

Kismet Mini–mini–howto: Una guia para Mendoza–Wireless

Harpo MAxx

harpo@lugmen.org.ar

Versión 0.3 (\$Id: Kismet–HOWTO.sgml,v 1.1 2003/09/09 23:20:21 harpo Exp \$)

Tabla de contenidos

1. [Razon de este documento.](#)
 - 1.1. [Que incluye este documento?](#)
 - 1.2. [Que no incluye este documento.](#)
2. [Que es Kismet y por que me puede servir.](#)
3. [Consiguiendo Kismet.](#)
4. [Configurando Kismet](#)
 - 4.1. [Que programas incluye Kismet](#)
5. [Editando kismet.conf.](#)
6. [Utilizando Kismet](#)
 - 6.1. [Ejecutando por primera vez](#)
 - 6.2. [Investigando el interface Curses.](#)
 - 6.3. [Algunas Opciones mas del interfaz Curses.](#)
 - 6.4. [Filtrando por direccion MAC.](#)
 - 6.5. [Usando la placa de Sonido](#)
 - 6.6. [Analizando los logs.](#)
7. [Comentario Final](#)

Tabla de contenidos

1. [Razon de este documento.](#)
 - 1.1. [Que incluye este documento?](#)
 - 1.2. [Que no incluye este documento.](#)
2. [Que es Kismet y por que me puede servir.](#)
3. [Consiguiendo Kismet.](#)
4. [Configurando Kismet](#)
 - 4.1. [Que programas incluye Kismet](#)
5. [Editando kismet.conf.](#)
6. [Utilizando Kismet](#)
 - 6.1. [Ejecutando por primera vez](#)
 - 6.2. [Investigando el interface Curses.](#)
 - 6.3. [Algunas Opciones mas del interfaz Curses.](#)
 - 6.4. [Filtrando por direccion MAC.](#)
 - 6.5. [Usando la placa de Sonido](#)
 - 6.6. [Analizando los logs.](#)
7. [Comentario Final](#)

1. Razon de este documento.

Este documento surge simplemente para servir como guía a la gente de que todavía está en periodo de pruebas antes de su ingreso a Mendoza–Wireless. <http://www.mendoza-wireless.net.ar> (Like Me!!!)

1.1. Que incluye este documento?

Este documento, pretende ser una guía o un breve resumen de parte de los README y las FAQ que se incluyen en la documentación de Kismet, además de el aporte que se puede dar basado en la experiencia personal en el uso de Kismet dentro de la MW.

Fundamentalmente está orientado a la experiencia que he tenido usando kismet con placas con chipset Prism2.x (DLink 520, Compaq WL200). Como en otros de mis pequeños aportes de documentación, aclaro que no soy un Guru de Kismet, ni mucho menos de los enlaces wireless 802.11(a|b). :)

1.2. Que no incluye este documento.

Este documento *NO* pretende ser un *MANUAL COMPLETO* de como utilizar Kismet y toda la gama de posibilidades que este programa ofrece. Para esto es aconsejable una lectura a conciencia la gran cantidad de README que vienen con la documentación de Kismet.

2. Que es Kismet y por que me puede servir.

Kismet es un sniffer para redes wireless basadas en la norma 802.11b de la IEEE. El cual ha resultado ser de mucha utilidad para la detección de problemas de conectividad en las primeras etapas del enlace de un nodo a la MW.

Como cualquier sniffer Kismet coloca la placa de red en un modo Promiscuo (modo RF monitor) y podemos ver que es lo que está pasando en las capas más bajas de nuestra Red.

Hay que tener en cuenta que no todas las placas tienen la posibilidad de pasarse a modo Monitor, y aun en algunos casos en que la placa posea dicha capacidad, no todos los drivers lo tienen soportado.

Imagénlo como un ethereal <http://www.ethereal.org> pero para conexiones wireless.

Algo realmente interesante es que si la máquina dispone de una placa de sonido Kismet da la posibilidad de ejecutar sonidos frente a ciertos tipos de eventos, particularmente a mi me resultó muy útil esto último, ya que muchas veces tenía que subir al techo de casa e ir moviendo la antena, y no tenía a nadie abajo mirando el monitor de Kismet y avisándome cada vez que detectaba una nueva red o cada vez que habían paquetes viajando por alguna de las redes encontradas.

