
ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

# DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

## CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

## TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

## TEMA: “IMPLEMENTACIÓN DE UN PROTOTIPO DE SISTEMA DE ANÁLISIS DE TRÁFICO DE REDES 802.11 UTILIZANDO LA MINICOMPUTADORA RASPBERRY PI”.

**AUTOR: PÁEZ ROJAS, TAMARA FABIANA**

**DIRECTOR: ING. ROMERO, CARLOS**

**CODIRECTOR: ING. SÁENZ, FABIÁN**

**SANGOLQUÍ**

**2015**

# UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE

## CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

## CERTIFICADO

Ing. Carlos Romero (DIRECTOR)
Ing. Fabián Sáenz (CODIRECTOR)

## CERTIFICAN

Que el trabajo titulado: "*Implementación de un prototipo de sistema de análisis de tráfico de redes 802.11 utilizando la minicomputadora Raspberry Pi*", realizado por la Señorita, Tamara Fabiana Páez Rojas, ha sido dirigida y revisada periódicamente y cumple con las normas estatutarias establecidas por la Universidad de las Fuerzas Armandas –ESPE en su reglamento.

Debido a que no existen modificaciones adicionales que se hayan recomendado a la alumna, se recomiendan su publicación.

Sangolquí, Junio del 2015.

Ing. Carlos Romero
DIRECTOR

Ing. Fabián Sáenz
CODIRECTOR

# UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE

## CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

## DECLARACIÓN DE RESPONSABILIDAD

Tamara Fabiana Páez Rojas

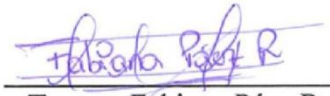
**DECLARO QUE:**

El proyecto de grado denominado "I*mplementación de un prototipo de sistema de análisis de tráfico de redes 802.11 utilizando la minicomputadora Raspberry Pi*", ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, considerándolos en citas a pie de página y como fuentes en el registro bibliográfico.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Junio del 2015.



Tamara Fabiana Páez Rojas

# UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE

## CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES Y COMUNICACIÓN DE DATOS

## AUTORIZACIÓN

Yo, Tamara Fabiana Páez Rojas

Autorizo a la Universidad de las Fuerzas Armadas-ESPE, la publicación en la biblioteca virtual de la institución del proyecto de grado titulado: "*Implementación de un prototipo de sistema de análisis de tráfico de redes 802.11 utilizando la minicomputadora Raspberry Pi*", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, Junio del 2015.

Tamara Fabiana Páez Rojas

# DEDICATORIA

*Dedico la realización de este proyecto de tesis a mis Padres por todo su apoyo, dedicación y consejos en este largo caminar; gracias por la entrega y la confianza que me supieron brindar, por demostrarme que con perseverancia y dedicación se logra aún el reto más difícil, por todo su amor y cariño, sin duda la mejor herencia que he recibido, porque todo lo que soy se los debo a ustedes.*

*A mis hermanos por los consejos y enseñanzas, han hecho que este sueño sea también suyo.*

*A ti Santiago que durante días me brindaste todo tu amor, tu fuerza, tu apoyo; tú por ser mi impulso y mi motor, gracias por estar siempre pendiente de mí, por darme ánimos para culminar esta etapa tan anhelada de mi vida.*

*A todos mis amigos que han visto crecer este sueño día a día, los quiero mucho desde el fondo de mi alma.*

*A todas las personas quienes han formado parte importante en esta etapa de mi vida.*

*Tamara Fabiana Páez Rojas*

# AGRADECIMIENTO

*Debo agradecer de manera especial a mis padres y hermanos, por su amor, su enseñanza, paciencia y el apoyo incondicional que me han brindado, los amo con todo mi corazón.*

*Y sobre todo a Dios por las personas que ha puesto en mi camino, han hecho de este tiempo la mejor etapa de mi vida; a mis amigos, por su lealtad, por su apoyo, gracias por esa amistad que perdurará por siempre. Por hacer agradable cada momento, sin duda una gran familia que Dios me puso, los quiero demasiado y siempre les voy a recordar.*

*A mis queridos ingenieros Carlos Romero y Fabián Sáenz por todo su valioso tiempo, apoyo, consejos y por los conocimientos impartidos.*

*Dios les bendiga y les múltiple mucho más a todos.*

*Tamara Fabiana Páez Rojas*

# ÍNDICE GENERAL

# ÍNDICE DE FIGURA

# ÍNDICE DE TABLA

# ÍNDICE DE FOTO

# RESUMEN

El presente proyecto tiene como fin la implementación de un sistema de análisis de tráfico de redes 802.11 mediante la utilización de la tarjeta Raspberry Pi. La necesidad e importancia de tener un analizador de tráfico que mediante un dispositivo portable y de bajo consumo de energía facilite la conexión, adquisición y procesamiento de los datos obtenidos; permitiendo junto al software Kismet bajo la plataforma Raspbian diseñar e implementar un analizador de tráfico de redes inalámbricas, capaz de proporcionar capturas en tiempo real de la información que atraviesa dentro del espectro de red del estándar 802.11en el campus de la Universidad de las Fuerzas Armadas - ESPE, además de identificar los *Access Point* utilizando la técnica de *georeferenciación* para determinar los diferentes parámetros de desempeño de la red; con lo cual se podrá validar y analizar el desempeño del prototipo mediante el análisis de *roaming* del cliente. Gracias a la información que se extrae de las capturas realizadas en los distintos escenarios, se dará a conocer cómo se encuentra constituida la infraestructura del entorno de red del campus universitario, estándares utilizados, velocidades requeridas por los AP, tipos de seguridad utilizados, eficiencia de las tramas de gestión, entre otros aspectos importantes para la construcción de una adecuada y eficiente infraestructura de red.

**PALABRAS CLAVES:**

- **ANALIZADOR DE TRÁFICO**
- **RASPBERRY PI**
- **KISMET**
- **GPS**
- **TRIANGULACIÓN**

# ABSTRACT

This project aims to implement a system of traffic analysis 802.11, using the Raspberry Pi card. The need and importance of having a traffic analyzer device using a portable and low power consumption facilitates connection, acquisition and processing of data; allowing by the Kismet software under the Raspbian platform design and implement a traffic analyzer wireless networks capable of providing real-time capture of information within the spectrum spanning network of 802.11 on the campus of the University of the Armed Forces - ESPE, and identify the Access Point using the technique of georeference determining different parameters determining network performance; whereby you can validate and analyze the performance of the prototype by analyzing customer roaming. Thanks to the information that is extracted from catches in the different scenarios, it will be revealed how is constituted the infrastructure of the network environment of the university campus, standards used, speeds required by the AP, security types used, authentication, efficiency of management frames, among other important aspects for the construction of infrastructure network adequate and efficient.

**KEYWORDS:**

- **SNIFFER**
- **RASPBERRY PI**
- **KISMET**
- **GPS**
- **TRIANGULATION**

# CAPÍTULO I

## 1.1 INTRODUCCIÓN

En los últimos años se ha generado un gran desarrollo de las comunicaciones, si recordamos las primeras comunicaciones eran mediante medios físicos, cables que representaban altos costos de instalación y pocos usuarios. Por tal motivo es de vital importancia perfeccionar los medios de transmisión de manera rápida con el fin de aumentar la velocidad de transmisión, capacidad, abarcar a más usuarios y obtener gran envío de información hasta como en la actualidad lo tenemos.

Actualmente el acceso y uso constante de internet se ha convertido en parte esencial de nuestras vidas, ya que todas las personas con simplemente tener un dispositivo de comunicación como un celular, *tablet* o computador tienen acceso a la red para mejorar sus actividades personales y empresariales de manera fácil y eficiente.

Debido a la gran cantidad de usuarios que continuamente acceden a las redes provocan que esta se sature por el excesivo tráfico o cantidad de información que circula en la red, por las múltiples actividades que se realizan como descarga de información, videos, música, videoconferencias, navegación web, envío de mails, etc, trayendo como consecuencia que la red presente lentitud, virus, pérdida de privacidad o robo de información.

Por esta razón el mercado tecnológico busca constantemente brindar soluciones de seguridad completas, eficaces y más flexibles, con esto se presenta la necesidad de utilizar herramientas como analizadores de tráfico, que permitan informar al administrador o cliente de que tipo es la información que circula con mayor

frecuencia por la red y de donde proviene el tráfico, con el fin de conseguir un adecuado entorno de red WLAN.

A lo largo de los años los analizadores de tráfico de red se han basado en dispositivos de hardware costosos, sin embargo los nuevos progresos tecnológicos han permitido crear analizadores de redes basados en software empleando nuevos dispositivos como es el caso de los ordenadores de placa reducida (SBC), particularmente los ordenadores Raspberry Pi, haciendo que el desarrollo de analizadores de tráfico de red sea más accesible para los administradores y convirtiéndose en una herramienta que permite identificar y solucionar con eficacia y menor inversión los problemas de la red [1].

El enfoque de este proyecto nos permitirá comprender y descifrar muchos aspectos en lo que se refiere al análisis de tráfico dentro de las redes inalámbricas, que gracias a la tarjeta Raspberry Pi nos va a facilitar la conexión, adquisición y procesamiento de los datos obtenidos, ya que al ser un dispositivo móvil, recurso vital para la movilidad entre *Access Point* (AP), autonomía, con bajo consumo de potencia y al permitir conectar periféricos como módulos de red, GPS, utilizado actualmente en un sin número de aplicaciones de todo tipo, como interfaces Hardware, control de otros dispositivos, encendido y apagado de luces, proyectos de domótica, etc.; permitirá capturar dentro del espectro de red el estándar 802.11, en la Universidad de las Fuerzas Armadas – ESPE.

## 1.2 OBJETIVOS

### 1.2.1 Objetivo General

Desarrollar un prototipo de un sistema de análisis de tráfico de red 802.11 mediante un dispositivo portable como una tarjeta *Raspberry Pi.*

### 1.2.2 Objetivos Específicos

Los objetivos específicos del presente trabajo son:

- Determinar la funcionalidad, características, configuraciones iniciales, para el correcto desempeño y uso de la minicomputadora *Raspberry Pi*, con su módulo GPS.
- Aprender a utilizar herramientas de software para el manejo de la tarjeta *Raspberry Pi* aplicado a Linux.
- Implementación del prototipo de análisis de tráfico de redes 802.11.
- Realizar el análisis de la información y paquetes capturados de la red, mediante el monitoreo y administración para determinar sus parámetros de red y eficiencia.
- Validar el prototipo a través de un análisis real, como el *Roaming* de un cliente en la red *Wireless*.

## 1.3 JUSTIFICACIÓN E IMPORTANCIA

El gran avance tecnológico que se muestra en estos últimos años ha repercutido directa e indirectamente en la vida de las personas, actualmente ni siquiera podemos imaginar las cosas que se pueden realizar con pequeñas tarjetas o integrados. Por esta razón diariamente el mundo de la electrónica, la programación y las telecomunicaciones se actualizan dejando obsoletos a otros dispositivos, con el fin de facilitar y hacer más sencilla la vida de las personas.

En la actualidad, existen varios sistemas que permiten capturar el tráfico de red, estos sistemas pueden estar basados en hardware o software, los cuales son conocidos como Analizadores de Tráfico de Red o *sniffer* cuya función se basa en obtener toda la información que viajan por la red, analizarlos por el administrador con todos los parámetros de red y así determinar la eficiencia del diseño de la red.

Por tal motivo, como proyecto de materia de graduación, se tiene como objetivo principal desarrollar un prototipo de un sistema de análisis de tráfico de red mediante la utilización de un dispositivo portable como, la tarjeta *Raspberry Pi*. La aplicación debe capturar y analizar el tráfico de red dentro del campus politécnico, realizando capturas en tiempo real y análisis de los principales parámetros de red, con esta información podemos indicar al administrador problemas que existan en la red, tramas 802.11 que se obtienen, tipo de encriptación y demás parámetros para administrar la red.

Con la utilización del módulo portable, tarjeta *Raspberry Pi* y trabajando bajo la plataforma LINUX, permiten conjuntamente con el software *Kismet* tener un sistema de analizador de tráfico de red 802.11 para el monitoreo y administración de la red así como para determinar el análisis de *Roaming* del cliente dentro de la red de la Universidad de las Fuerzas Armadas – ESPE.

Una de las mayores ventajas de emplear el ordenador de placa reducida *Raspberry Pi* es el bajo consumo de potencia, la portabilidad del dispositivo debido a su tamaño reducido frente a los ordenadores dedicados a este fin, y los costos en cuanto a software para desarrollo, debido a que esta tarjeta funciona en conjunto con el sistema operativo LINUX, uno de los sistemas operativos de software libre y código abierto, proponiendo facilidad de colocar la tarjeta de red en modo monitor ya que en soluciones con Windows abarcaría mayores costos por hardware y software; permitiendo de esta manera un ahorro significativo frente a los analizadores de tráfico de red existentes actualmente en el mercado [2], [3].

