

Ekoparty 2025

(notes in Spanish, ekoparty is a security conference-event hosted in Buenos Aires)

Wardiving

es buscar redes wireless de acceso publico en un vehiculo en movimiento

Hermanito menor del Wardialing, se utilizaba en su momento para hacer mapeos de numeros de telefono (bluebox)

IEEE 802.11 = WIFI

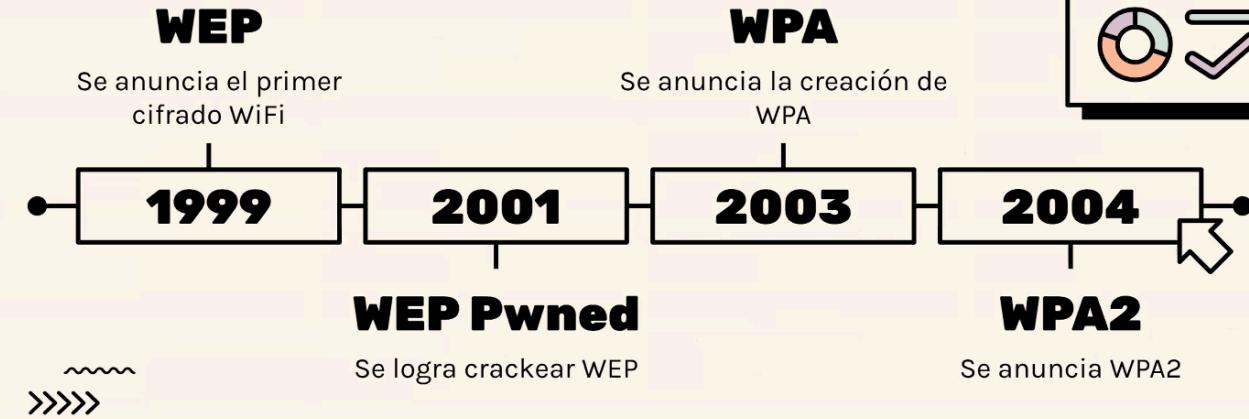
.....	YEAR	Frequency Band	Rate teórico
B	1999	2.4GHz	11 mbps
G	2003	2.4GHz	54 mbps
N	2009	2.4GHz 5.8GHz	600 mbps

normativas

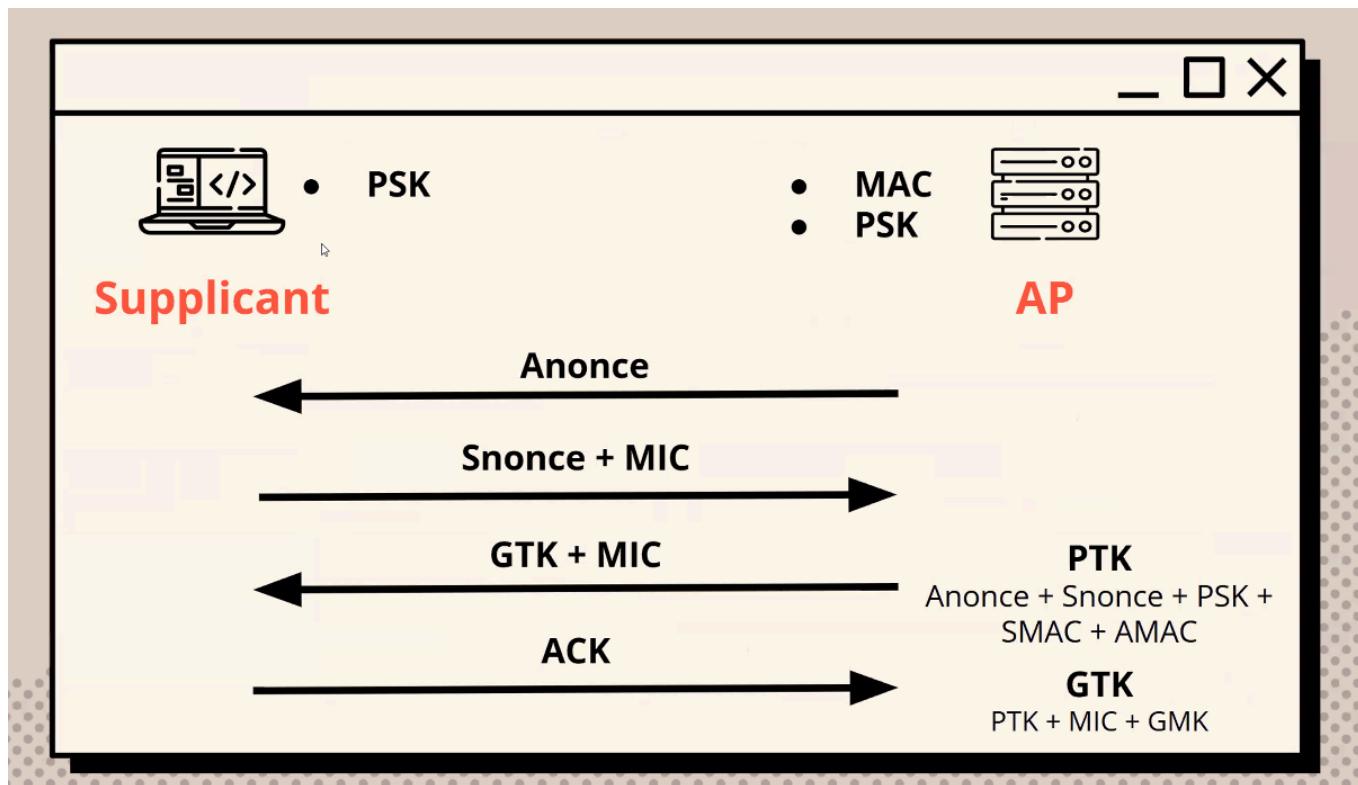
El rate teorico si bien va incrementando depende de la cantidad de hosts que esten conectadas a la misma porque se reparten el ancho de banda.

