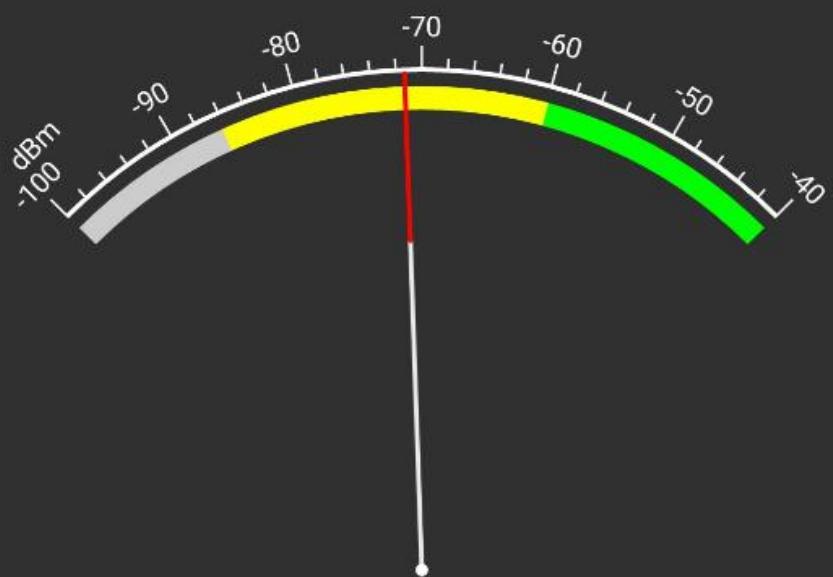
Canal 11 ★★★★★★★★★★

Canal 12 ★★★★★★★★★★

Canal 13 ★★★★★★★★★★

Canal 14 ★★★★★★★★★★

Wifi Analyzer

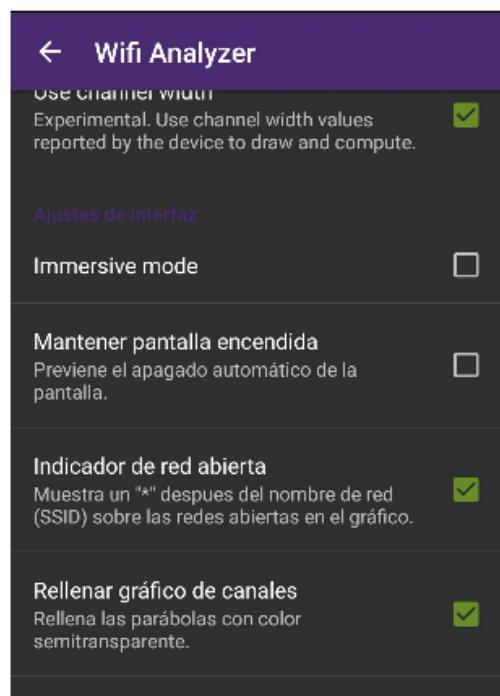


INV [REDACTED] (9c:d6:43: [REDACTED])