## 1.4 ALCANCE

Durante este proyecto se realizarán: i) un estudio de las funcionalidades, características de la tarjeta *Raspberry Pi*, periféricos USB a ser usados, modos de

operación de tarjetas de red inalámbricas; ii) estudio de la funcionalidad y características del módulo GPS soportado en Linux, funcionamiento, modo de operación a implementar para identificar georeferencialmente los AP determinando diferentes parámetros de desempeño de la red; iii) posteriormente se procederá a la descripción e implementación tanto en hardware y software, utilizando la tarjeta. Para finalmente poder validar y analizar el desempeño del prototipo mediante el análisis de *Roaming* del cliente en la red *Wireless* de la Universidad de las Fuerzas Armadas - ESPE.

# CAPÍTULO II

# MARCO TEORICO

En este capítulo se describirá el marco teórico iniciando con la definición del concepto de analizador de tráfico de red, su funcionamiento, principales *sniffers* utilizados en el mercado; especificaciones técnicas, configuraciones iniciales, funcionalidades y aspectos generales de la minicomputadora *Raspberry Pi*; así también características y especificaciones técnicas de los dispositivos USB inalámbricos y GPS utilizados para el diseño del prototipo; mecanismo utilizado para determinar mediante ubicación GPS la georeferenciación de los AP.

## 2.1 ANALIZADOR DE TRÁFICO DE RED

### 2.1.1 Definición

Su definición en informática, es un programa especializado de monitoreo y análisis, que captura tramas o paquetes de una red de datos. Es un software informático que puede interceptar y registrar tráfico de paquetes pasando sobre una red de datos. Mientras el flujo de datos va y viene en la red, el *sniffer* captura cada unidad de datos del protocolo, puede decodificar y analizar su contenido, de acuerdo a la especificación del programa [4].

Su uso varía desde la detección de un cuello de botella en una red hasta el análisis de fallas en las redes, aunque también es habitual su uso para fines maliciosos, como robo de contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de chat, obtener datos personales, entre otros.

La cantidad de tramas que puede obtener un Analizador de tráfico de red depende de la topología de red, del diseño del analizador, así como el medio de transmisión [4].

### 2.1.2 Funcionamiento

Para explicar el funcionamiento de un analizador de tráfico de red es necesario tener presente varios conceptos. Una red de datos, está formada por varias computadoras conectadas entre sí por un medio cableado o inalámbrico, que están conectados a otros dispositivos como conmutadores y estos a su vez a otros dispositivos llamados enrutadores, el cual se encarga de escoger rutas y dirigir los paquetes de información hacia la computadora destino como podemos ver en la Figura 1 [4].

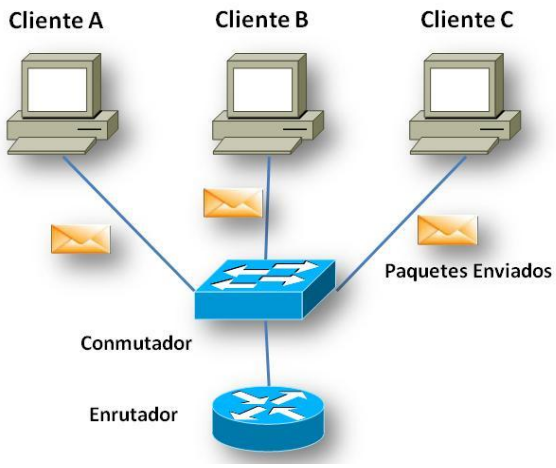



**Figura 1.** Conexión de una red LAN

Es muy común en las redes LAN, con una topología tipo bus que un analizador de tráfico de red pueda operar en dicha red, ya que todas las computadoras están conectadas a un mismo medio compartido, donde todo el tráfico es transmitido y recibido por todas las máquinas que pertenecen a esa red local, es decir comparten un medio común.

Otro medio donde los analizadores de tráfico de red pueden desenvolverse tranquilamente es en la máquina de la víctima, pero para este caso es necesario tener acceso a la maquina víctima, donde se instala el programa y el fin de hacer esto es

encontrar información de otros usuarios y tener acceso a otros dispositivos, que normalmente se accede desde la máquina víctima [4].

Los analizadores de tráfico de red funciona por una simple razón, existen protocolos que son de acceso remoto y las máquinas transmiten las claves de acceso remoto en forma de texto plano por esta razón es que se captura la información que se transmite por la red, ya que nos da la información correcta para tener acceso a alguna maquina  determinada.

Como ejemplo de cómo procede la captura en la Figura 2, tenemos una máquina que transmite un dato, lo hace a través del cable compartido, en el cual están conectadas todas las máquinas, las máquinas que están conectadas tienen la misma posibilidad de ver los datos que en ese momento se están transmitiendo, pero eso no sucede ya que cada tarjeta de red que tienen las máquina conectadas, solo reciben o capturan los paquetes de datos que van dirigidos hacia ellos, y todos los otros datos que se transmiten son ignorados, por ese motivo cuando se va a comenzar a capturar los datos se activa la tarjeta en modo promiscuo [4].

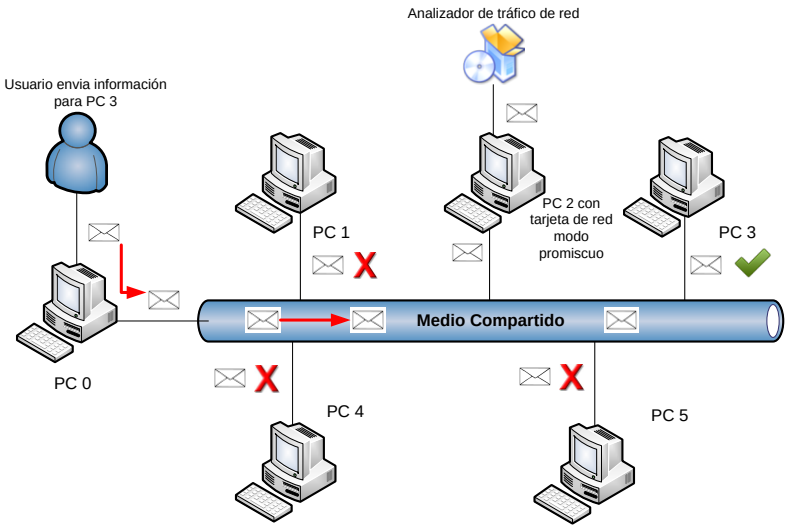



**Figura 2.** Funcionamiento general de un analizador de redes

Así es como un analizador de tráfico de red trabaja accediendo a los datos que pasan por una tarjeta de red, sea esta inalámbrica o Ethernet. Una vez que se accede a los datos, lo que realiza el analizador de tráfico de red es filtrar todos los paquetes, los examina y mira las peticiones de los puertos según los filtrados del usuario como TCP, UDP, POP3, etc [4].

### 2.1.3 Analizadores de tráfico existentes en el mercado

Por su popularidad e importancia tenemos los siguientes tipos de Analizadores de tráfico de red:

**Nessus** es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un *daemon, nessusd,* que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos [5].

**Snort** es una sistema de detección de intrusiones de red de poco peso (para el sistema), capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP. Puede realizar análisis de protocolos, búsqueda/identificación de contenido y puede ser utilizado para detectar una gran variedad de ataques y pruebas, como por ejemplo: escaneos indetectables de puertos, ataques a CGI, pruebas de SMB, intentos de reconocimientos de sistemas operativos, etc, [5].

**Netcat** una utilidad simple para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP. Está diseñada para ser una utilidad del tipo "*back-end*" confiable que pueda ser usada directamente o fácilmente manejada por otros programas y scripts [5].

**TCPDump / WinDump** Tcpdump es un conocido analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en

una interfaz de red (*network interface*) que concuerden con cierta expresión de búsqueda. Se utiliza esta herramienta para rastrear problemas en la red o para monitorear actividades de la misma [5].

**Wireshark** es un analizador de protocolo de red para Unix y Windows. Le permite examinar los datos de una red de un archivo de captura en disco. Tiene varias características de gran alcance, incluyendo el idioma de la pantalla del filtro y la capacidad de ver la secuencia reconstruida de una sesión TCP [6].

**Kismet** es un programa para Linux que permite detectar redes inalámbricas mediante la utilización de tarjetas *wireless* en los estándar 802.11a/b/g. Permite verificar que la red está bien configurada, además nos ayuda a detectar todos los AP que están a nuestro alrededor ejecutando WarDriving [6].

**KisMAC** hace mucho de lo que Kismet puede hacer, pero con una interfaz gráfica Mac OS X. Es un escáner pasivo que registra datos en disco en formato PCAP. No es compatible con el examen pasivo con AirportExtreme tarjetas (debido a las limitaciones en el controlador inalámbrico), pero soporta el modo pasivo con una variedad de tarjetas inalámbricas USB [7].

**Nmap** es un programa de código abierto que permite desarrollar rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos, además de descubrir servicios o servidores en una red informática [6].

## 2.2 RASPBERRY PI

### 2.2.1 Definición

Raspberry Pi es una computadora de pequeñas dimensiones, el cual puede conectarse fácilmente a una televisión vía HDMI o RCA. Además, se puede usarla, lógicamente, con un teclado y un ratón. Tiene conexión a internet y unos pines GPIO

(*General Purpose Input/Output*), para que podamos interactuar con nuestra placa con sensores, botones, o lo que se requiera. En el mercado existen varios modelos de la Raspberry Pi como: el modelo A, modelo B, B+ y recientemente la tarjeta Pi 2 modelo B.

Raspberry Pi es un ordenador de placa reducida (SBC) de bajo costo desarrollado por la Fundación Raspberry Pi, con el objetivo de estimular la enseñanza de ciencias de la computación en las escuelas. El diseño no incluye un disco duro o una unidad de estado sólido, ya que usa una tarjeta SD para el almacenamiento permanente; tampoco incluye fuente de alimentación o carcasa [8].

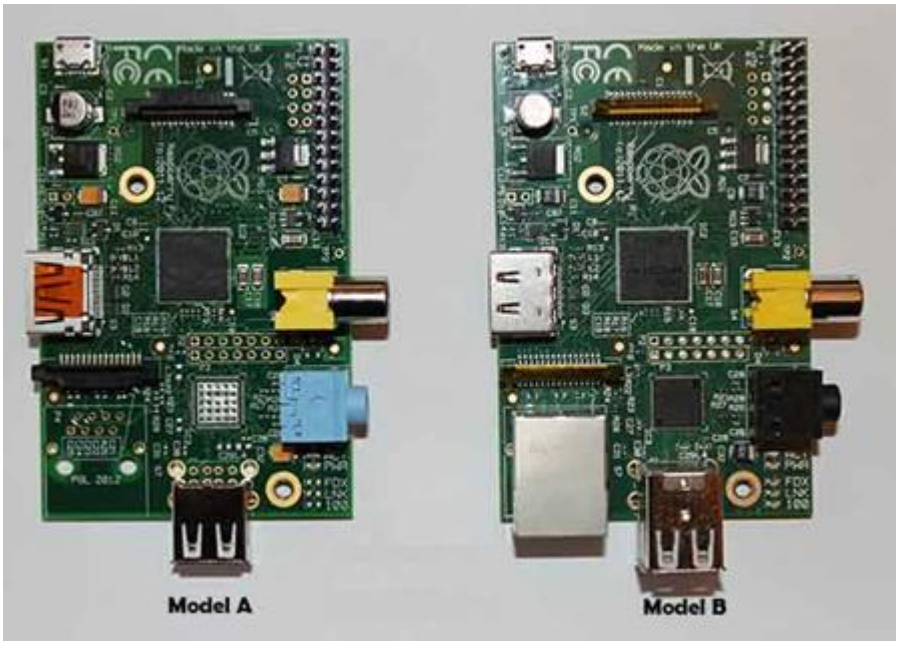



**Figura 3.** Raspberry Pi Model A y Model B

Con unas dimensiones de placa de 8.5 por 5.3 cm, el diseño de la Raspberry Pi modelo B, incluye un *System-on-a-chip* Broadcom BCM2835, que contiene un procesador central (CPU) ARM1176JZF-S a 700 MHz, un procesador gráfico (GPU) *VideoCore IV*, y 512 MB de memoria RAM aunque originalmente al ser lanzado eran 256 MB (Raspberry Pi modelo A). En cuanto a vídeo se refiere, también cuenta

con una salida de vídeo compuesto y una salida de audio a través de un minijack. Posee una conexión Ethernet 10/100 y, si bien es cierto que podría hacer falta una conexión *Wifi*, gracias a los dos puertos USB incluidos se puede suplir dicha carencia con un adaptador *Wifi* si se lo necesita [8], [9].

### 2.2.2 Especificaciones de Hardware

La Raspberry Pi dispone de diferentes componentes como [8], [10]:

- LED's indicadores: proveen retroalimentación visual de ciertos procesos.
- Salida de audio análogo. Contiene un conector de audio de 3.5 mm para poder manejar cargas de alta impedancia.
- Salida de video compuesto: Dispone de un conector RCA capaz de proveer señales de video compuesto NTSC o PAL, está es de más baja resolución que HDMI.
- Entrada de energía: Se dispone de un conector microUSB de alimentación de 5V. Consumo energético 500 mA y 2,5W en su modelo A y 700mA y 3,5W en el modelo B.
- Pines de propósito general: Estos pines permiten la conexión de dispositivos externos, para comunicación, energía, mediciones u otros.