.....

Un poco de historia



empiezan a existir los protocolos de seguridad



Forward Handshake (WPA2 Y WPA)

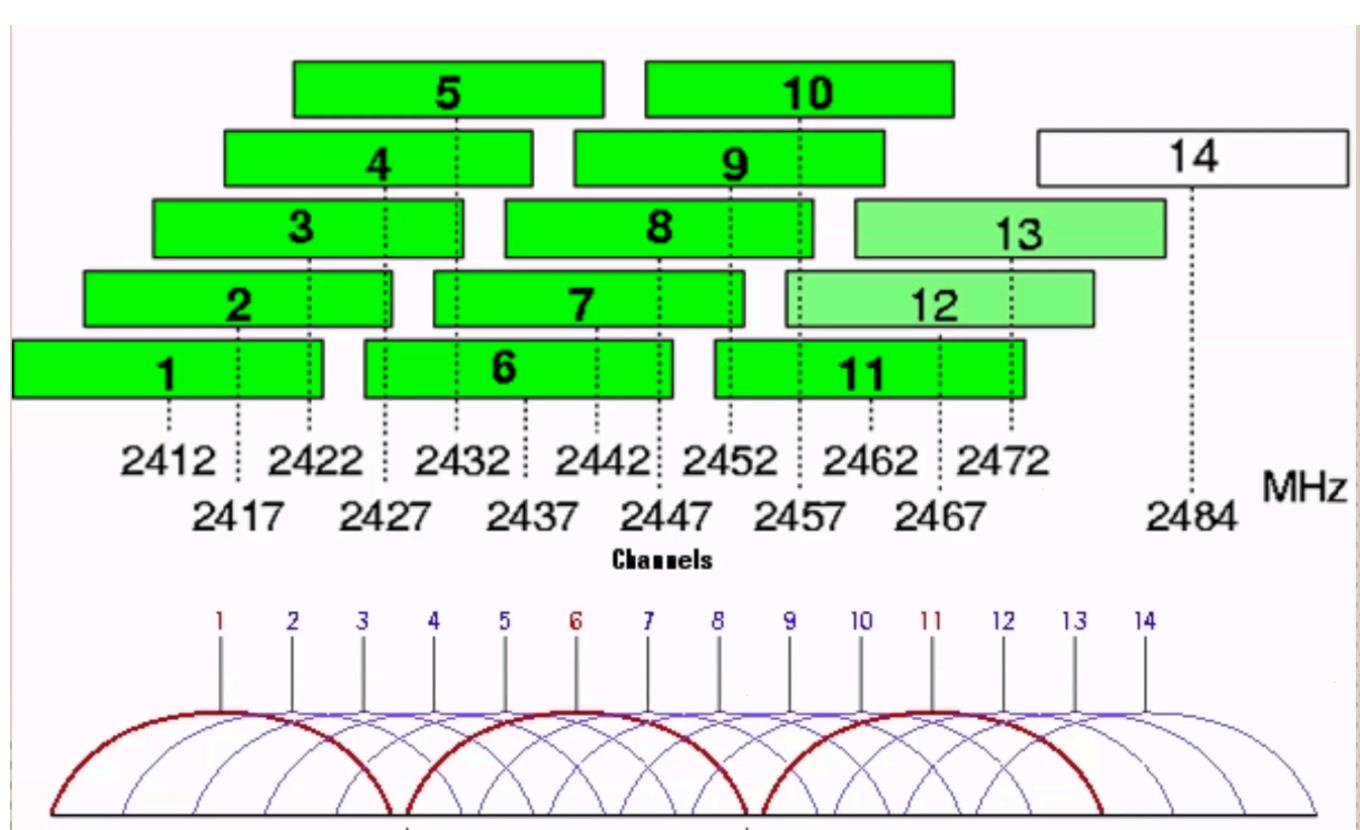
Access Point

1. se manda un numero aleatorio del AP al supplicant
2. hace exactamente lo mismo y genera un Snonce (numero aleatorio) + message integrity code
3. para formar el PTK que es el mensaje que se va a enviar, se requiere el Anonce, el snonce, el PSK (pre shared key, la contraseña) la mac del supplicant y la mac del access point
4. acknowledge

Como crackearlo: se intenta de-authenticar a los dispositivos conectados al access point, el supplicant va a intentar volver a conectarse y nosotros vamos a estar escuchando los mensajes que manda, cuando mande esos mensajes (encriptados) como se desencripta? separamos todas las partes (nonce, snonce, psk), se