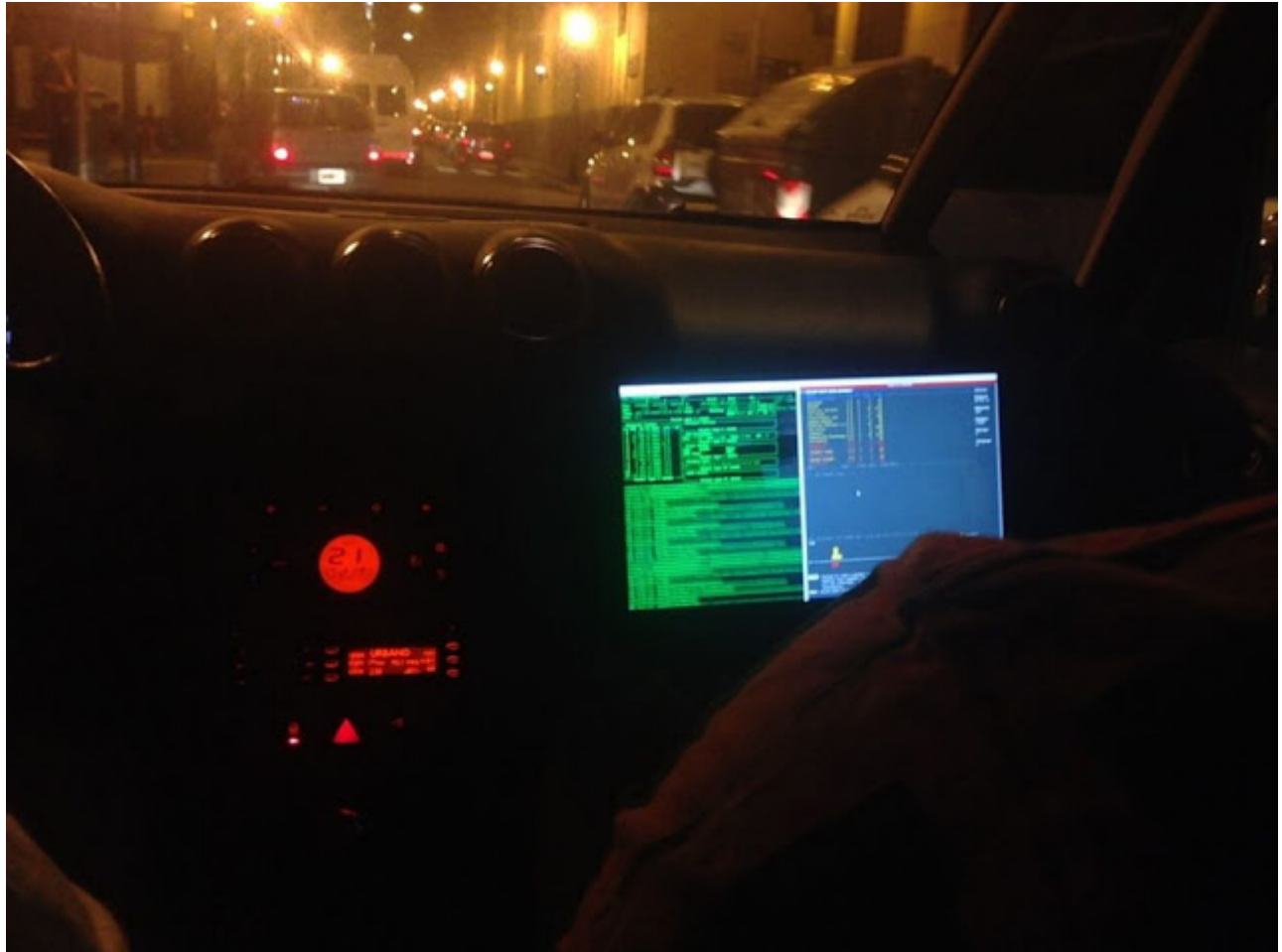




# Wardriving en KALI LINUX

[Cread Pag](#) mayo 21, 2018

Antes de empezar quisiera agradecer a toda la gente de EKOSPACE que ayudaron a vivir una experiencia con el wardriving.



Desde la EKOPARTY siempre pensé que era eso, pero solo puede subir a un colectivo de la ekoparty en su ultimo día donde solo era celebrar pero no me quejo la pase genial.