**Tabla 1.**

Especificaciones Técnicas

| | RPI Model A | RPI Model A+ | RPI Model B | RPI Model B+ | RPI 2 Model B |
|---|---|---|---|---|---|
| SoC | Broadcom BCM2835 | Broadcom BCM2835 | Broadcom BCM2835 | Broadcom BCM2835 | Broadcom BCM2836 |
| CPU | ARM11 ARMv6 700 MHz. | ARM11 ARMv6 700 MHz. | ARM11 ARMv6 700 MHz. | ARM11 ARMv6 700 MHz. | ARM11 ARMv7 ARM Cortex-A7 4 núcleos @ 900 MHz. |
| GPU | Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0 | Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0 | Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0 | Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0 | Broadcom VideoCore IV 250 MHz. OpenGL ES 2.0 |

CONTINÚA

| RAM | 256 MB LPDDR SDRAM 400 MHz. | 256 MB LPDDR SDRAM 400 MHz. | 512 MB LPDDR SDRAM 400 MHz. | 512 MB LPDDR SDRAM 400 MHz. | 1 GB LPDDR2 SDRAM 450 MHz. |
|---|---|---|---|---|---|
| USB 2.0 | 1 | 1 | 2 | 4 | 4 |
| Salidas de vídeo | HDMI 1.4 @ 1920x1200 píxeles | HDMI 1.4 @ 1920x1200 píxeles | HDMI 1.4 @ 1920x1200 píxeles | HDMI 1.4 @ 1920x1200 píxeles | HDMI 1.4 @ 1920x1200 píxeles |
| Almacena-miento | SD/MMC | microSD | SD/MMC | microSD | microSD |
| Ethernet | No | No | Sí, 10/100 Mbps | Sí, 10/100 Mbps | Sí, 10/100 Mbps |
| Tamaño | 85,60x56,5 mm | 65x56,5 mm. | 85,60x56,5 mm | 85,60x56,5 mm | 85,60x56,5 mm |
| Peso | 45 g. | 23 g. | 45 g. | 45 g. | 45 g. |
| Precio | 25 dólares | 20 dólares | 35 dólares | 35 dólares | 35 dólares |

### 2.2.3 Sistemas Operativos

Entre los sistemas operativos que funcionan, se han portado, o están en proceso de ser portados a *Raspberry Pi*, se encuentran [8]:

- Android
- Arch Linux ARM
- Debian Whezzy Soft-Float, versión de Debian sin soporte para coma flotante por hardware
- Firefox OS
- Gentoo Linux
- Kali Linux
- Open webOS
- PiBang Linux , distribución Linux derivada de Raspbian con diferente escritorio y aplicaciones
- Pidora, versión Fedora Remix optimizada
- QtonPi, distribución linux con un framework de aplicaciones multiplataforma basado en Qt framework

- Raspbian, versión de Debian Wheezy para ARMv6 con soporte para coma flotante por hardware
- Slackware ARM, también conocida como ARMedslack
- OpenELEC (Media Center)
- Xbian

### 2.2.4 Configuraciones iniciales en la Raspberry Pi

#### 2.2.4.1 Configuración de *Raspbian* en memoria SD

La tarjeta *Raspberry Pi* se entrega sin sistema operativo; por esta razón se debe instalarlo sobre una tarjeta SD que se introduce en la ranura de la *Raspberry Pi* y hace la función de disco duro, en esta se almacenan todos los archivos de datos y se crea la imagen del sistema operativo que se instala. El software puede obtenerse de la sección de descargas de la página web de *Raspberry Pi*. Existen varias versiones que pueden utilizarse, de acuerdo a las funcionalidades ofrecidas y a los requerimientos que se necesitan para realizar el proyecto, se utiliza el sistema operativo *Raspbian Wheezy*. A continuación se detalla el procedimiento para realizar la configuración de *Raspbian Wheezy* en la memoria SD [10], [11]:

- Descargar una imagen del sistema operativo en la página web de descargas de *Raspberry Pi* (http://www.raspberrypi.org/downloads). Para nuestro estudio descargamos el sistema operativo *Raspbian* (archivo *.img*).

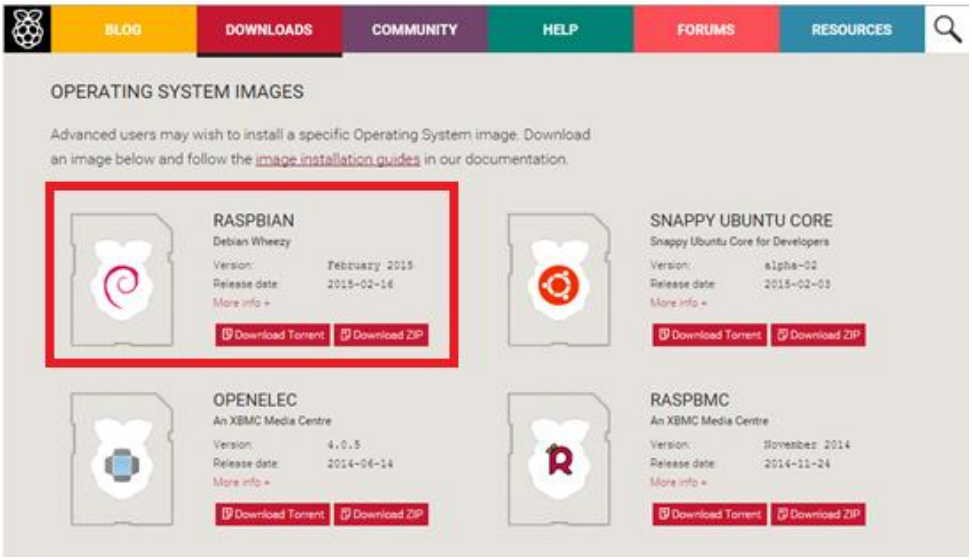



**Figura 4.** Web de descargas Raspberry Pi

- Continuando, se descarga el programa Win32DiskImager desde la fuente http://sourceforge.net/projects/win32diskimager/files/latest/download, programa que permite transferir los datos del archivo (.img) hacia la tarjeta SD. Se abre el archivo y se extrae el contenido. Finalmente se ejecuta Win32DiskImager.

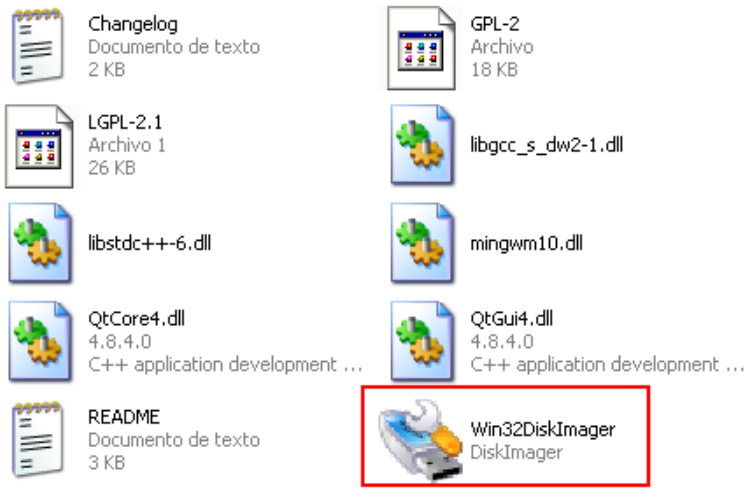



**Figura 5.** Icono de Win32DiskImager

- Se introduce la tarjeta SD en el lector de tarjetas del ordenador, luego seleccionar la imagen y se da clic en "*Write*".

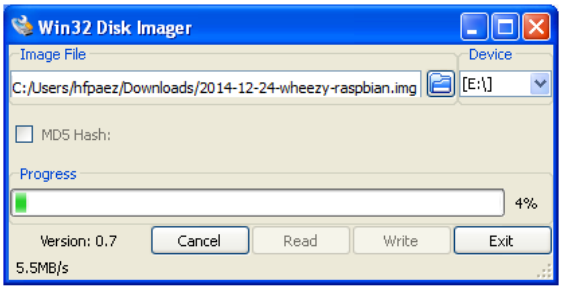



**Figura 6.** Captura de Win32DiskImager

- Finalizado el proceso, se inserta la memoria SD en la Raspberry Pi, se la conectar para proceder con el arranque inicial de la misma.

### 2.2.4.2 Configuración de arranque inicial

#### 2.2.4.2.1 Configuración de parámetros principales

Al encender por primera vez la *Raspberry Pi* se observará en la pantalla el arranque de varios procesos como la inicialización de la interfaz de red, reconocimiento de los periféricos USB, entre otros [10], [11].

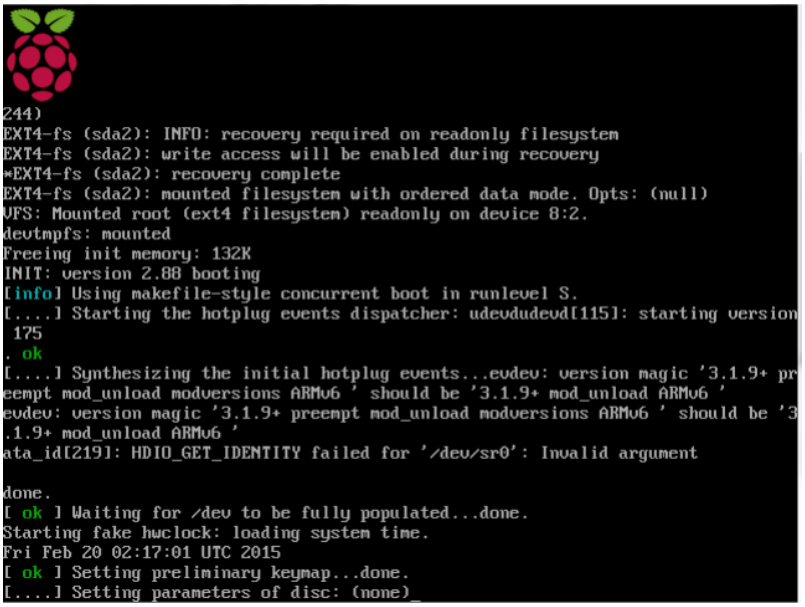



**Figura 7.** Proceso de arranque en Raspberry Pi

Al finalizar estos procesos, se despliega en pantalla el menú raspi-config para el establecimiento de la configuración de la *Raspberry Pi* [10].

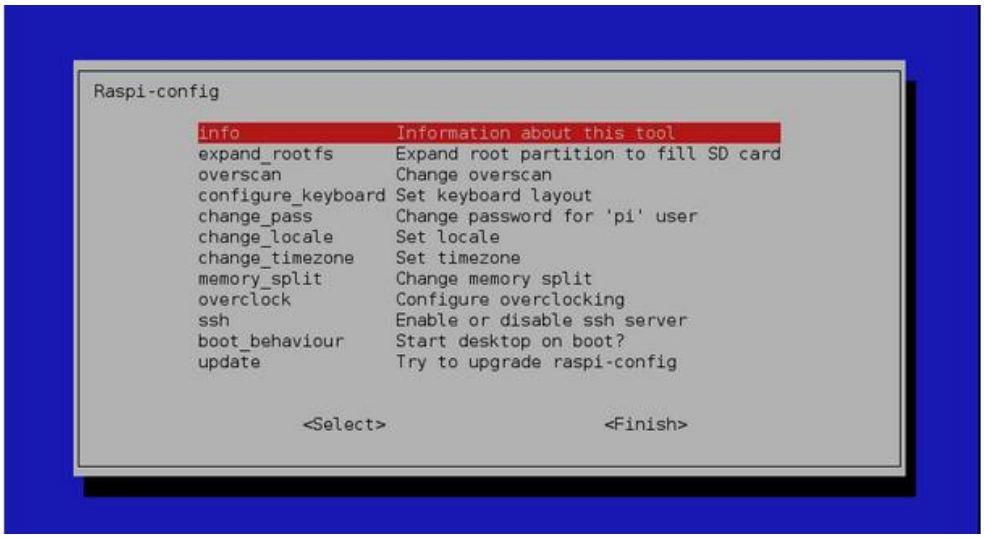



**Figura 8.** Menú Raspi-config

A continuación se describirá cada uno de estos parámetros [10], [11]:

- Info: brinda información acerca de la herramienta Raspi-config.
- Expand_rootfs: permite expandir la partición en la memoria SD hasta abarcar toda la capacidad de esta y así tener la posibilidad de usar toda la memoria disponible.
- Overscan: esta opción sirve para habilitar o deshabilitar el sobre escaneo, en caso de que la salida de video no despliegue la imagen entera en la pantalla que se está utilizando.
- Configure_keyboard: reconfigura el modelo del teclado.
- Change_pass: permite cambiar la contraseña para el usuario.
- Change_locale: reconfigura la codificación de caracteres.
- Change_timezone: reconfigura la zona horaria del sistema.