intenta separar las cosas que van a ser fijas de las que son dinámicas, como es la contraseña. Agarramos el mensaje y corremos un diccionario con distintas contraseñas, cuando el resultado sea exactamente igual al handshake, descubrimos cuál es la contraseña.

Tenemos un montón de caracteres que no entendemos, es imposible de leer, se separa lo que ya sabemos, y pasamos el diccionario por donde no sabemos

Es un ataque de fuerza bruta



canales 2.4GHz

podemos visualizar el solapamiento de los canales, separación de 22mhz por canal
los que no tienen solapamiento son el 11, el 6 y el 1.

hoy en día se pueden combinar canales para reducir disponibilidad y los routers modernos se adaptan a la capacidad de los canales

Hands on

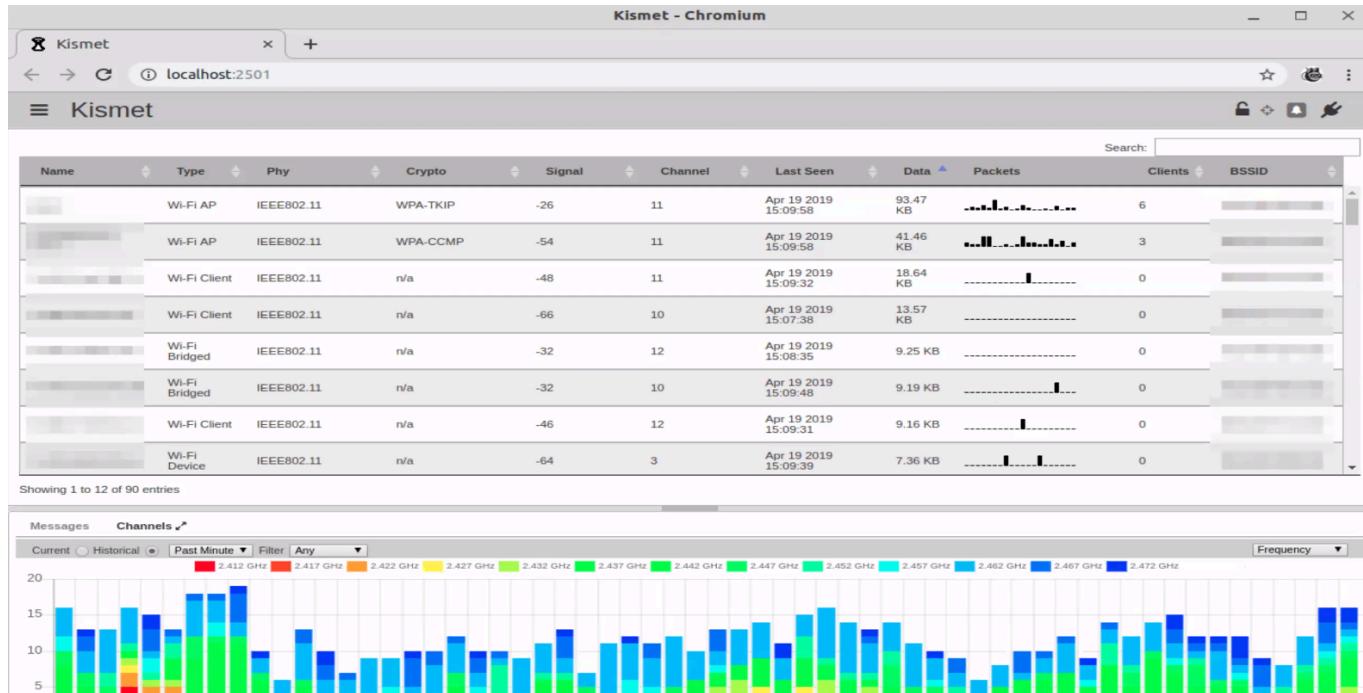
- Que necesitamos?