Ahora volví hacer un wardriving en EKOSPACE porque un amigo tenia herramientas entonces me puse a probar todas las herramientas para usarlo con KALI LINUX.

Pero antes de empezar vamos a ver

### ¿Qué es WARDRIVING?

**Wardriving** a la búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Implica usar un coche o camioneta y un ordenador equipado con Wi-Fi, como un portátil o una PDA, para detectar las redes.

### ¿Qué herramientas use?

Una ALFA una antena que omg era muy grande.



Luego usamos un GPS “Bu-353S4”



Luego usamos algunos software para hacer el escaneo. Pero antes de seguir, quisiera agradecer a “DIEGO” unos de los compañeros de va a la ekospace por haberme prestado algunas herramientas.

### **¿Qué software?**

Obviamente tenemos que tener un KALI LINUX actualizado y instalaremos lo siguiente.

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

```
sudo apt-get install -y screen gpsd libncurses5-dev libpcap-dev tcpdump libn1-dev  
gpsd-clients python-gps
```

Luego conectar nuestras herramientas y recuerda con

```
dmesg |grep ttyUSB0
```

```
dmesg
```

Puedes fijarte sobre su driver.

Ahora vamos a instalar la herramienta “KISMET”

```
apt-cache search kismet
```

```
apt-get install kismet
```

Tenemos que correr el ps

```
gpsd -n -N -D /dev/ttyUSB0
```

```
ps aux| grep gps
```

```
kismet
```

Luego es muy fácil de usar, colocar lo siguiente.

Yes – Para hacer automático server Kismet

start – Par iniciar kismet

Puedes configurar tu interface con kismet.

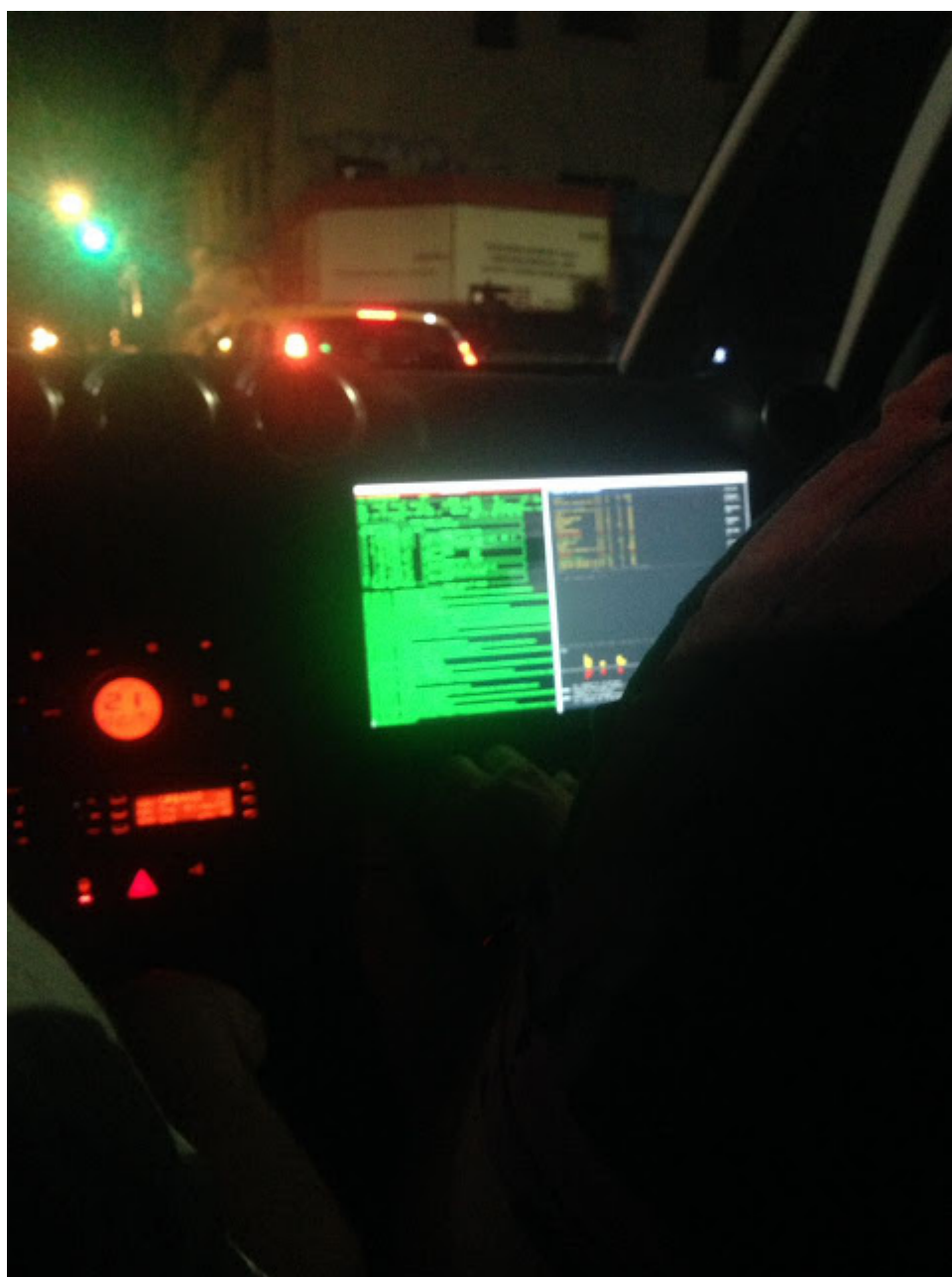
Lo tuve que probar si todo corría perfectamente con “GPSMON” en el balcón