- Memory_split: configuración de la cantidad de RAM que se asigna a la unidad de procesamiento gráfico o GPU por sus siglas en inglés y el resto se asigna al procesador.
- Overclock: si se desea permite subir la frecuencia de operación del procesador para hacerlo más rápido, pero puede causar inestabilidad en el sistema y sobrecalentar la tarjeta.
- SSH: habilita o deshabilita el servicio SSH en la Raspberry Pi.
- Boot_behaviour: sirve para habilitar o deshabilitar la ejecución por defecto del entorno gráfico al encender la raspberry pi.
- Update: esta opción actualizará los repositorios (# apt-get update) e intentará actualizar la herramienta raspi-config (# apt-get install raspiconfig).

Al finalizar los cambios se selecciona finalizar y esto mostrará la línea de comando, entonces en la terminal se debe escribir el comando: *sudo reboot* para reiniciar la *Raspberry Pi* y completar la configuración.

## 2.3 DESCRIPCIÓN DEL SOFTWARE

### 2.3.1 *Debian*

*Debian* es un sistema operativo libre, viene con más de 43000 paquetes (software precompilado y empaquetado en un formato amigable para una instalación sencilla en su máquina), un gestor de paquetes (APT), y otras utilidades que hacen posible gestionar miles de paquetes en miles de ordenadores de manera tan fácil como instalar una sola aplicación [12].

#### 2.3.1.1 *Raspbian*

*Raspbian* es un sistema operativo libre basado en *Debian* optimizado para el hardware de *Raspberry Pi*. *Raspbian* ofrece más que un SO puro; viene con más de 35000 paquetes, programas precompilados con un formato que hace más fácil la instalación en su *Raspberry Pi* [13].

La versión de *Raspbian* que se instala inicialmente sobre la *Raspberry Pi* trae un pequeño grupo de programas, por lo que es necesario descargar e instalar los programas que se requieren de acuerdo a la utilización. Esta trae el LXDE (Lightweight X11 Desktop Environment) como el entorno gráfico de escritorio predeterminado, este es un entorno recortado desplegable de los sistemas X Windows que se ha utilizado en las interfaces gráficas de usuario en Unix y Linux, en general este permite manejar las vistas y da la sensación del manejo de ventanas y menús para controlarle [10].

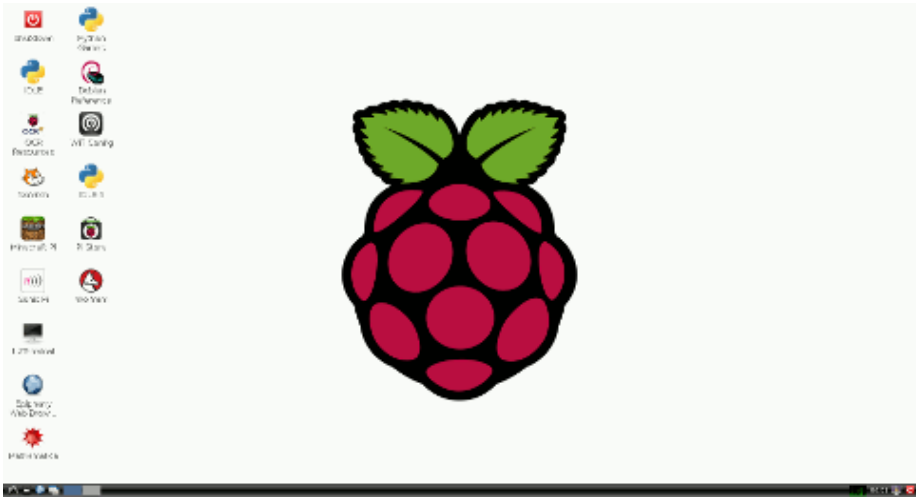


**Figura 9.** Interfaz gráfica de Raspbian

Entre las herramientas de manejo dentro de este entorno se pueden encontrar [10]:

- Buscador Web. *Midori* es el buscador web que por defecto se encuentra en *Raspbian*, la ventaja de este sobre otros más populares se debe al bajo uso de recursos provocando una disminución en procesamiento para ser aprovechado por otras tareas que se ejecutan en paralelo.
- Audio y video. Omxplayer es el reproductor de audio y video para Raspbian y está diseñado para trabajar con la Unidad de Procesamiento de Gráficos.
- Editores de texto. Leafpad es el editor de texto por defecto de Raspbian y se puede encontrar en el menú principal.
- Consola. Se utiliza para ejecutar comandos de línea de modo que se pueda realizar alguna tarea que no puede ejecutarse desde el modo gráfico.

### 2.3.2 Escaneando

Existen dos métodos de búsqueda de redes [14]:

- escaneado activo y
- escaneado pasivo

El escaneado activo envía paquetes de solicitud de rastreo, estos son usados por los clientes siempre que están buscando una red. Mientras que el pasivo escanea las ondas de cualquier paquete en un determinado canal y analiza dichos paquetes para determinar qué clientes se comunican con qué puntos de acceso [14].

Para nuestro caso se utilizará el modo monitor, equivalente al modo promiscuo en redes cableadas. Este pertenece al escaneado pasivo y su función es el análisis de todos los paquetes que circulan por el aire ya que estos tienen la información del emisor, el receptor, el canal, tamaño, entre otros parámetros.

### 2.3.3 Software de detección

Para la detección de paquetes se usará *Kismet*; ya que es un analizador de tráfico en Linux para redes inalámbricas en los estándares 802.11a/b/g/n.

#### 2.3.3.1 KISMET

*Kismet*, es un analizador de tráfico de red; un poderoso *sniffer* y sistema de detección de intrusiones para redes inalámbricas 802.11 en capa 2 utilizado en sistemas basados en Unix (Linux, FreeBSD, NetBSD, OpenBSD) y Windows por medio de Cygwin. Detecta bloques de IP automáticamente por medio de paquetes de UDP, ARP, y DHCP. También incluye la habilidad de graficar redes detectadas y rangos de red estimados sobre mapas o imágenes [5], [15].

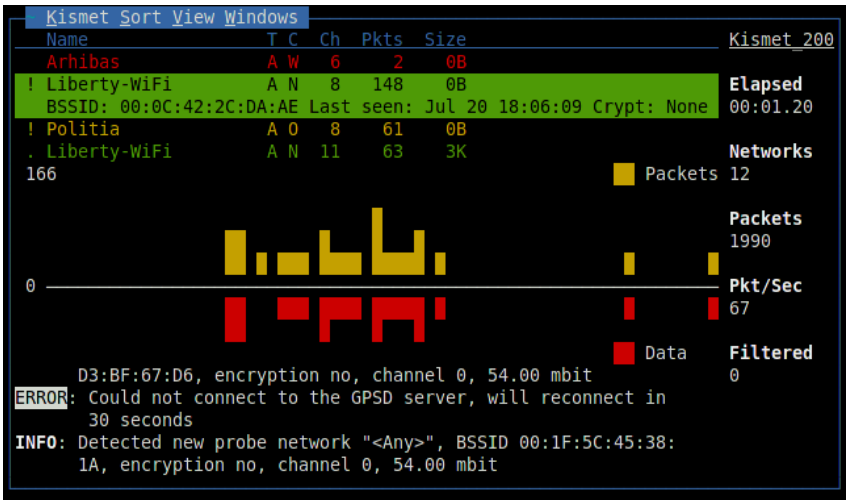



**Figura 10.** Interfaz Kismet

Esta herramienta funciona como [15]:

- Un escáner de redes *wireless*: Kismet permite ver redes inalámbricas sin importar si esta sea oculta, mostrándonos el nombre y los dispositivos asociados, así como sus direcciones MAC.
- Un *sniffer:* lo mejor de todo es su silencio, ya que no podremos ser detectados por otro cazador que quizás también este buscándonos.

Tiene varios usos, como [16]:

a) Verificar que nuestra red está bien configurada.
b) Detectar otras redes que pueden causar interferencias a la nuestra.
c) Sirve para *WarDriving*, es decir, detecta todos los AP que están a nuestro alrededor.
d) Muestra información sobre los clientes conectados a la red.
e) Indica el tipo de protección (WEP, WPA, WPA2).
f) Funciona con la tarjeta en modo monitor y guarda un archivo o *logs* con los paquetes capturados.

#### 2.3.3.1.1 Instalación de Kismet

*Kismet* está disponible para una fácil descarga e instalación desde la página web http://www.kismetwireless.net/code/, para nuestro estudio se descarga la versión disponible 2013-03-R1b (*Kismet*, 2013). A continuación se detalla una serie de pasos para la instalación de este paquete [17]:

- Se descarga el código fuente con el comando:

```
wget http://www.kismetwireless.net/code/kismet-2013-03-R1b.tar.gz
```

Antes de que el código sea compilado e instalado, hay algunas dependencias necesarias que se requieren descargar:

```
sudo apt-get install screen ncurses-dev libpcap-dev tcpdump libnl-dev wireshark
```

- Extraer el código fuente del archivo *.tar.gz*, con el comando:

```
tar xfvz kismet-2013-03-R1b.tar.gz
```

- Navegar hasta el directorio recién extraída mediante el comando:

```
cd kismet-2013-03-R1b
```

- Preparar el código para compilar y ejecutar la instalación, con el comando: **./configure**
- Se instala *Kismet* con el comando:

**make, sudo make suidinstall**

Finalizada la instalación, se requiere editar ciertas partes en el archivo de configuración para que funcione correctamente.

- Para editar el archivo de configuración *Kismet* se introduce el comando:

**sudo nano /usr/local/etc/kismet.conf**

- Se navega por el documento y se verifica la línea:

**#ncsource=wlan0**

Donde se elimina el comentario de esta línea (quitar el #), y se cambia "wlan0" de acuerdo al identificador de dispositivo descubierto con el comando ifconfig, como se muestra en el Figura 11.

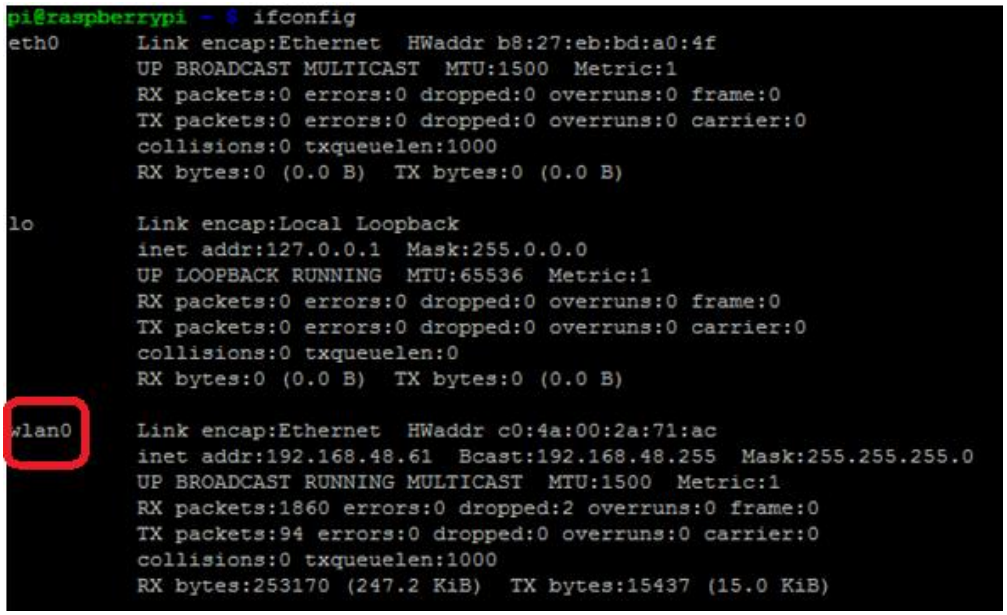



**Figura 11.** Dispositivo de red inalámbrico Wlan0

#### 2.3.3.1.2 Explicación de la interfaz de usuario

La interfaz principal de *Kismet* se compone de tres secciones. La ventana principal en la parte superior izquierda conocida como *Network List Panel*, en la cual aparecen las diversas redes que se van localizando. La ventana de información situada a la derecha es donde se puede ver el conteo del tiempo transcurrido, las redes detectadas, los paquetes recibidos, la velocidad de captura y los paquetes filtrados. Y la ventana de estado ubicada en la parte inferior, es donde se remarcan los últimos eventos, como redes descubiertas, IP's, direcciones MAC, etc, [16].

##### 2.3.3.1.2.1 Ventana Principal

La ventana central, está dividida en varias columnas, las cuales nos detallan información de las diversas redes según se vayan capturando. La ventana principal contiene varios parámetros que se detallan a continuación [16], [18]:

- Name: Por defecto el SSID o nombre de la red detectada.
    - Al lado de *Name* se encuentra 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 una actividad detectada en los últimos 3 segundos.
        - "." Indica una actividad detectada en los últimos 6 segundos.
        - "" No hay actividad.
    - Los colores indican la encriptación:
        - Verde, sin encriptación.
        - Amarillo, con encriptación (WEP, WPA, etc).
        - Rojo, usa su configuración por defecto.

- Azul, redes que ocultan su SSID.

*Kismet* puede detectar el nombre o SSID de una red *wireless* que este oculta, siempre que haya clientes autentificados y asociados a la misma, en este caso el color del SSID o el nombre de la red será visible en color azul [16].