- un NIC, los que tienen capacidad de modo a monitor y que tengan capacidad de inyección de paquetes, (ALFA network)
- <https://articulo.mercadolibre.com.ar/MLA-1103677032-adaptador-de-red-wi-fi-usb-30-banda-dual-1900-mbps-JM> / https://es.aliexpress.com/item/1005005537887765.html?spm=a2g0o.productlist.main.1.187749e0FYAUpn&algo_pvid=2400f383-1ec6-4539-806b-e05f657e87a9&algo_exp_id=2400f383-1ec6-4539-806b-e05f657e87a9&algo_ext_f=%7B%22order%22%3A%229%22%2C%22eval%22%3A%221%22%7D&pdp_np_i=4%40dis%21ARS%21290904.28%21159997.36%21%21%211999.00%211099.45%21%402101ef5e17388818674916293e808b%2112000033457919161%21sea%21AR%210%21ABX&curPageLogUid=58BslXpG4Mff&utparam-url=scene%3Asearch%7Cquery_from%3AAALFA AC1900
- https://articulo.mercadolibre.com.ar/MLA-620233910-kit-auditoria-antena-yagi-24-dbi-usb-wifi-modo-monitor-JM#polycard_client=search-nordic&position=9&search_layout=stack&type=item&tracking_id=6e8155e5-6f44-4299-9742-c1b14e13895b ralink
- no conectar sin antena puesta