Kismet se encuentra entre las primeras pruebas a realizar, ya que al permitir ver lo que está "viajando" por el aire, podemos decir que si no vemos nada con Kismet, entonces *ESTAMOS EN PROBLEMAS!!!*

3. Consiguiendo Kismet.

Kismet viene en la distro que uso habitualmente (Debian Sid), por lo que no tengo más que hacer un

```
harpo@wired# apt-get install kismet
```

y salgo andando.

Pero tengo entendido que muchas otras distros lo incluyen entre sus paquetes.

Como siempre si se sienten alocados, puede bajarse la última versión de kismet de la homepage del proyecto. <http://www.kismetwireless.net> y seguir los pasos que allí se indican.

La última versión estable a la hora de escribir este documento es la versión 2.8.1, sin embargo en mi distro la versión que existe es la 2.6.2 por lo que desgraciadamente este documento se basará principalmente en esa versión.

4. Configurando Kismet

La configuración de kismet es el archivo ubicado en `/etc/kismet/kismet.conf` (o el lugar que corresponda si no usan Debian)

4.1. Que programas incluye Kismet

Antes de seguir con la configuración, vale comentar que las últimas versiones de kismet constan de 6 programas.

kismet_server: Este es el corazón de kismet, el cual corre como demonio y es quien se encarga de todas las tareas de sniffing. Como clásico modelo Cliente/Servidor permite varios clientes en distintas máquinas analizando la misma ráfaga.

kismet_hooper: Programa que va saltando de canal en canal, así poder poder ver `_TODO_` lo que está pasando en el aire.

kismet_monitor: un script que dependiendo el tipo de chipset y driver intentará poner la placa en modo monitor. Con la última versión de hostap, hay que hacerlo a mano. (esto último se soluciona fácilmente editando el script).

kismet_unmonitor: hace lo inverso al anterior.

kismet_curses: este es el cliente de kismet. Permite seleccionar 2 tipos de GUI distintos, como así también la dirección y puerto en donde corre `kismet_server`.

kismet: por último este script es el comúnmente usaremos, ya que se encarga de levantar el server y el cliente, como así también el hooper y el paso a modo monitor (estos 2 últimos, dependerá de la configuración que hayamos seleccionado).

5. Editando kismet.conf.

Bueno ahora vamos a lo bueno. Vamos a tocar solamente las opciones necesarias para tener kismet andando.

Estas son las tres principales opciones que tenemos que tocar en el archivo de configuración de kismet.

```
capinterface=wlanX|ethX
```

Obviamente seleccionamos el interfaz que queremos poner en modo monitor, normalmente wlan0 o eth0 serian opciones validas.

```
captype=pcap|prism2
```

Esta opcion permite seleccionar el motor de captura que va usar kismet, normalmente uno creeria que deberiamos seleccionar prism2 como el motor por defecto, sin embargo no es asi, a partir de las ultimas versiones de los drivers *wlan-ng* y *hostap*, la opcion adecuada es pcap. Que como se imaginan no otra que la vieja y querida *libpcap* que usan *tcpdump* y *ethereal* entre otros muchos programas. Aunque ha sido especialmente modificada para trabajar con redes wireless.

```
cardtype=prism2_pcap
```

En la version 2.8.1 la sintaxis cambio y para configurarla usar la seccion source siguiendo este orden `source=capture_cardtype,capture_interface,capture_name`

Para el caso puntual de una configuracion usando hostap

```
source=prism2_hostap,wlan0,Kismet
```

Aca tenemos que seleccionar nuestro driver, hay una gran cantidad de drivers que podemos elegir, nosotros los chicos prism2.x deberiamos jugar con *prism2_pcap* si usamos *wlan-ng* o *prism2_hostap* si usamos hostAp. ** Falta ver como hacerlo andar con las Samsung **

Si queremos que el script kismet lance automaticamente el **kismet_monitor** y **kismet_hooper**. Deberiamos setear :

```
auto_monitor=true  
auto_hooper=true
```

En la version 2.8.1 permite seleccionar logeo de capa fisica (PHY) y de los beacons que el AP manda. Es recomendable colocar estas opciones como true

```
beaconlog=true  
phylog=true
```

Hay muchas otras opciones que podriamos tocar, pero por ahora tenemos lo basico como para para salir a sniffear.

6. Utilizando Kismet

6.1. Ejecutando por primera vez

Si las cosas salieron OK, entonces escribiendo:

```
harpo@wired# kismet
```

en la línea de comando deberíamos salir andando como toro (coronel's dixit)

A mi me paso utilizando el driver hostap, kismet_monitor no sabia como ponerla en modo monitor a la placa, por lo que tuve que hacerlo yo manualmente.

```
harpo@wired# iwconfig wlan0 mode monitor;kismet
```

Por supuesto que si activamos el modo monitor de manera manual entonces debemos comentario la línea

```
auto_monitor=true
```

del archivo de configuración.