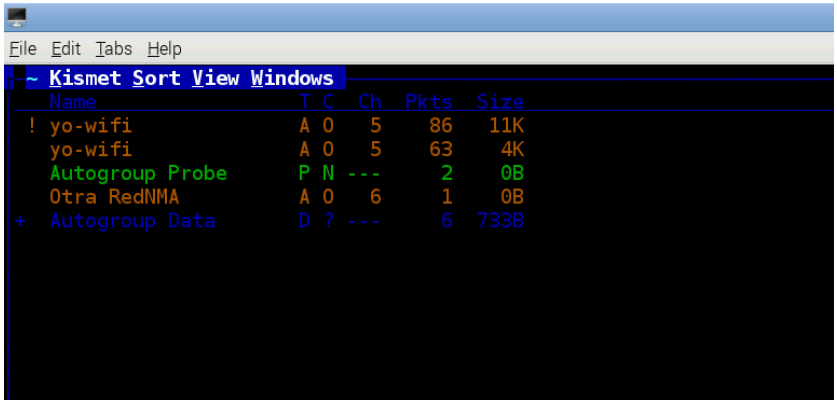



**Figura 12.** Redes ordenadas por SSID

En este caso la red llamada "*Autogroup Data*" son dudas o peticiones no resueltas por el servidor de *Kismet*, este crea un grupo automático donde deja esas peticiones perdidas.

- **T (Tipo)**: indica el tipo o modo de red del dispositivo detectado [18].
  - "A (*Acces Point*)", es un punto de acceso.
  - "D (*Data Network*)", los paquetes de datos se han visto, pero *Kismet* no ha capturado ningún *beacon* o tramas de gestión y por lo tanto aún no pueden decir qué tipo de red es.
  - "H (*Ad-hoc*)" si esta en modo Ad-Hoc.
  - "G (*Group*)" si es un grupo de redes *wireless*.
  - "P (*Probe Request*)", dispositivo que envía "*Probe Request*" (Solicitud de Rastreo) y no recibe respuesta (*probe response*) por lo tanto no está asociado a ningún AP).

- "T (*Turbocell*)" router Turbocell, Karlnet y Lucent

- **C**: indica si existe encriptación [18].
  - "W" encriptación (WEP) en uso.
  - "N" sin cifrado.
  - "O" la red se cifra con algo que no sea WEP (por ejemplo, WPA).
- **Ch (Channel)**: canal en el que opera la red.
  - Si es un grupo de redes "G" aparece un guión "-".
- **Pkts (Paquetes)**: número de paquetes capturados.
- **Size:** indica el tamaño de los paquetes capturados de cada red.

**2.3.3.1.2.2 Ventana de Estado**

Situada en la parte inferior de la pantalla de *Kismet*, muestra información sobre las redes y clientes que va encontrando y otras alertas, así como del estado de la batería. Entre los mensajes al usuario que se visualizan se pueden encontrar [16], [18]:

- Actualizaciones: *Kismet* publicará un mensaje al panel de estado cuando encuentra una nueva red, y proporcionar información adicional acerca de las redes cuando esté disponible.
- Problemas: *Kismet* le alertará de información sobre posibles problemas con la conexión de *Kismet* a otros servicios; por ejemplo, si *Kismet* no puede conectarse a *gpsd*.
- Alertas: Estos son principalmente útil cuando se utiliza *Kismet* como un sistema de detección de intrusiones (IDS); proporciona integración con sistemas de terceros (es decir, de Snort).
- Medidor de batería: *Kismet* indicará si está conectado a la alimentación externa (AC), y mostrará el porcentaje de vida útil restante de la batería.

#### 2.3.3.1.2.3 Ventana de Información

Es la que está en el lado derecho y muestra [16], [18]:

- El número total de redes encontradas (*Networks*)
- El número total de paquetes capturados (*Packets*)
- En número de paquetes capturados por segundo (Pkts/s)
- El tiempo que *Kismet* lleva ejecutándose (*Elapsed*)
- Números de tramas filtradas con filtros configurados en *Kismet* (*Filtered*)

#### 2.3.3.1.3 Archivos de Kismet

*Kismet* graba los datos automáticamente mientras se está ejecutando; los guarda en el archivo ***/var/log/kismet***. Por defecto, genera los archivos [16], [18]:

- .alert: Archivo de texto de registro para las alertas.
- .gpsxml: Registro GPS por paquete XML.
- .nettxt: Archivo de texto con los datos de las redes detectadas.
- .netxml: Archivo de texto con los datos de las redes detectadas en formato xml.
- .pcapdump: Captura de archivos pcap del tráfico observado.

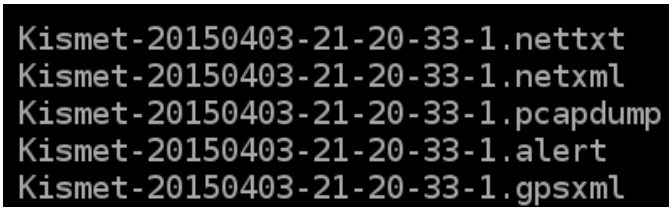



**Figura 13.** Lista de los archivos generados por Kismet

### 2.3.3.2 GPSD

Se hace uso también de GPSD para manejar las coordenadas GPS, esta aplicación es un demonio que recibe datos de un receptor GPS y proporciona esa

información a múltiples aplicaciones a la vez, ya sea *Kismet*, o cualquier navegador GPS. Utiliza una unión con el puerto de transporte 2947 [17].

A continuación se indica los pasos de instalación de GPSD,

**sudo apt-get install gpsd gpsd-clients**

Asegúrese de que el adaptador *wifi* y *GPS* están conectados, a continuación, introduzca el siguiente comando:

**lsusb**

Esto mostrará una lista de los dispositivos USB conectados al sistema. Asegúrese de que el dispositivo *GPS* está en la lista.

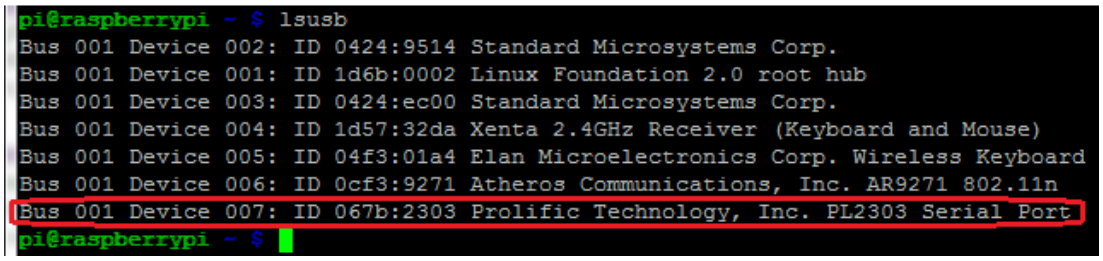



**Figura 14.** Dispositivo USB GPS conectado

A continuación, ejecute el comando siguiente para descubrir donde está conectado el dispositivo *GPS*. En algunas partes de la información "ttyUSB0" devueltas o similares deben imprimirse.

**dmesg | grep tty**

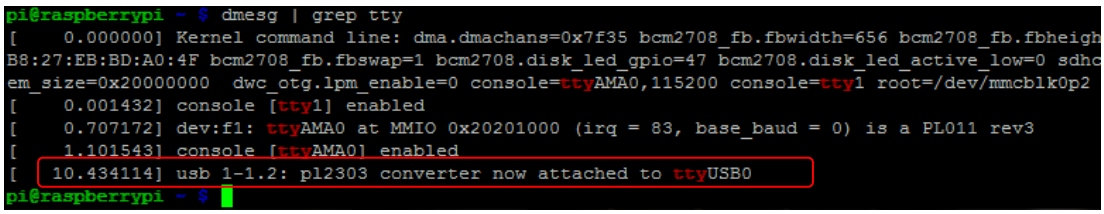



**Figura 15.** Ubicación del GPS conectado

En la figura 15, se muestra la ubicación del dispositivo GPS y debe tenerse en cuenta para uso futuro. Para configurar el software GPSD, se ejecuta el siguiente comando:

**sudo dpkg-reconfigure gpsd**

Navegue a través de las preguntas y responda de acuerdo a la ubicación del dispositivo GPS "/dev/ttyUSB0".

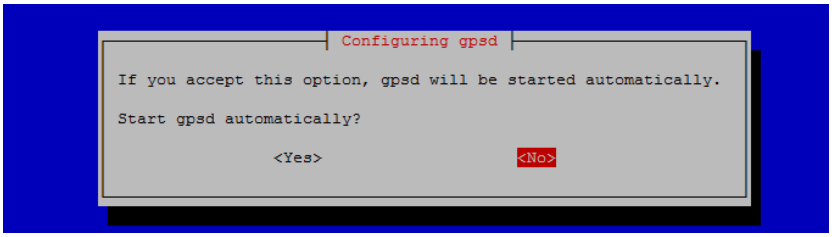



**Figura 16.** Ventana de configuración automática GPSD

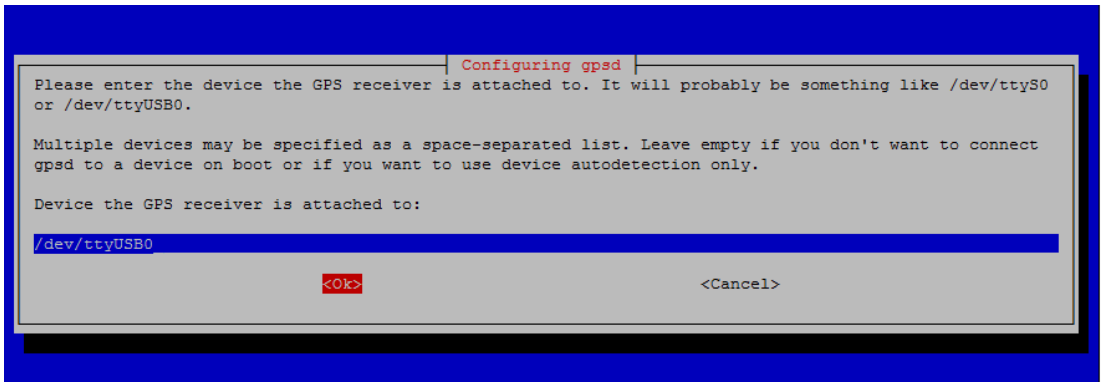



**Figura 17.** Adjuntar dispositivo receptor GPS

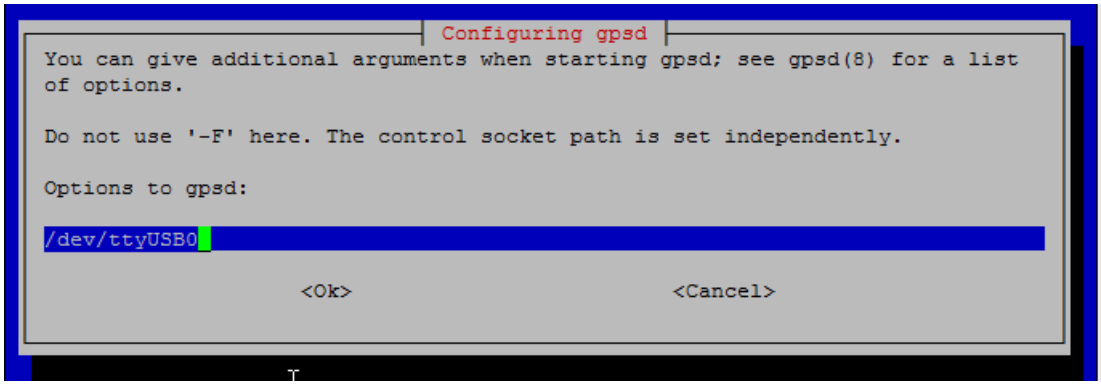



**Figura 18.** Ventana de configuración - Opciones de GPS

Una vez completados los cambios de configuración, se reinicia el *Raspberry Pi* y DSGP ahora se iniciará automáticamente como un servicio cuando el sistema se pone en marcha. Para verificarlo, asegúrese de que el dispositivo GPS está conectado con el dispositivo GPS situado cerca de una ventana para recibir una señal y ejecutar el comando:

**cgps -s**

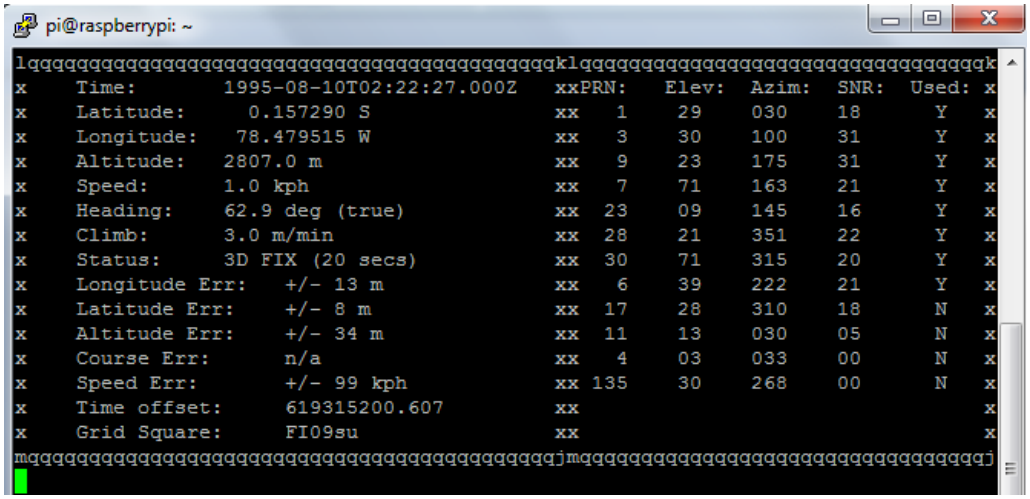



**Figura 19.** Salida CGPS

## 2.4 DESCRIPCIÓN DEL HARDWARE

### 2.4.1 Controladores y tarjetas

Algunos de los controladores de Linux más conocidos e importantes, se detallan a continuación [14]:

- Atheros (AR5XXX, AR9XXX).
- Broadcom (familia B43XX).
- Intel Pro *Wireless* e Intel Wifi Link (Centrino)
- Ralink (RT2X00)
- Realtek (RTL8187)

La característica más importante para seleccionar el dispositivo usb inalámbrico que necesitamos es el soporte de *modo monitor*.