<https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html>

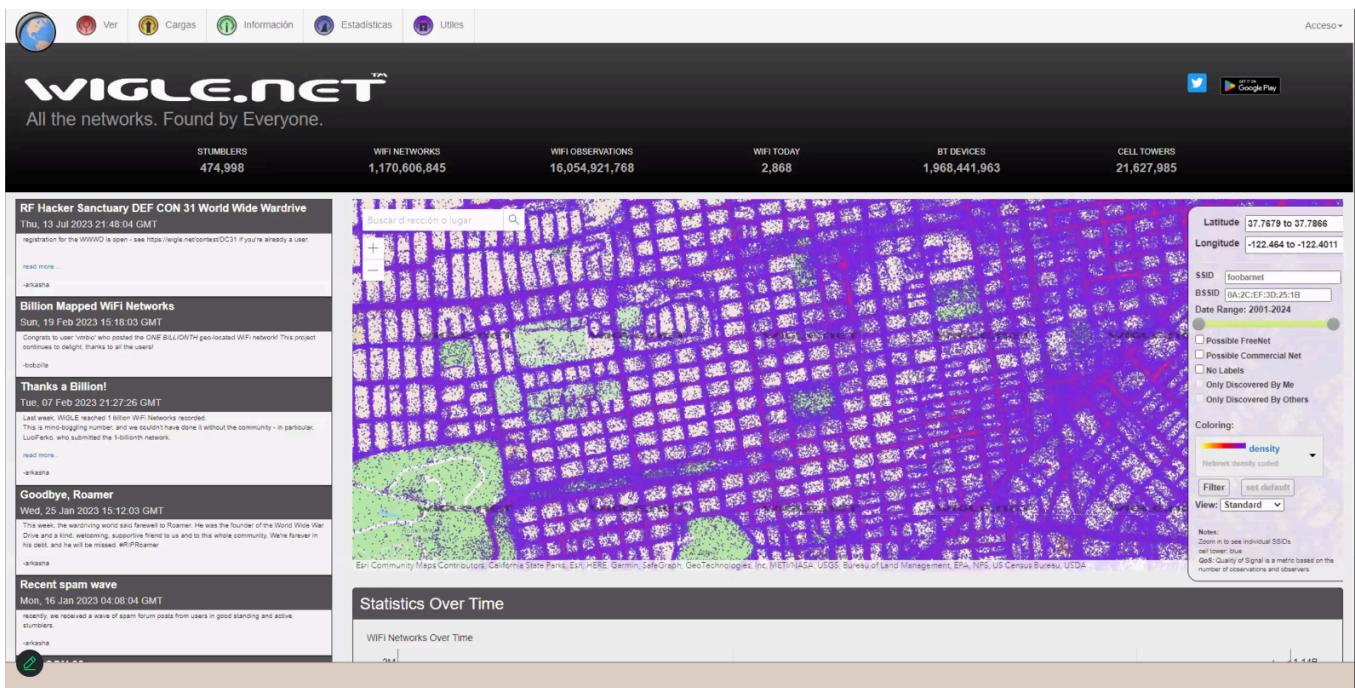
Aplicaciones

Kismet- Airodump- Wigle (android)



kismet

(no capturamos trafico porque es