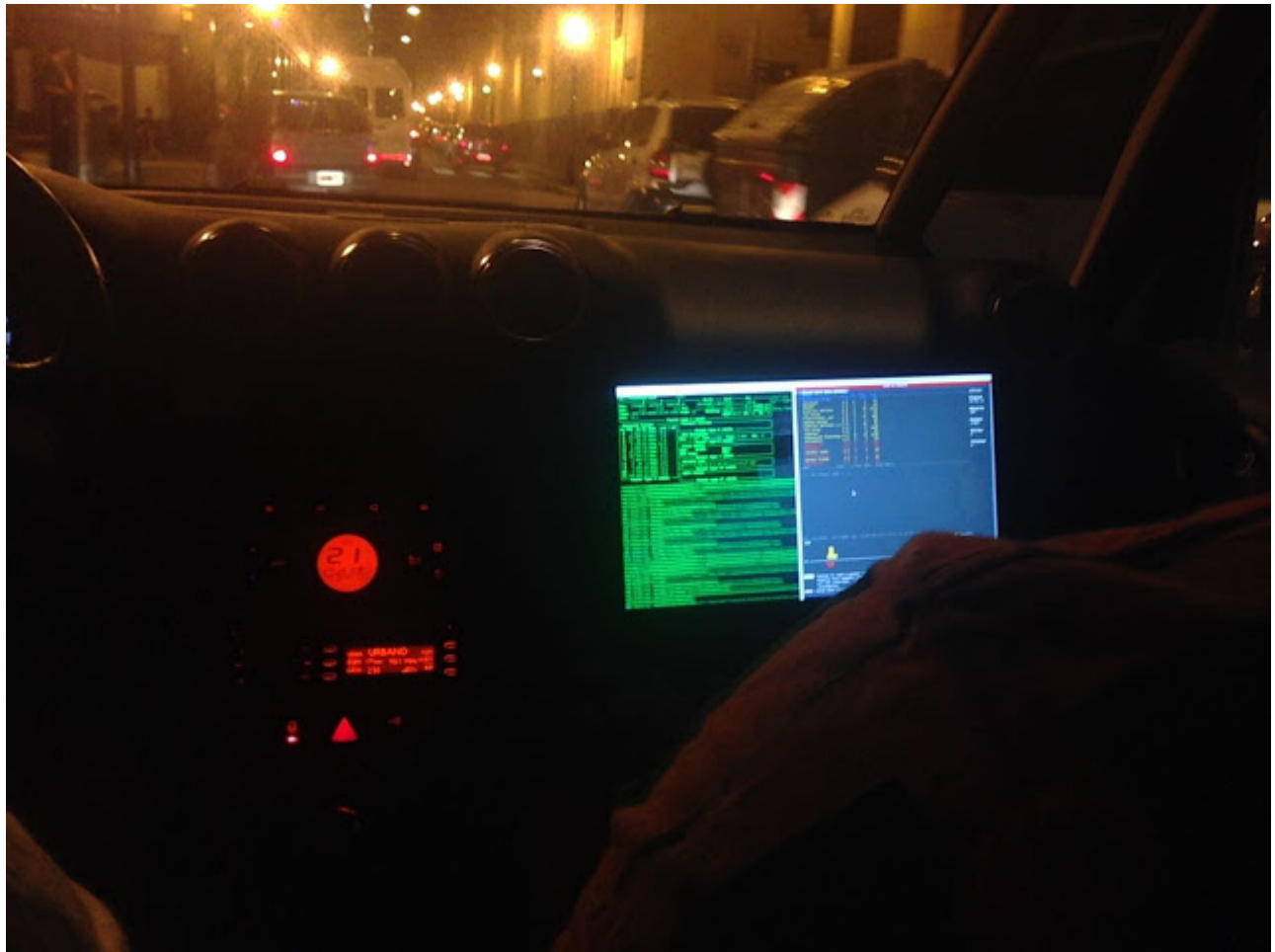
```
gpsmon
```





Y cuando teníamos todo listo nos fuimos a dar un paseo.





Hice un vídeo pero creo que luego lo publicare o puedes visitar la pagina de “EKOSPACE”  
Luego llegamos a nuestro espacio y como kismet te deja unos archivos en “HOME” tuvimos que exportarlo y continuar el proceso.