### 2.4.1.1 Adaptador USB inalámbrico TP-LINK TL-WN722N

Adaptador USB inalámbrico le permite conectar una computadora de escritorio o portátil a una red inalámbrica y acceso de alta velocidad de conexión a Internet. Compatible con el estándar IEEE 802.11n, que proporciona velocidades inalámbricas de hasta 150Mbps. Además, el encriptado de seguridad inalámbrica puede establecerse simplemente en un empuje de QSS (Seguridad de configuración rápida) el botón, la prevención de la red de amenazas externas [19].

**Figura 20.** Módulo USB inalámbrico TP-LINK TL-WN722N

A continuación se detallan algunas características del equipo [19]:

**Tabla 2.**

Especificaciones Técnicas TP-LINK TL-WN722N

| CARACTERÍSTICAS INALÁMBRICAS | |
|---|---|
| **Estándares Inalámbricos** | IEEE 802.11n, IEEE 802.11g, IEEE 802.11b |
| **Frecuencia** | 2.400-2.4835GHz |
| **Velocidad de Señal** | 11n: Hasta 150Mbps (dinámico), 11g: hasta 54Mbps (dinámico) 11b: hasta 11Mbps (dinámico) |
| **EIRP** | <20dBm (EIRP, los países con normas CE) <27dBm (EIRP, los países con normas de la FCC) |

CONTINÚA

| | |
|---|---|
| **Sensibilidad de Recepción** | 130M:-68dBm @ 10% PER<br>108M:-68dBm @ 10% PER<br>54M:-68dBm @ 10% PER<br>11M:-85dBm @ 8% PER<br>6M:-88dBm @ 10% PER<br>1M:-90dBm @ 8% PER |
| **Modos Inalámbricos** | Modo Ad-Hoc/infraestructura |
| **Seguridad Inalámbrica** | Compatible con 64/128 bit WEP, WPA-PSK/WPA2-PSK |
| **Tecnología de Modulación** | DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM |
| **Funciones de Servicio** | WMM, Soft AP (para Windows XP / Vista), PSP X-LINK (sólo para Windows XP), Roaming |

### 2.4.1.2 Adaptador USB inalámbrico Alfa Network AWUS036NH

El dispositivo permite a los usuarios utilizar la normativa 802.11bgn a velocidades de 150Mbps en la banda de 2.4Ghz, la cual también es compatible con la anterior banda, la 802.11b/g para dispositivos de 54Mbps. Se puede configurar el AWUS036NH en modo ad-hoc para conectar con otros PCs o en modo infraestructura para conectar con AP o routers para conectarte a internet. Compatible con la normativa 802.11n y 802.11bgn. A continuación se detallan algunas características del equipo [20]:

**Tabla 3.**

Especificaciones Técnicas Alfa Network AWUS036NH

| **Modelo** | **AWUS036NH** |
|---|---|
| **Normativa** | Wireless: IEEE 802.11b/g/n, USB 2.0 standard |
| **Velocidad** | 802.11b: UP to 11Mbps<br>802.11g: UP to54Mbps<br>802.11n: UP to 150Mbps |
| **Sistemas Operativos** | Windows 2000, Windows XP, Windows Vista, Windows 7 Linux 2.6, Mac 10.4, 10.5, 10.6 |
| **Conector** | USB 2.0 mini USB |
| **Tipo de antena** | 1 x 2.4Ghz RP-SMA connector |
| **Chipset** | RT3070 |
| **Antena** | 5dBi 2.4GHz Antena |
| **Frecuencias** | 2.412~2.483 GHz |
| **Canales** | 1~11 channels ( North America )<br>1~13 channels ( General Europe)<br>1~14 channels (Japan) |

CONTINÚA

| | |
|---|---|
| **Potencia de salida** | 802.11b : 33dBm±1<br>802.11g : 32dBm±1<br>802.11n (HT20) : 32dBm±1<br>802.11n (HT40) : 33dBm±1 |
| **Sensibilidad** | 11b: -92dBm<br>11g: -76dBm<br>11n: -73dBm@HT20<br>-70dBm@HT40 |
| **Modulación** | BPSK,QPSK, CCK and OFDM |
| **Potencia** | Voltaje: 5V+5% |
| **Seguridad** | WEP 64/128<br>802.1X support<br>Wi-Fi Protected Access (WPA)<br>WPA-PSK, WPA II<br>Cisco CCX support<br>WAPI-PSK, WAPI-CERT Environment |
| **Temperatura** | 0°C ~ +50°C |
| **Almacenamiento** | -10°C ~ +65°C |
| **Cobertura** | 2000mW |


**Figura 21.** Módulo USB inalámbrico Alfa Network AWUS036NH

### 2.4.2 Receptor GPS

En la actualidad ya no es usual ver a gente utilizando un receptor GPS, ya que un chip GPS viene implementado en Smartphones, tablets, portátiles, etc. Pero hace no muchos años, cuando los GPS estaban en su auge, se sacó a la venta un tipo de receptor GPS, el cual no tenía pantalla, pero contenía unos LEDs para comprobar su funcionamiento y se podían conectar con USB o por Bluetooth. El receptor GPS que se ha decido utilizar tiene una conexión por cable USB con el cual se energiza.

### 2.4.2.1 GPS USB (GlobalSat BU-353S4 USB receptor de navegación GPS)

El BU-353-S4 es un GPS receptor USB que cuenta con un chipset de bajo consumo de energía de alta sensibilidad. El modo MicroPower del Bu-353-S4 permite que el receptor permanezca en una condición de arranque como en caliente de manera casi continua, mientras que consume muy poca energía [21].


**Figura 22.** Módulo GPS USB BU-353S4

Entre algunas características del equipo, se establecen [21]:

- Cantidad de canales: 48
- GPS, Precisión - posición: 2,5m. Peso: 62,37g
- Readquisición: 0,1s
- Sensibilidad: -163 dBm
- Sistema operativo MAC, Windows, Linux
- Tiempo de adquisición - caliente: 1s
- Tiempo de adquisición - frío: 35s
- Velocidad de actualización: 1 Hz
- Voltaje: 5V ± 5%, Corriente: 60mA típico
- Protocolo de GPS por defecto:
  - NMEA 0183 (Secundaria: SiRF binario)
  - SiRF binario >> posición, velocidad, altitud, estado y control
  - NMEA 0183 V3.0 protocolo MEA0183 y soportes

- Datos GPS salida: comando GGA, GSA, GSV, RMC, VTG, GLL v2.2 (VTG y GLL son opcionales)
- Velocidad de transferencia de GPS: ajuste de comandos de software (por defecto: 4800, n, 8,1 para NMEA)

## 2.5 WIRESHARK

### 2.5.1 Definición

*Wireshark* es una herramienta de red que captura el tráfico de la máquina dónde se está ejecutando, muestra mediante su interfaz gráfica los paquetes capturados. Permite analizar el tráfico que pasa por nuestro equipo, analizar los protocolos de red, ver direcciones IP, direcciones MAC, crear gráficas de tráfico, etc, [22].

### 2.5.2 Instalación

Una de las maneras de instalar en Linux, se describe a continuación [22]:

**sudo apt-get install wireshark**

- Si *wireshark* no está bien configurado no se podrá ver las tarjetas de red ni capturar y mostrará un error como el de la imagen siguiente:

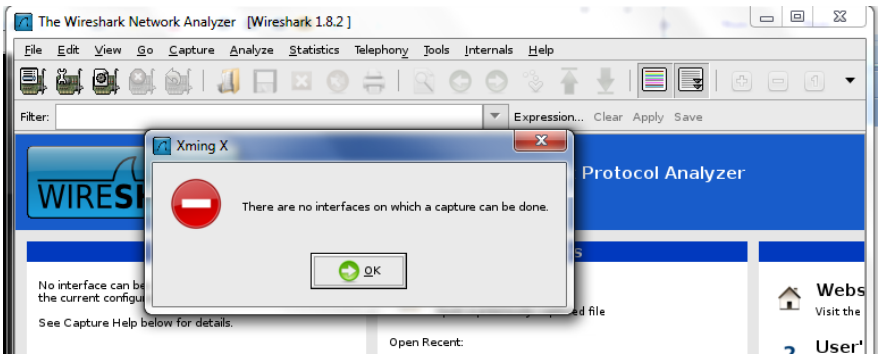



**Figura 23.** Error de instalación de Wireshark

Para solucionar el error y empezar a capturar con *wireshark*, se requiere dar privilegios de red para *dumpcap*.

```
sudo setcap 'CAP_NET_RAW+eip CAP_NET_ADMIN+eip' /usr/bin/dumpcap
```

- Ahora, ya se puede ejecutar como *root*.

```
sudo wireshark
```

### 2.5.3 Formato .pcap

La especificación PCAP es es el formato de fichero utilizado para almacenar capturas de tráfico de red desde analizadores de red [23]. El formato original PCAP, sin embargo, es deficiente en la descripción de cualquier cosa excepto los paquetes. Por suerte, hay un nuevo formato PCAP, PCAP-NG (Next Generation PCAP), con el apoyo inicial en libpcap, Wireshark, y otro software de análisis [24].

Los datos en un archivo PCAPNG se almacenan en bloques separados, lo que ayuda a estructurar los datos capturados por lo que puede ser reconstruido. Cada archivo PCAPNG contiene varios bloques o datos, que contienen diferentes tipos de información. Ejemplos de bloques incluyen el bloque de encabezado de sección, descripción de la interfaz de bloque, mayor bloque de paquete, el bloque de paquete simple, bloque de resolución de nombres, y el bloque de estadísticas de la interfaz. Estos bloques pueden ser utilizados para reconstruir los paquetes capturados en datos reconocibles [25].

Un archivo .pcap se estructura de la siguiente manera [26]:


**Figura 24.** Estructura archivo .pcap

- Las partes en azul son añadidos por el software *libpcap*, mientras que las partes en rojo son los datos reales capturados.

La primera parte del archivo es el encabezado global (*Global Header*), que se inserta una sola vez en el archivo, en el inicio. La cabecera global tiene un tamaño fijo de 24 bytes [26].

```
typedef struct pcap_hdr_s {
        guint32 magic_number;   /* magic number */
        guint16 version_major;  /* major version number */
        guint16 version_minor;  /* minor version number */
        gint32  thiszone;       /* GMT to local correction */
        guint32 sigfigs;        /* accuracy of timestamps */
        guint32 snaplen;        /* max length of captured packets, in octets */
        guint32 network;        /* data link type */
} pcap_hdr_t;
```

**Figura 25.** Estructura Global Header

En la Tabla 4, se detalla la funcionalidad de los campos de la estructura Global Header [27].