ilegal, solamente logeamos los beacons de announcements de los access points, informacion publica)



wiggle

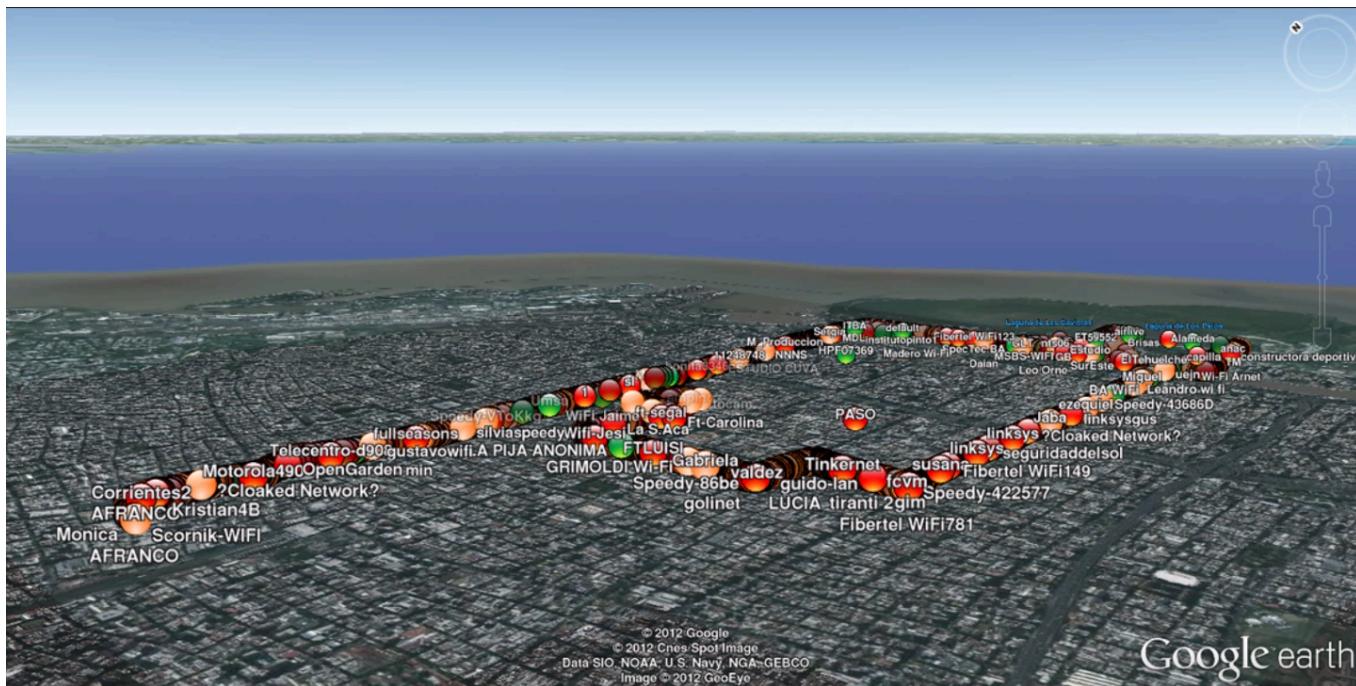
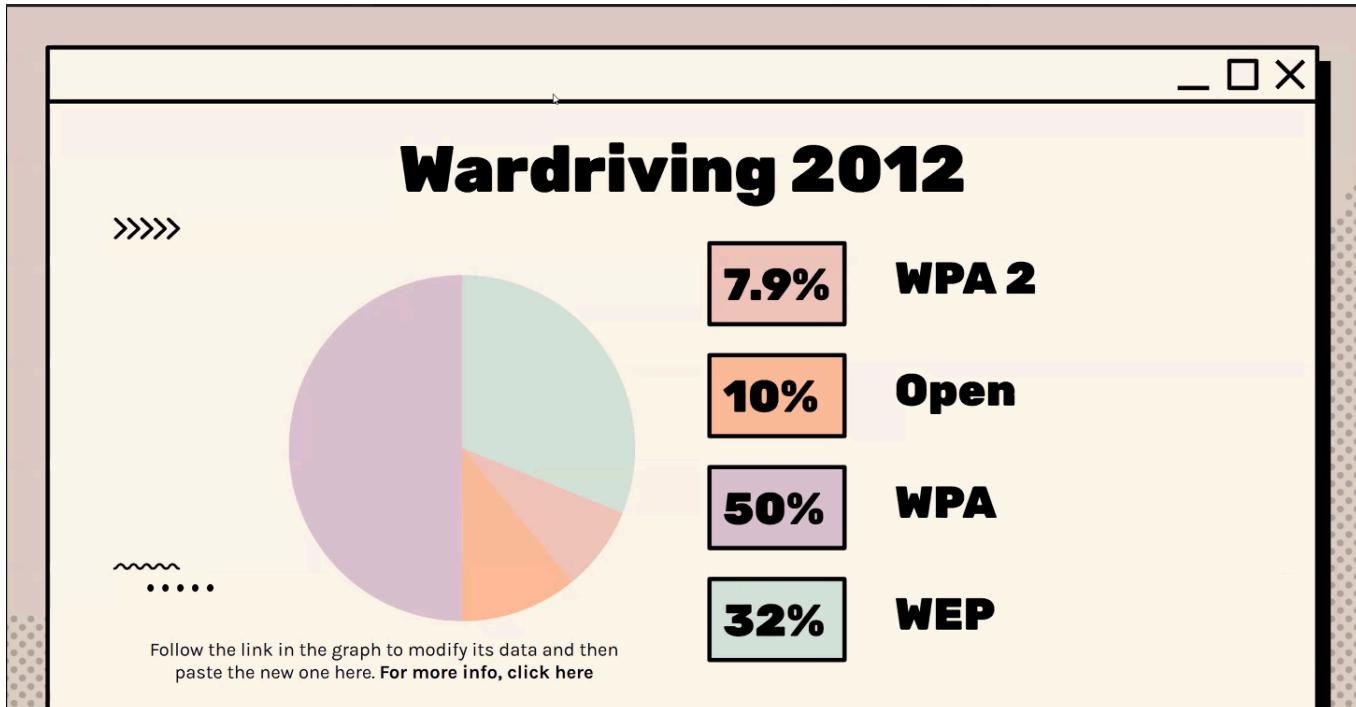
Geoposicionamiento