Por si das dudas el creador del código elimina su código te dejo el [pastebin](#)

Pero usamos el siguiente comando

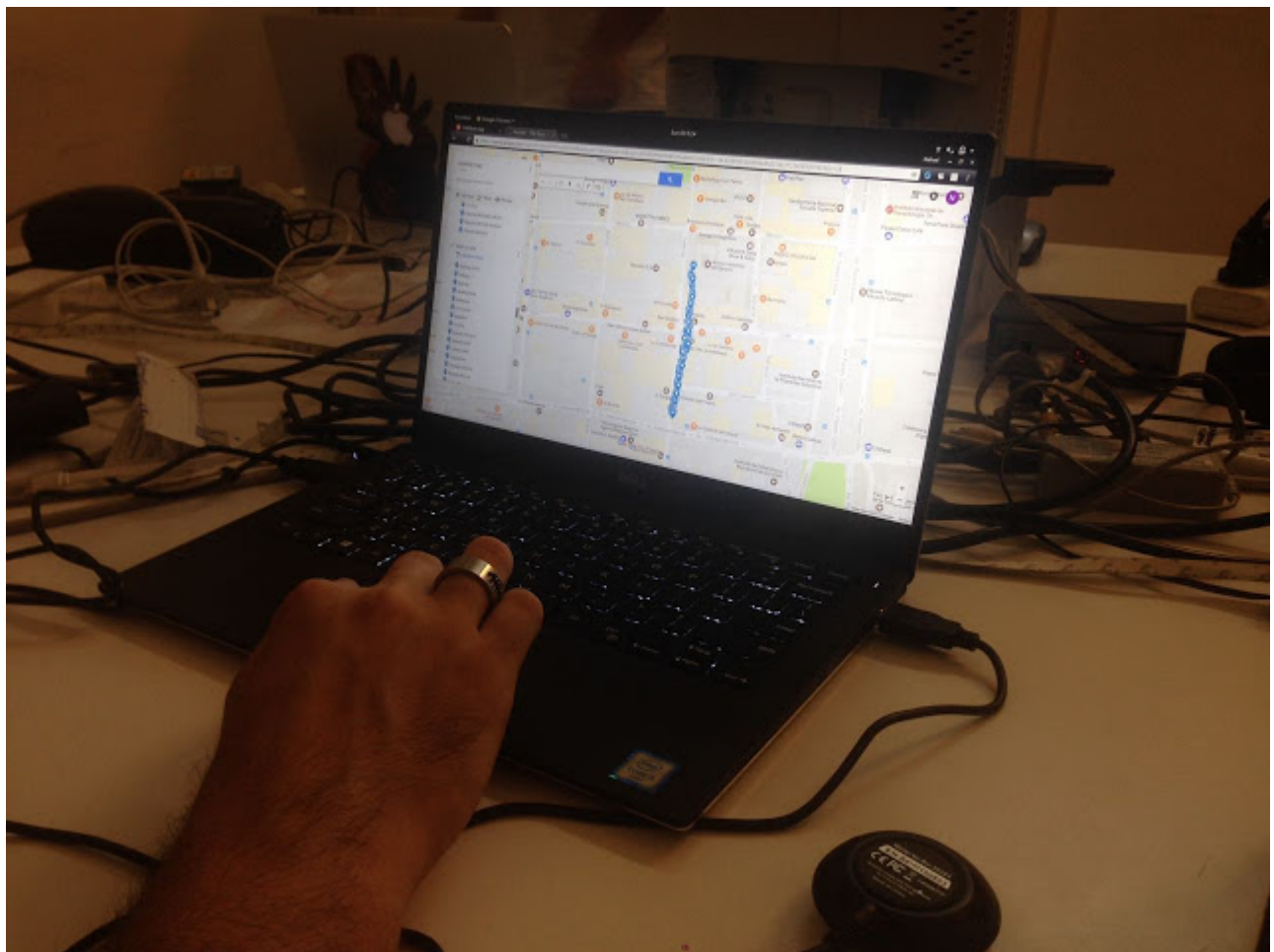
```
wget
```

```
https://gist.githubusercontent.com/ScottHelme/5c6869e17c3e9c8b2034dc8fc13e180b/raw/  
31c2d34f66748b6bd26415fd7d120c06b3d92eaf/netxml2kml.py -O netxml2kml.py
```