**Tabla 4.**

Global Header Fields

| | |
|---|---|
| **01-04b:** | Los primeros 4 bytes constituyen al parámetro *magic number* que se utiliza para identificar archivos pcap. |
| **05-08b:** | Los próximos 4 bytes son: major version number (2 bytes) y minor version number (2 bytes). El cuál es el número de versión del formato de archivo libpcap (la versión actual es 2.4). |
| **09-16b:** | El tiempo de corrección en segundos entre GMT (UTC) y la zona horaria local de las marcas de tiempo de encabezado de paquetes. En la práctica, las marcas de tiempo siempre están en GMT, por lo que esta zona es siempre 0. |
| **17-20b:** | Campo Snapshot Length (4 bytes) que indica la longitud máxima de los paquetes capturados (DataX) en bytes. Se establece en ff ff 00 00 lo que equivale a 65.535 (0xffff), el valor predeterminado para tcpdump y Wireshark. |
| **21-24b:** | Los últimos 4 bytes especifican *data link layer type*, especificando el tipo de encabezados en el principio del paquete (por ejemplo, 1 para Ethernet, esto puede ser de varios tipos, como 802.11, con diversa información de radio, PPP, Token Ring, FDDI, etc. |

Después de la cabecera global, tenemos un cierto número de: *packet header / data packet.*

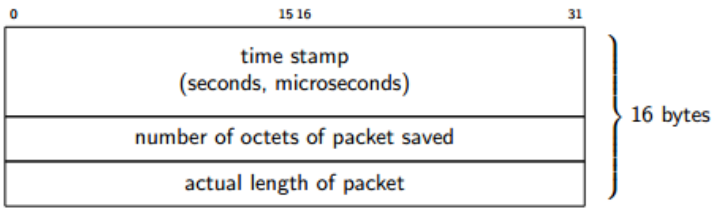



**Figura 26.** Estructura Packet Header

A continuación se detallan los campos del parámetro *packet header* [28]:

**Tabla 5.**

Packet Header Fields

| | |
|---|---|
| **ts_sec:** | Fecha y hora en que fue capturado el paquete. Este valor es en segundos Este es el número de segundos desde el comienzo de 1970, también conocido como Unix Epoch. |
| **ts_usec:** | Tiempo en microsegundos cuando fue capturado el paquete, como un desplazamiento a ts_sec. |
| **incl_len:** | El número de bytes de datos de paquetes realmente capturados y guardados en el archivo. Este valor no debe ser más grande que orig_len o el valor snaplen de la cabecera global. |
| **orig_len:** | La longitud del paquete que aparece en la red cuando fue capturado (54 Bytes). |

Después del parámetro *Packet Header* vienen los datos. El paquete de datos corresponde a 54b.

## 2.6 ESTÁNDAR IEEE 802.11

La especificación IEEE 802.11 es un estándar internacional que define las características de una red de área local inalámbrica (WLAN). En la práctica, Wifi admite ordenadores portátiles, equipos de escritorio, asistentes digitales personales (PDA) o cualquier otro tipo de dispositivo de alta velocidad con propiedades de conexión también de alta velocidad (11 Mbps o superior) dentro de un radio de varias docenas de metros en ambientes cerrados (de 20 a 50 metros en general) o dentro de un radio de cientos de metros al aire libre [29], [30].

Los estándares de la familia 802.11x se muestran en la tabla siguiente [29], [31]:

**Tabla 6.**

Familias de Estándares 802.11

| Estándar | Descripción |
|---|---|
| **802.11** | Estándar WLAN original, Soporta de 1 a 2 Mbps. |
| **802.11a** | Estándar WLAN de alta velocidad en la banda de los 5GHz. Soporta hasta 54Mbps. |
| **802.11b** | Estándar WLAN para la banda de 2.4GHz. Soporta 11 Mbps. |
| **802.11c** | Es una versión modificada del estándar 802.11d que permite combinar el 802.11d con dispositivos compatibles 802.11 (en el nivel de enlace de datos capa 2 del modelo OSI) |
| **802.11d** | Permite que distintos dispositivos intercambien información en rangos de frecuencia según lo que se permite en el país de origen del dispositivo móvil. |
| **802.11e** | Esta dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio. |
| **802.11f** | Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores. |
| **802.11g** | Establece una técnica de modulación adicional para la banda de los 2.4GHz. Dirigido a proporcionar velocidades de hasta 54Mbps. |
| **802.11h** | Define la administración del espectro de la banda de los 5GHz para uso en Europa y en Asia Pacifico. |
| **802.11i** | Esta dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. |
| **802.11n** | En la actualidad ya existen varios productos que cumplen el estándar N con un máximo de 600 Mbps (80-100 estables). El estándar 802.11n hace uso simultáneo de ambas bandas, 2,4 Ghz y 5 Ghz |
| **802.11ac** | El estándar consiste en mejorar las tasas de transferencia hasta 433 Mbit/s por flujo de datos, consiguiendo teóricamente tasas de 1.3 Gbit/s empleando 3 antenas. Opera dentro de la banda de 5 GHz, amplia el ancho de banda hasta 160 MHz (40 MHz en las redes 802.11n), utiliza hasta 8 flujos MIMO e incluye modulación de alta densidad (256 QAM). |

La norma 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI, es decir, capa física y la capa de enlace.

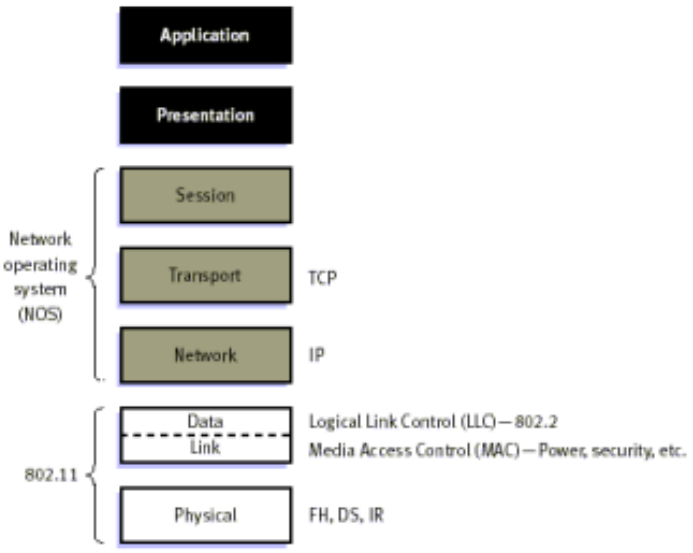



**Figura 27.** Modelo OSI y Familia IEEE 802.11

La capa física se divide en dos subcapas [32]:

- La subcapa inferior, PMD (Physical Media Dependent), que corresponde al conjunto de especificaciones de cada uno de los sistemas de transmisión a nivel físico. El estándar define cuatro: Infrarrojos, FHSS, DSSS u OFDM.
- La subcapa superior, PLCP (Physical Layer Convergence Procedure), se encarga de adoptar las diversas especificaciones de la subcapa PMD a la subcapa MAC, inmediatamente superior.

La capa de enlace también se divide a su vez en dos subcapas [32]:

- La subcapa MAC (Media Access Control), donde se especifica el protocolo de acceso al medio propiamente dicho, así como una serie de peculiaridades propias de redes inalámbricas como son el envío de acuses de recibo (ACK), la posibilidad de realizar fragmentación de las tramas y los mecanismos de encriptación para dar confidencialidad a los datos transmitidos.
- La subcapa LLC (Logical Link Control), ofrece un servicio de transporte único para todas las tecnologías.

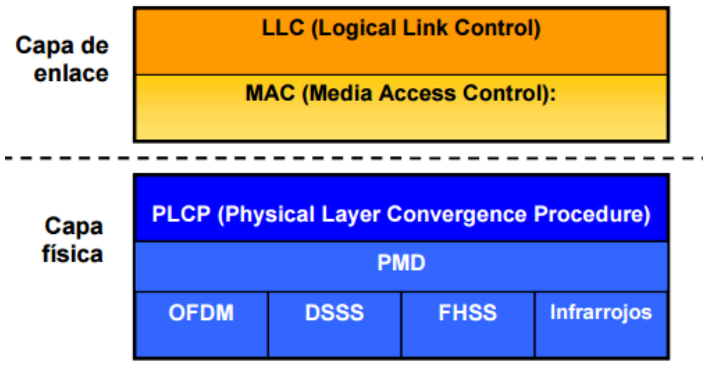



**Figura 28.** Modelo de referencia detallado de IEEE 802.11

### 2.6.1 Formato de Trama

El estándar 802.11 define varios tipos de tramas, las cuales se pueden clasificar dependiendo de la función que desempeñan. En la Figura 29 se muestra el formato general de la trama MAC para IEEE 802.11 [33].

Esta admite tres tipos de tramas:

- *Tramas de gestión*. Las tramas 802.11 de gestión son las que permiten mantener comunicaciones a las estaciones inalámbricas.
- *Tramas de control*. Las tramas 802.11 de control se utilizan para colaborar en la entrega de tramas de datos entre estaciones.
- *Tramas de datos.* Son las tramas que transportan la información de capas superiores.

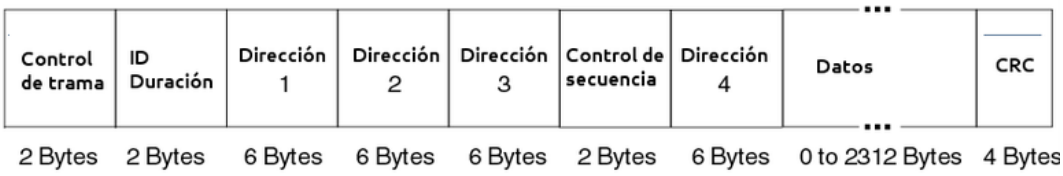



**Figura 29.** Formato trama MAC 802.11

Cada trama contiene distintos campos de control, que incluyen por ejemplo el tipo de trama, si WEP está activo, si está activo el ahorro de energía, la versión del protocolo 802.11. Una trama 802.11 también incluye las direcciones MAC de origen y destino, un número de secuencia, un campo de control y el campo de datos.

Para nuestro estudio los tipos de tramas más relevantes son las tramas de administración y control. En concreto las siguientes [29], [33], [34]:

#### 2.6.1.1 Tramas de Gestión

- **Beacon Frame**: Estas tramas son emitidas por el AP periódicamente, para anunciar la presencia de redes Wifi, la información de la red, el SSID, etc, a las estaciones clientes en su radio de cobertura. Mantienen el sincronismo entre las estaciones que usan la misma capa física ya que incorporan una marca de tiempo. Permiten a las estaciones obtener una lista de AP disponibles buscando tramas *Beacon* continuamente en todos canales 802.11. Contienen toda la información necesaria para identificar las características de la red y poder conectar con el AP deseado.
- **Probe Request:** Estas tramas son emitidas por los clientes cuando necesitan obtener información de un punto de acceso específico, especificando su SSID, o todos los puntos de acceso dentro del área de cobertura, especificando un SSID broadcast. Los clientes envían Probe Request en un canal y esperan durante un pequeño periodo de tiempo la respuesta (Probe Response). Si no reciben respuesta en este periodo de tiempo saltan de canal y vuelven a repetir el proceso.
- **Probe Response:** Cuando una estación recibe una Probe Request, responde con una trama Probe Response. Esta trama es unicast ya que va dirigida al cliente que ha realizado la petición. Esta trama contiene la información necesaria como por ejemplo capacidad necesaria, tasas de transmisión, etc.
- **Authentication:** Es el proceso por el cual un AP acepta o rechaza la identidad de un nodo que pretende conectarse con él. El nodo inicia el procedimiento enviando una trama de autenticación, si la autenticación es Abierta, el AP simplemente contesta con una trama de respuesta

afirmativa o negativa. Si el AP tiene definido el tipo opcional de Autenticación por frase de paso compartida (Shared Key Authtentication), el AP responde con una trama de respuesta conteniendo una frase de texto. El nodo deberá ahora enviar una versión encriptada de la palabra de paso usando su clave WEP para encriptar. El AP se asegura que el nodo tiene la clave WEP correcta desencriptando y comparando la frase de texto con la que envió previamente. Una vez validada la identidad del nodo, el AP envía una trama de respuesta afirmativa al nodo.

- **Association request:** Este tipo de trama la utiliza la estación cliente para iniciar el proceso de asociación por el cual el AP reserva recursos y sincroniza con una estación cliente. La asociación la inicia el cliente enviado al AP una trama de solicitud de asociación y el AP establece un ID de asociación para identificar al cliente y le reserva memoria. Las tramas de asociación contienen los datos necesarios para esta función como son el SSID de la red, las tasas de transferencia, etc.
- **Association response:** Este tipo de trama la utilizan los AP para responder una solicitud de asociación. Esta trama puede contener si se acepta o rechaza la asociación. Si se acepta la asociación la trama también incluye el ID de asociación y las tasas de transferencia admitidas.

#### 2.6.1.2 Tramas de Control

Las tramas 802.11 de control se utilizan para colaborar en la entrega de tramas de datos entre estaciones [33]:

- Trama Request to Send (RTS): Se utilizan para reducir las colisiones en el caso de dos estaciones asociadas a un mismo punto de acceso pero mutuamente fuera de rango de cobertura. La estación envía una trama RTS para iniciar el diálogo de comienzo de transmisión de una trama.
- Trama Clear to Send (CTS): Las estaciones utilizan las tramas CTS para responder a una trama RTS para dejar el canal libre de transmisiones. Las tramas CTS contienen un valor de tiempo durante el cual el resto de las estaciones dejan de transmitir el tiempo necesario para transmitir la trama.
- Tramas Acknowledgement (ACK): Las tramas ACK tienen como objetivo confirmar la recepción de una trama. En caso de no llegar la trama ACK el emisor vuelve a enviar la trama de datos.

El estándar 802.11 define dos funciones de escaneado diferentes; la exploración activa y pasiva [35]:

- Exploración Pasiva (Passíve Scanning): En este caso la estación debe esperar a recibir la Trama de Aviso (*Beacon* Frame) del AP, la cual es enviada periódicamente por el AP y contiene información de sincronización.
- Exploración Activa (*Active Scanning*): La estación trata de localizar al AP por transmisión de una Trama de Petición de Detección (*Probe Request Frame*), y espera por la respuesta (*Probe Response*) del AP.