- dongle gps

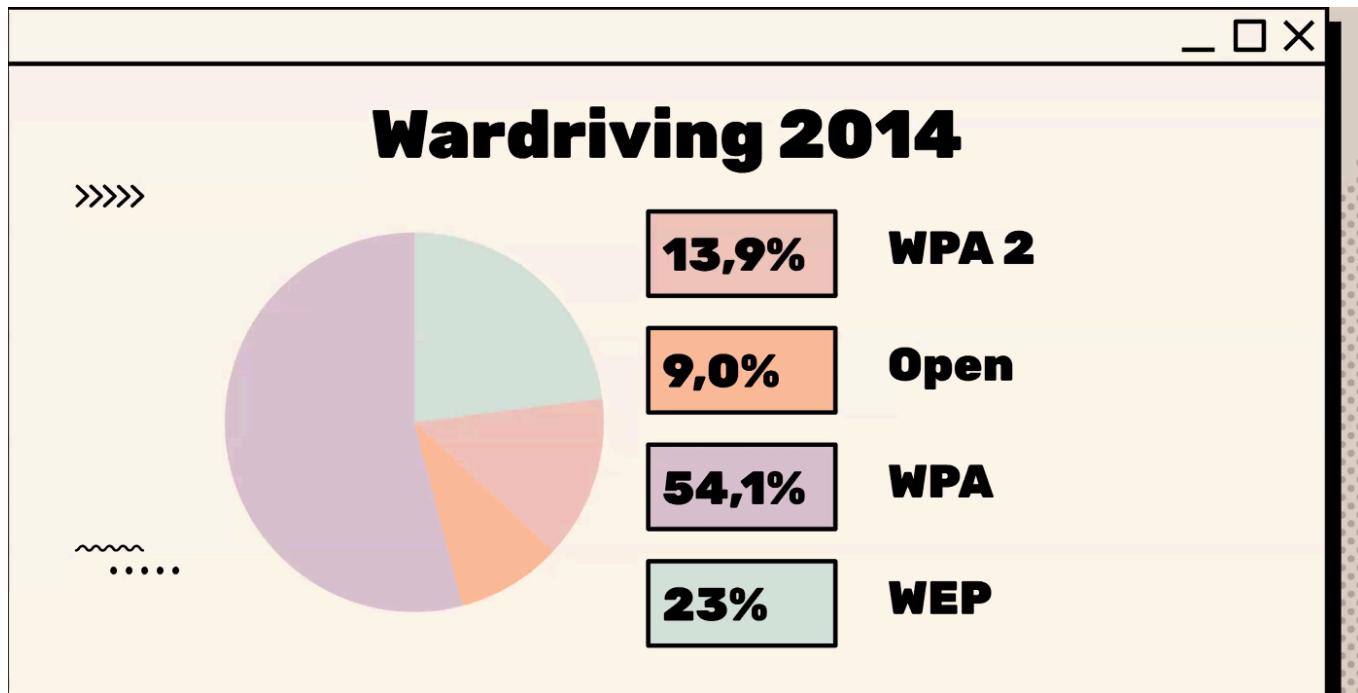


-
- GPSD dentro de linux
- se puede usar el del celular

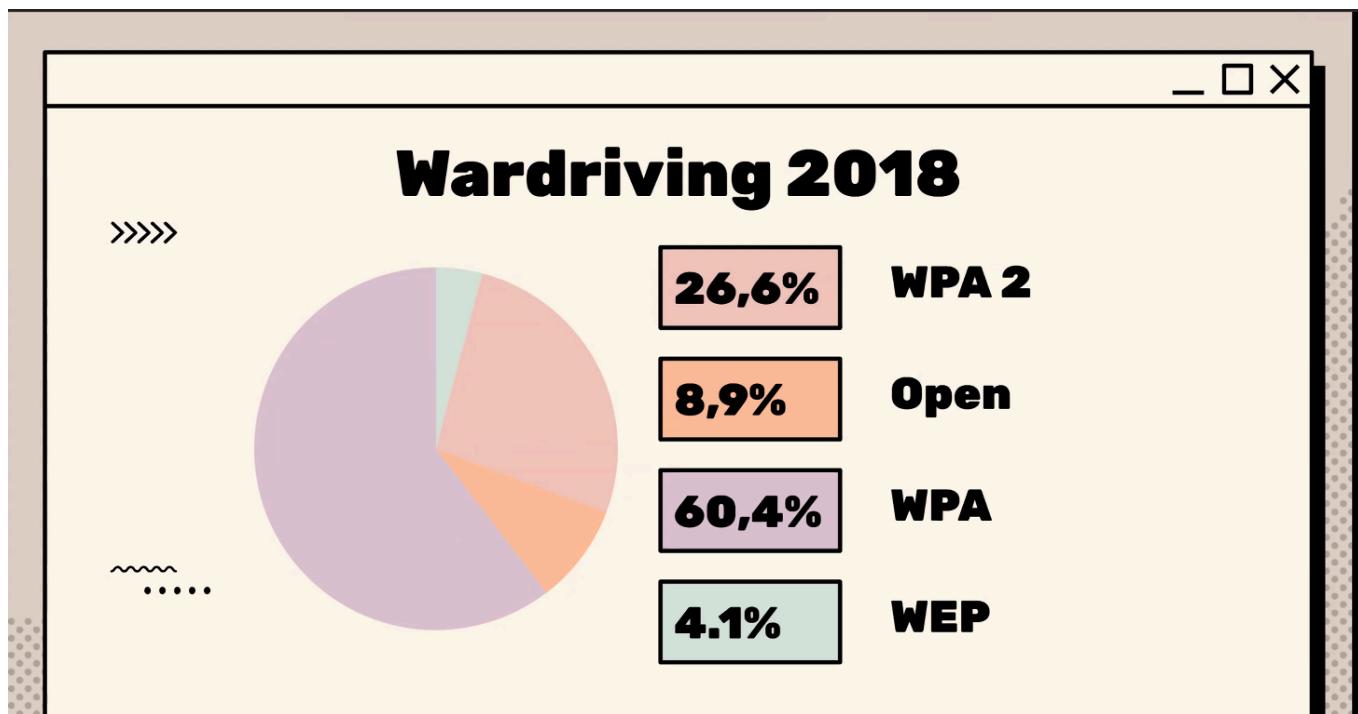
datos de años anteriores



2012



2018

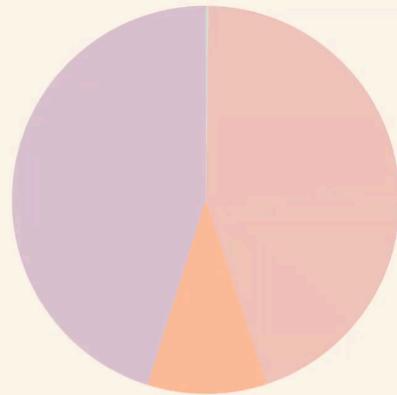


2014

en 2018 entre 20 a 25mil redes en BSAS

Wardriving 2021

>>>

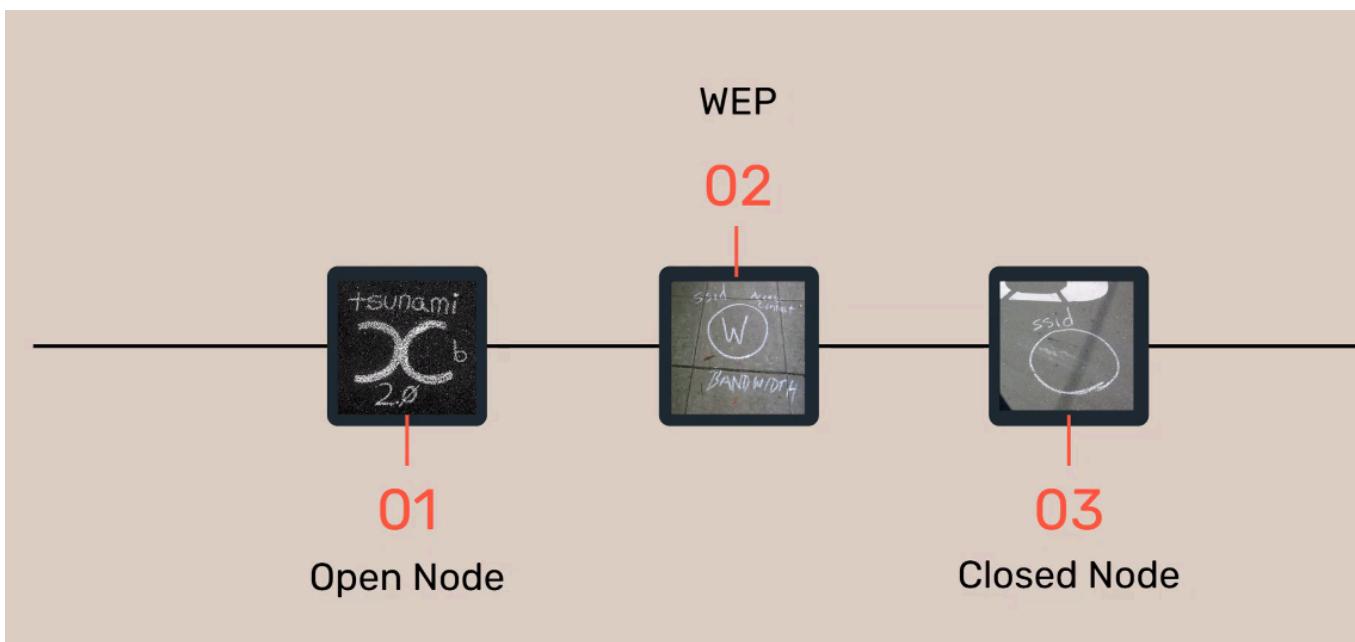
**WPA 2****9,9%****Open****45,1%****WPA****0,1%****WEP y WPA3**

~~~~~

\*2021

## Warchalking

- Marcado de redes inalámbricas en el mundo físico
- hobo symbols



ejemplos

# Hands on en kali

```
(kali㉿kali)-[~]
$ airmon-ng
```

```
(kali㉿kali)-[~]
$ sudo airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

PID Name
711 NetworkManager
30304 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0      wlan0          rtl8192cu    Realtek Semiconductor Corp. RTL8188RU 802.11n WLAN Adapter
          (monitor mode enabled)
```

sudo airmon-ng check kill para que no interfieran procesos con la placa de red y nos borre el progreso

kismet viene instalado

```
(kali㉿kali)-[~]
$ kismet -c wlan0mon --override wardrive
```