Sonido

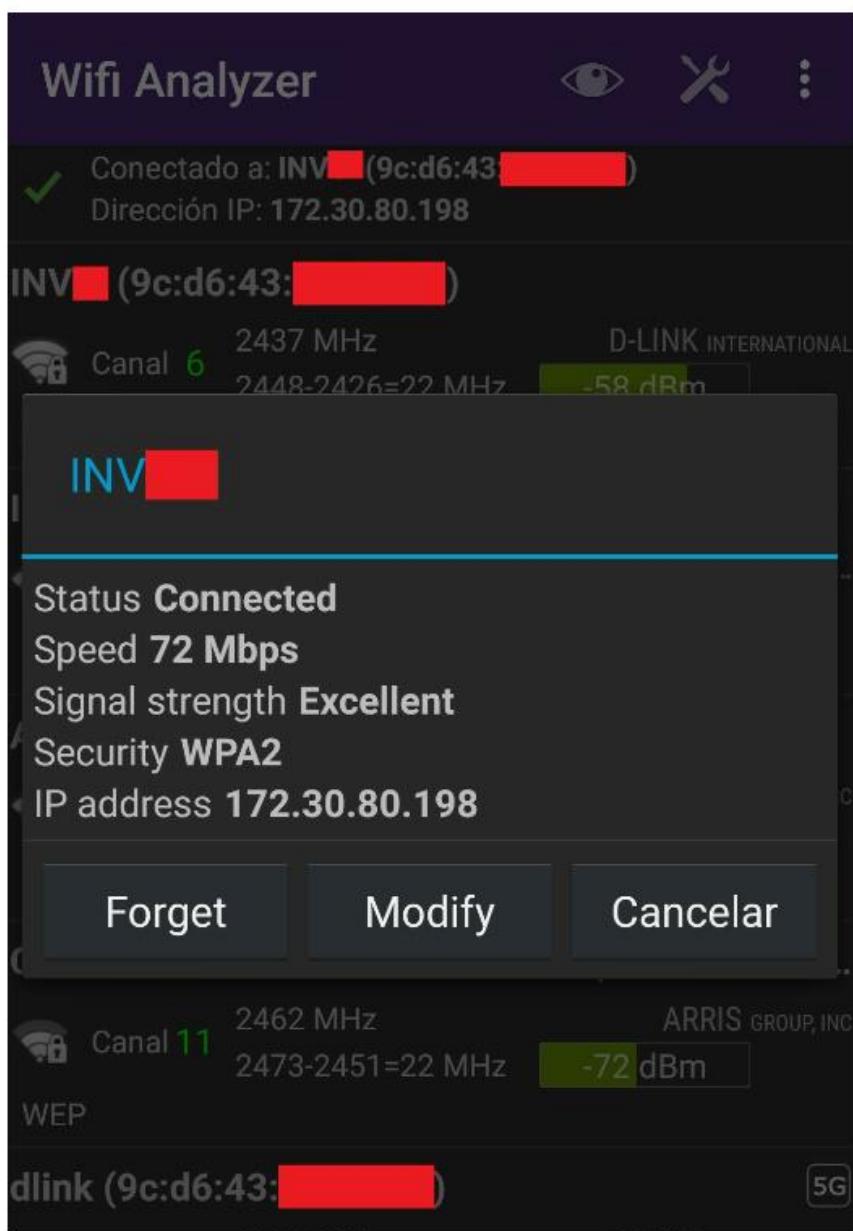
NO

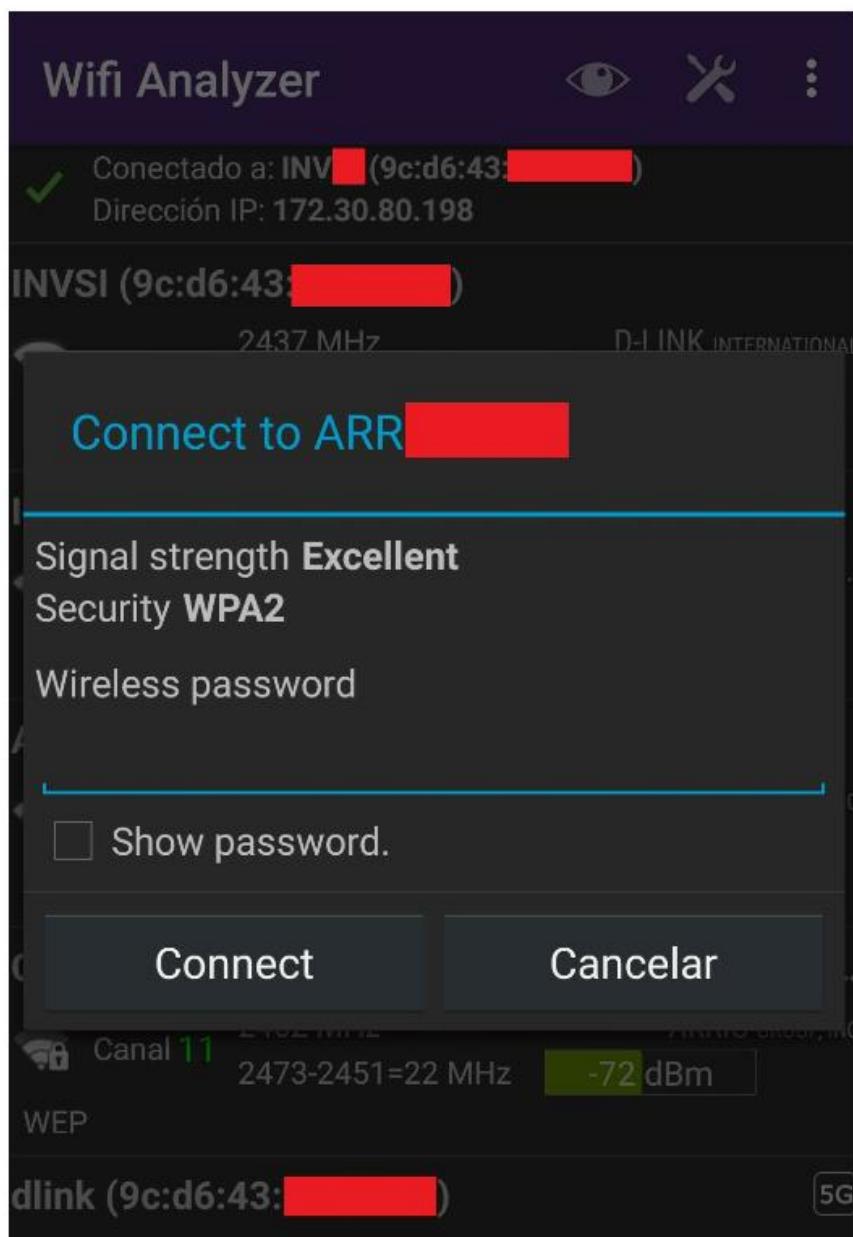
8. Wifi Analyzer tiene además opciones de configuración que podemos acceder escogiendo el ícono de herramientas en la parte superior. Una opción bastante útil es activar “Indicador de red abierta”. Con esto veremos un símbolo asterisco (*) al lado del nombre de una WLAN que no use autenticación.



9. Volvamos ahora a la vista con el listado de APs (ícono ojo -> Lista de AP). Si tocamos la WLAN a la que estamos conectados veremos información de la misma.

10. Si por el contrario tocamos una WLAN a la que no estemos conectados, entonces nos pedirá la clave de conexión si fuese una red con autenticación, o se conectará automáticamente si se tratase de una red abierta.





11. Tal y como hemos notado Wifi Analyzer es un stumbler muy útil y gratuito, además.

Recursos útiles

- **Artículo:** SANS Institute. (2002). A Guide to Wardriving. Sans.org. Recuperado en 2017, de <https://www.sans.org/reading-room/whitepapers/wireless/guide-wardriving-detecting-wardrivers-174>.
- **Vistumbler Wiki:** <https://github.com/RIEI/Vistumbler/wiki>.
- **Documentación de la suite Aircrack-ng:** <http://www.aircrack-ng.org/doku.php>.
- **Libro:** Burns, B., & Killion, D. (2007). Security power tools (1st ed.). Sebastopol, Calif.: O'Reilly.
- **Libro:** Ramachandran, V. (2015). Kali Linux wireless penetration testing beginner's guide: master wireless testing techniques to survey and attack wireless networks with Kali Linux (1st ed.).
- **Libro:** Pretty, B. (2017). Build an Aircrack Super Cluster: with Raspberry Pi (1st ed.). ISBN Canada.