6.2. Investigando el interface Curses.

El interfaz Curses de kismet es realmente completo, tiene una gran cantidad de opciones, así que vamos a ir comentando las que a mi me fueron de utilidad.

La interfaz de Kismet consta de 3 pantallas y varias ventanas de tipo popup. La ventana principal es donde aparecerán las diversas "Redes" que podemos llegar a ver.

La ventana de estadísticas, donde se puede llevar un conteo de los paquetes recibidos, el tiempo, etc.

Por último la ventana de estado en donde se remarcan los últimos eventos, como ser redes descubiertas, IPs, direcciones MAC, etc

```
Network List
Name           T W Ch Packts  Flags  IP Range
!lugmen        A N 6  1243          0.0.0.0
.centro        A N 9  2121
```

Figura 1.

En mis pruebas en distintos puntos de Mendoza era común cruzarse con varias redes wireless más allá de la MW. En la Figura 1 como vemos tenemos 2 redes "lugmen" es el SSID del AP de MW y "centro" que vaya uno a quien pertenece jeje.

Ahora vamos a interpretar esto un poco. Al lado de Name encontramos un signo de exclamación (!) un punto (.) o simplemente nada (), esto nos indica el tiempo que ha pasado desde que se recibió un paquete en esa red.

- (!) Indica actividad detectada en los últimos 3 segundos.
- (.) Indica actividad detectada en los últimos 6 segundos.
- () No hay actividad.

La "T" nos indica el tipo de red, siendo (A) para AP Mode y (H) para AD–HOC Mode.

La "W" indica si esta utilizando WEP.

Con esta informacion podemos facilmente ubicar nuestra red y ver la tasa de transferencias de paquetes que recibimos, ubicar el rango de ip en que trabaja.

Con lo anterior tenemos lo basico, como dije antes si no logramos ver con kismet el AP del lugar, entonces estamos mal. Sin embargo el hecho de verlo no nos garantiza que tengamos la posibilidad de asociarnos.

Segun mi interpretacion el hecho de toparnos con el AP del lugar, solo nos garantiza que podemos recibir, pero no garantiza que tengamos capacidad para transmitir.

6.3. Algunas Opciones mas del interfaz Curses.

Para sacarle el jugo a kismet y poder empezar a ver detalles sobre una red en particular, lo primero es sacar la ventana de redes del modo Autofit, y ordenar las redes segun nuestros deseos. Presionando la tecla (S)ort podemos elegir la opcion de orden que queramos.

Una vez echo esto podemos jugar con otras opciones y detalles.

(P)ackets Types

Muestra el tipo de paquetes que pasa por la red. Esto es interesante ya que permite determinar si se tratan de *NOISE* o *BEACONS* o directamente trafico recibido de alguna *STA*

Network Deta(i)ls

Informacion sobre la red, MAC del AP, clientes conectados actualmente, Paquetes recibidos, (diferencia entre paquetes LLC y de datos).

(C)lients List

Listado de clientes encontrados dentro de la RED, esta opcion tira info interesante, como la calidad de la señal, la direccion MAC , la direccion IP, y el ID del fabricante.

(D)ump packets

Muestra los datos recibidos en format ASCII.

6.4. Filtrando por direccion MAC.

En muchos casos vemos demasiado trafico, pero no el trafico que queremos. Por ejemplo el otro dia estaba teniendo 10 paquetes por segundo, pero de los cuales 5 eran de una STA que estaba enfrente. Como mi objetivo es medir la cantidad de Beacons que estoy recibiendo, decidi filtrar esa direccion MAC asi no me aparece en las estadisticas generales.

Para esto Kismet tiene una opcion en su archivo de configuracion que permite agregar una lista de Direcciones MAC separadas por comas.

```
macfilter= ff:ff:00:12:12:12,
```

6.5. Usando la placa de Sonido

Antes que me olvide, como mencione antes si tienen la suerte de disponer de una STA con placa de sonido, pueden usar decirle a Kismet que reproduzca sonidos ante cada eventos (paquete transmitido, red nueva descubierta,etc).

Hay simplemente que instalar el paquete de su distro que contenga algun player de archivos *Wav* y luego descomentar las opciones de sonido en el archivo de configuracion.

