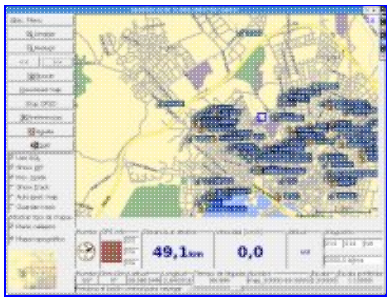
Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Wardriving - Localizando redes wireless (92290 lectures)

Per **David Martín**, ***Suki*** (http://sukiweb.net)

Creado el 20/04/2004 15:11 modificado el 20/04/2004 15:11



*(1) La búsqueda de redes inalámbricas se denomina **wardriving**. Consiste en localizar redes wireless (encriptadas o no) para conocer su posición.*

Esto se consigue paseando con un equipo dotado de una tarjeta de red wireless y opcionalmente con un GPS para que nos ayude a posicionar en un mapa cada una de las redes localizadas.

Con GNU/Linux tenemos excelentes herramientas de wardriving. Es este pequeño artículo voy a explicar como utilizar Kismet(2) y gpsdrive(3) en conjunto. Además, para acomodarnos la búsqueda, haremos que nuestro equipo nos hable, indicándonos cuando localiza una red, su nombre y otras cosas más.

Primero debemos instalar los diferentes paquetes. Voy a explicar la forma de hacerlo en debian, aunque los pasos a seguir para configurar los mismos programas no difieran practicamente nada en las diferentes distribuciones.

- **Kismet** es el programa que utilizaremos para localizar las redes wireless con nuestra tarjeta de red. Es un programa basado en consola con muchísimas opciones.
- **Gpsdrive** es la utilidad que nos mostrará sobre un mapa nuestra posición y la de las redes que encontremos, necesitando para esto un receptor GPS.
- **Festival** es un sintetizador de voz, que utilizaremos para escuchar a viva voz de nuestro equipo las alertas de Kismet.

Instalamos entonces festival, kismet y gpsdrive de la siguiente manera:

```
apt-get install kismet gpsdrive festival festvox-ellpc11k
```

El último paquete especificado es el de idioma, para poder escuchar las alertas de kismet en castellano.

Ahora vamos a configurar el archivo de configuración de kismet /etc/kismet/kismet.conf
Este archivo puede variar mucho, dependiendo de como lo quiera personalizar cada uno. Yo simplemente indicaré los pasos básicos a seguir para que funcionen las opciones mínimas, luego cada uno que utilice su ingenio para mejorarlo :)

Activamos el soporte de GPS en el kismet.

```
# Do we have a GPS?
gps=true
```

Esto lo ponemos para que Festival nos hable en castellano.

```
# Does the server have speech?
speech=true
```

```
# Server's path to Festival
festival=/usr/bin/festival --language spanish

# How do we speak?  Valid options:
# speech    Normal speech
# nato      NATO spellings (alpha, bravo, charlie)
# spell     Spell the letters out (aye, bee, sea)
speech_type=speech
```

Y ahora le decimos las frases que tiene que pronunciar cada vez que detecte una red nueva.

```
speech_encrypted=Red detectada,  %s, canal %c, Red encriptada.
speech_unencrypted=Red detectada,  %s, canal %c, Red abierta.
```

Para que utilice el formato métrico.

```
# Use metric measurements in the output?
metric=true
```

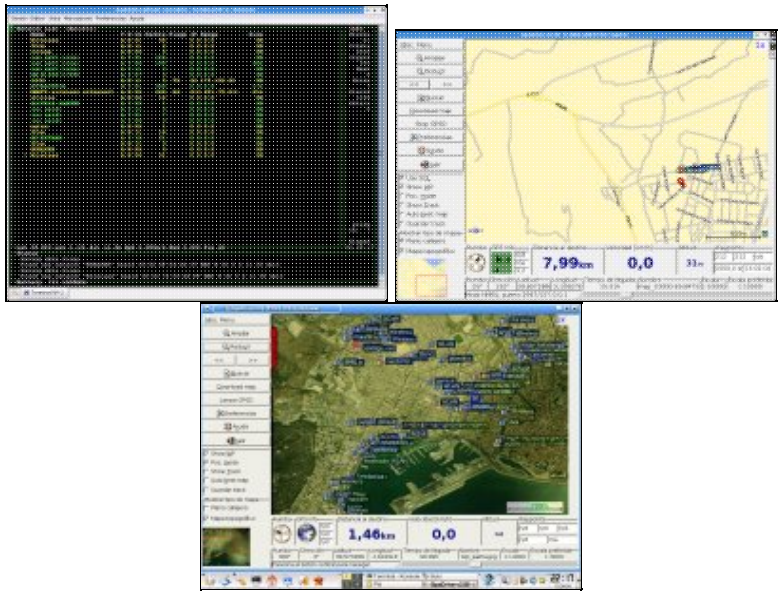
Si no tienes servidor SQL instalado, o simplemente te conformas con latitud, longitud y MAC de la red encontrada, puedes utilizar este sistema que va escribiendo en un archivo los datos que va encontrando.

```
# Do we write waypoints for gpsdrive to load?
# recent versions of GPSDrive's native support of Kismet.
waypoints=true
# GPSMap waypoint file.  This WILL be truncated.
waypointdata=%h/.gpsdrive/way_kismet.txt
```

Pero si realmente quieres tener más datos disponibles, lo mejor es utilizar una base de datos de gpsdrive para ello. Yo he utilizado mysql, creando la base de datos **geoinfo** y luego las tablas del archivo: /usr/share/gpsdrive/create.sql

```
$> mysqladmin create geoinfo

$> mysql geoinfo </usr/share/gpsdrive/create.sql
```



Vista aerea de Palma (Gracias Celso) (4)

Ahora llega el turno de poner en marcha el gpsdrive. Lo configuraremos presionando sobre el botón preferencias, seleccionando las opciones de sql en el caso de que queramos utilizarlo.

Ya estamos listos para arrancar los dos programas a la vez. Lanzamos el gpsd desde el gpsdrive y arrancamos el kismet.
Desde este momento ya estamos localizando redes wireless a nuestro alrededor. Cualquier red que entre en nuestra cobertura lanzará un aviso hablado a través de nuestro kismet, indicándonos su nombre SSID, el canal en que opera y si esta abierto o encriptado. Unos segundos después de ser localizado, sera visible en el mapa GPS.

Para ver algunas capturas de pantalla más grandes, he dejado un galeria justo aquí[4].

Lista de enlaces de este artículo:

1. http://bulma.net/body.phtml?nIdNoticia=2015
2. http://www.kismetwireless.net/
3. http://gpsdrive.kraftvoll.at/
4. http://bulma.net/~david/gpsdrive/images.html

E-mail del autor: suki_ _ARROBA_ bulma.net
Podrás encontrar este artículo e información adicional en: http://bulma.net/body.phtml?nIdNoticia=2015