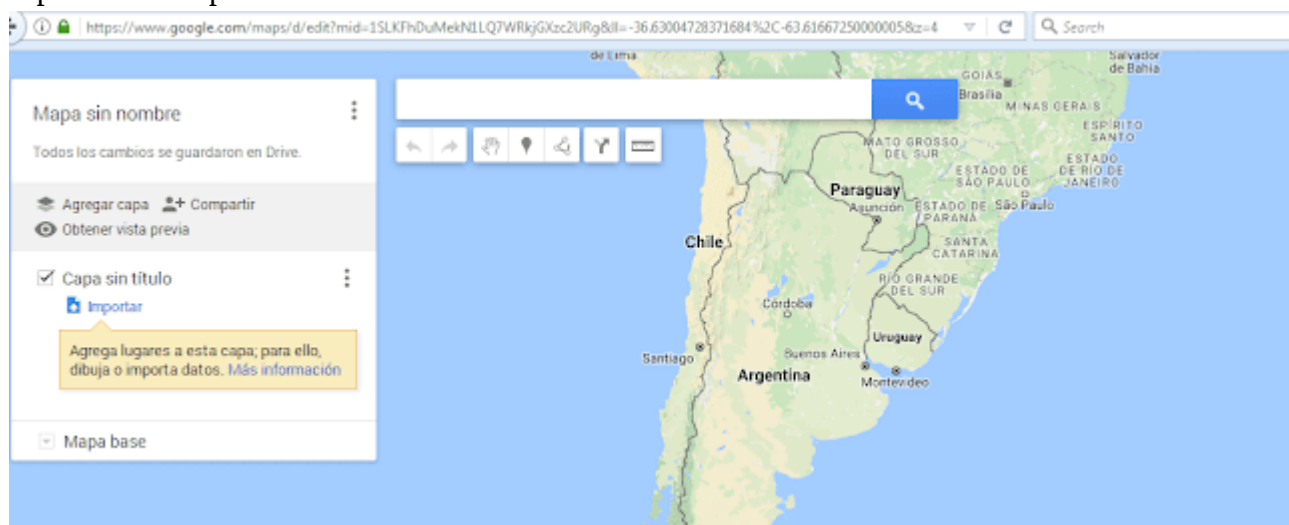
Exportamos todos.

```
python netxml2kml.py --kml -o output *.xml
```





Ahora intenta hacerlo desde Google y súbelo el resultado desde [aquí](#).  
Así podrás ver exportarlo



Lo intente hacer con mi maquina pero mi batería no iba aguantar el viaje entonces todo el proceso se logro. En caso de alguna configuración hacer lo siguiente

```
sudo nano /etc/default/gpsd
```

```
START_DAEMON="true"
GPSD_OPTIONS="-n"
```

```
DEVICES="/dev/ttyUSB0"  
USB_AUTO="true"  
GPSD_SOCKET="/var/run/gpsd.sock"
```

Y listo espero que lo pruebes y te diviertas. Muchas Gracias a ekospace, no te olvides en compartirlo para seguir escribiendo.