Seria util hacer un pequeño parche para utilizar el parlante de la PC y ya que normalmente la maquina en la que uno tiene la placa wireless normalmente no posee placa de sonido.

O tambien como kismet posee en su archivo de configuracion la posibilidad de elegir la aplicacion para ejecutar los sonidos, podria colocarse una que simplemente emita diversos tipos de *Beeps*.

6.6. Analizando los logs.

Kismet mantiene una cantidad de logs en `/var/log/kismet` cada uno en diversos formatos, la opcion `logtypes` establece el formato de archivo en que vamos a realizar el log.

```
logtypes=dump, network, csv, xml, weak, cisco, gps
```

En este ejemplo estamos seleccionando todos los tipos de logs.

dump

paquete en formato crudo (Raw dump) este es muy util para despues pasar por un ethereal o tcpump

network

redes detectadas en texto plano

csv

redes detectadas en texto plano en formato CSV

weak

weak packets (en formato airsnot)

cisco

cisco equipment CDP broadcast

xml

En formato XML, tanto para paquetes de red como para paquetes Cisco

gps

Coordenadas de GPS en caso de que tengamos GPS

EL mas interesenta en mi opinion es el formato *dump* el cual posteriormente puede ser procesado por ethereal o tcpdump. `tethereal -i wlan0< /var/log/kismet/Kismet-Jan-20-2003-10.dump`

Con este comando basico podemos volver el archivo `.dump` a un archivo ASCII que con toda la informacion sobre los paquetes capturados.

Kismet Mini-mini-howto: Una guía para Mendoza-Wireless

```
Frame 1 (92 bytes on wire, 92 bytes captured)
  Arrival Time: Jan 19, 2003 21:40:40.181691000
  Time delta from previous packet: 0.000000000 seconds
  Time relative to first packet: 0.000000000 seconds
  Frame Number: 1
  Packet Length: 92 bytes
  Capture Length: 92 bytes
IEEE 802.11
  Type/Subtype: Beacon frame (8)
  Frame Control: 0x0080
    Version: 0
    Type: Management frame (0)
    Subtype: 8
    Flags: 0x0
      DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS:
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = WEP flag: WEP is disabled
        0... .... = Order flag: Not strictly ordered
  Duration: 0
  Destination address: ff:ff:ff:ff:ff:ff (Broadcast)
  Source address: 00:e0:03:04:b0:a2 (NokiaWir_04:b0:a2)
  BSS Id: 00:e0:03:04:b0:a2 (NokiaWir_04:b0:a2)
  Fragment number: 0
  Sequence number: 4038
IEEE 802.11 wireless LAN management frame
  Fixed parameters (12 bytes)
    Timestamp: 0x0000002A5085027E
    Beacon Interval: 0.102400 [Seconds]
    Capability Information: 0x0001
      .... .1 = ESS capabilities: Transmitter is an AP
      .... .0. = IBSS status: Transmitter belongs to a BSS
      .... 00.. = CFP participation capabilities: No point coordinator at AP (0x0
      .... ...0 .... = Privacy: AP/STA cannot support WEP
      .... .0. .... = Short Preamble: Short preamble not allowed
      .... .0.. .... = PBCC: PBCC modulation not allowed
      .... 0... .... = Channel Agility: Channel agility not in use
      .... .0.. .... = Short Slot Time: Short slot time not in use
      ..0. .... .... = DSSS-OFDM: DSSS-OFDM modulation not allowed
  Tagged parameters (56 bytes)
    Tag Number: 0 (SSID parameter set)
    Tag length: 6
    Tag interpretation: lugmen
    Tag Number: 1 (Supported Rates)
    Tag length: 4
    Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
    Tag Number: 3 (DS Parameter set)
    Tag length: 1
    Tag interpretation: Current Channel: 6
    Tag Number: 5 ((TIM) Traffic Indication Map)
    Tag length: 4
    Tag interpretation: DTIM count 0, DTIM period 5, Bitmap control 0x0, (Bitmap suppressed)
    Tag Number: 133 (Reserved tag number)
    Tag length: 31
    Tag interpretation: Not interpreted
```

Lo anterior fue solo un extracto de la información que tiene un beacon del SSID "Lugmen"

7. Comentario Final

Bueno como ven no es ninguna ciencia configurar y hacer uso de kismet. De aquí en más corre por su cuenta el uso que harán con la información que kismet les brinda.

Como siempre los parches a este documento son bienvenidos y espero que les haya servido de algo.