Ambos métodos son válidos, y son elegidos de acuerdo al consumo de energía o desempeño de la conexión. Una vez que la estación localizó a un AP, y decide asociarse con este BSS, se debe pasar a través de un Proceso de Autenticación. Esto

es un intercambio de información entre la estación y el AP, donde la estación prueba pertenecer al dominio y da una clave de acceso. Una vez que la estación ha sido autenticada, comienza el Proceso de Asociación, consistente en el intercambio de información sobre las estaciones y las características de la BSS, con lo cual, los demás AP conocen la ubicación de la nueva estación. La estación estará habilitada a transmitir y recibir paquetes de información únicamente luego de haberse completado el Proceso de Asociación [35].

La figura 30 ilustra la etapa de establecimiento de conexión paso a paso.

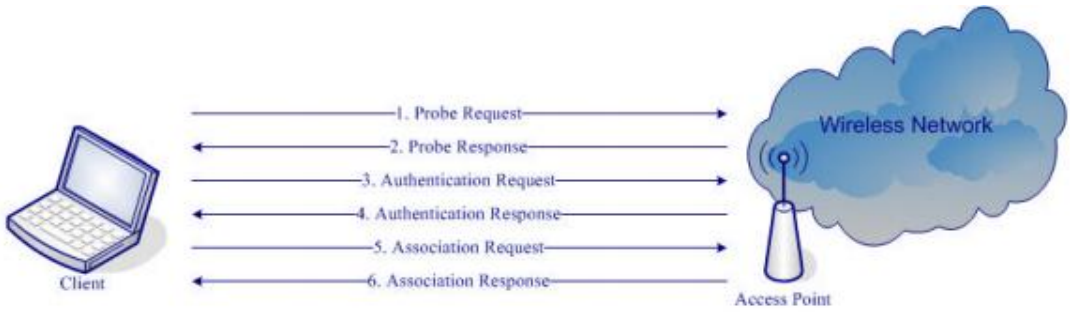



**Figura 30.** Client Authentication Process

El Estándar 802.11 define dos métodos para que los clientes se conecten a un AP los cuales son: Autenticación Abierta y Autenticación de Clave Compartida

El proceso de autenticación de cliente 802.11 consta de las siguientes operaciones [36]:

1. Los Ap envía continuamente *Beacon Frames* que son recogidos por los clientes WLAN cercanos.
2. El cliente también puede transmitir su propia *Probe Request* en cada canal.
3. Los AP dentro del rango responden con una trama *probe response*.

4. El cliente decide qué AP es el mejor para el acceso y envía una solicitud de autenticación (*authentication request*).
5. El AP envía una respuesta de autenticación (*authentication reply*).
6. Tras la autenticación exitosa, el cliente envía una trama de solicitud de asociación (*association request*) al AP.
7. El AP responde con una asociación de respuesta (*association response*).
8. El cliente es ahora capaz de pasar tráfico al AP.

El método de autenticación por clave compartida funciona de manera similar a la autenticación abierta, solo que comprueba el cliente, lo que requiere que ambos extremos tengan la misma clave compartida. Estos mecanismos originalmente estaban asociados al protocolo WEP, el primero que brindaba seguridad a las redes inalámbricas [37].

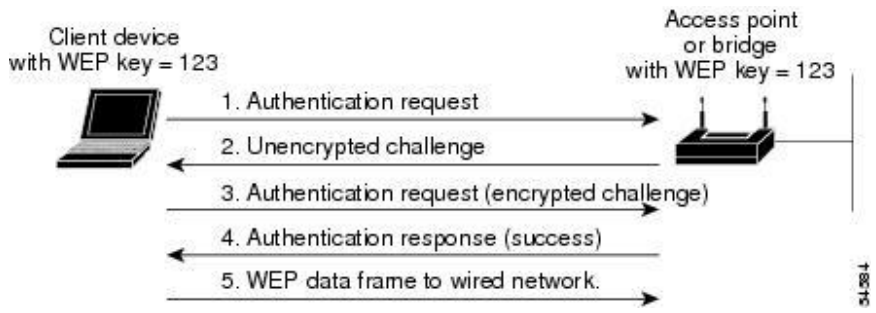



**Figura 31.** Autenticación de Clave Compartida

En la autenticación mediante clave compartida, WEP es usado para la autenticación. Este método se puede dividir en cuatro fases [38]:

1. El cliente envía una petición de autenticación al AP.
2. El AP genera un texto plano de 128 bytes aleatorio que envía al cliente esperando que éste, cifre dicho texto utilizando la clave WEP.

3. El cliente tiene que cifrar el texto usando la clave WEP ya configurada, y reenviarlo al AP en otra petición de autenticación.
4. El AP descifra el texto codificado y lo compara con el texto modelo que había enviado. Dependiendo del éxito de esta comparación, el AP envía una confirmación o una denegación. Después de la autenticación y la asociación, WEP puede ser usado para cifrar los paquetes de datos.

El Acceso protegido WPA/WPA2 es una mejora de la seguridad que aumenta considerablemente el nivel de protección de datos y el control del acceso a una red inalámbrica. Se definen dos mecanismos de autenticación. En el primero, los nodos son autenticados a través de una clave inicial compartida *PSK (Pre-Shared Key),* este modo está orientado para usuarios domésticos o pequeñas redes. La otra opción es el uso de *IEEE 802.1X* y el protocolo *EAP (Extensible Authentication Protocol),* que ofrecen mayor seguridad y generan una clave común como parte del proceso de autenticación [39].

**Tabla 7.**

Mecanismos de autenticación WPA/WPA2

| | | WPA | WPA2 |
|---|---|---|---|
| **Modo Personal** | Autenticación | PSK | PSK |
| | Cifrado | TKIP (RC4) / MIC | CCMP (AES) / CBC-MAC |
| **Modo Empresarial** | Autenticación | 802.1 x / EAP | 802.1 x / EAP |
| | Cifrado | TKIP (RC4) / MIC | CCMP (AES) / CBC-MAC |

Una de las mayores diferencias y mejoras entre WEP y WPA es que WPA ya no utiliza claves estáticas para cifrar los paquetes, si no que usa claves dinámicas. La contraseña de la red *Wifi* será el *Passpfrase*, a partir de esta se obtiene el PSK de 256 bit, ambas estarán también en el AP [40].

1. Una vez el cliente está conectado al AP, este envía un paquete llamado *Anonce* con información acerca del método que se usará para cifrar entre otras cosas.
2. Después el cliente generará para la conexión una clave PTK. La clave PSK 256 bits también es llamada PMK. El cliente contesta con un paquete que contiene el *Snounce* y MIC. El que nos importa es MIC que se ha creado a partir del PTK, es decir, que el AP lo descifrará y podrá comprobar que tiene el mismo PTK que el cliente.
3. El tercer paquete que se envía del AP al cliente es el *key installation*, indicando que se guarde la clave en el cliente.
4. Por último el cliente enviará un paquete ACK al AP y este guardará entonces la clave y así ambos tendrán la misma.

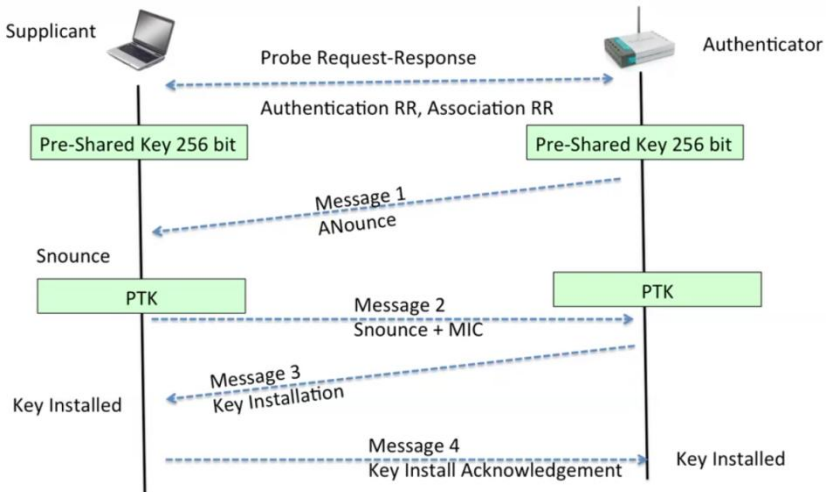



**Figura 32.** Autenticación PSK

802.1X utiliza un protocolo de autenticación llamado EAP que actúa como intermediario entre un solicitante y un motor de validación permitiendo la comunicación entre ambos. El proceso de validación está conformado por tres elementos [41], [42]:

- un solicitante que quiere ser validado mediante unas credenciales,
- un punto de acceso y
- un sistema de validación situado en la parte cableada de la red.

Para conectarse a la red, el solicitante se identifica mediante una credencial que pueden ser un certificado digital, una pareja nombre/usuario u otros datos. Junto con las credenciales, el cliente solicitante tiene que añadir también qué sistema de validación tiene que utilizar. Evidentemente no podemos pretender que el punto de acceso disponga del sistema de validación. En general EAP actúa de esta forma, recibe una solicitud de validación y la remite a otro sistema que sepa cómo resolverla y que formará parte de la red cableada. De esta forma vemos como el sistema EAP permite un cierto tráfico de datos con la red local para permitir la validación de un solicitante. El punto de acceso rechaza todas las tramas que no estén validadas, que provengan de un cliente que no se he identificado, salvo aquéllas que sean una solicitud de validación. Estos paquetes EAP que circulan por la red local se denominan EAPOL (EAP over LAN). Una vez validado, el punto de acceso admite todo el tráfico del cliente [41], [42].

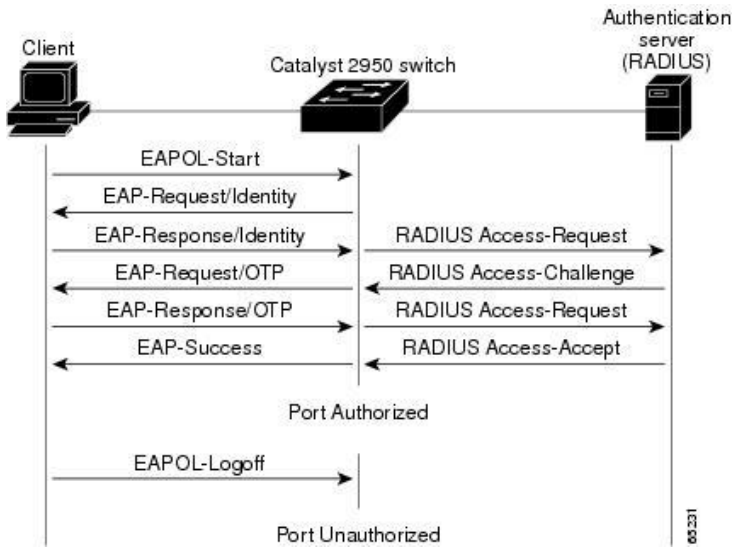



**Figura 33.** Autenticación 802.1x

El sistema de autenticación puede ser un servidor RADIUS situado en la red local. Los pasos que sigue el sistema de autenticación 802.1X son [42]:

1. El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
2. El AP responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
3. El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajena al AP.
4. El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
5. El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
6. El AP devuelve un paquete EAP de acceso o de rechazo al cliente.
7. Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

El protocolo 802.1X tiene un mecanismo de autenticación independiente del sistema de cifrado. Si el servidor de validación 802.1X está configurado adecuadamente, se puede utilizar para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación. El punto de acceso utiliza las claves de sesión para construir, firmar y cifrar el mensaje de clave EAP que se

manda tras el mensaje de aceptación. El cliente puede utilizar el contenido del mensaje de clave para definir las claves de cifrado aplicables [43].

## 2.7 ROAMING WIFI

Un aspecto muy importante de las redes *Wifi* es la movilidad. Por ejemplo, una persona puede caminar a través de una instalación en el ejercicio de una conversación sobre un teléfono *Wifi* o al descargar un archivo de gran tamaño desde un servidor. El radio *Wifi* en el interior del dispositivo de usuario se desplaza automáticamente de un AP a otro según sea necesario para proporcionar una conectividad sin fisuras.

### 2.7.1 Roaming

La itinerancia, más conocido por su término en ingles *roaming* es un concepto que define la capacidad de un dispositivo inalámbrico para poder desplazarse de una zona de cobertura a otra. Cada zona de cobertura está gobernada por un AP diferente. El concepto de *roaming*, cuando es utilizado en las redes inalámbricas, significa que el dispositivo cliente puede desplazarse e ir registrándose en diferentes bases o puntos de acceso, sin perder en ningún momento acceso a la red. Para que esta itinerancia sea posible, tiene que haber una pequeña superposición en las coberturas de los AP, de tal manera que los usuarios puedan desplazarse y siempre tengan cobertura [44].

Los AP Inalámbricos tienen un radio de cobertura aproximado de 100 m aunque, esto varía bastante en la práctica entre un modelo y otro y según las condiciones ambientales y físicas del lugar (obstáculos, interferencias, etc). Si nos interesa permitir la itinerancia y movilidad de los usuarios, es necesario colocar los AP de tal

manera que haya "*overlapping*" - superposición - entre los radios de cobertura, como indica la próxima Figura 34:

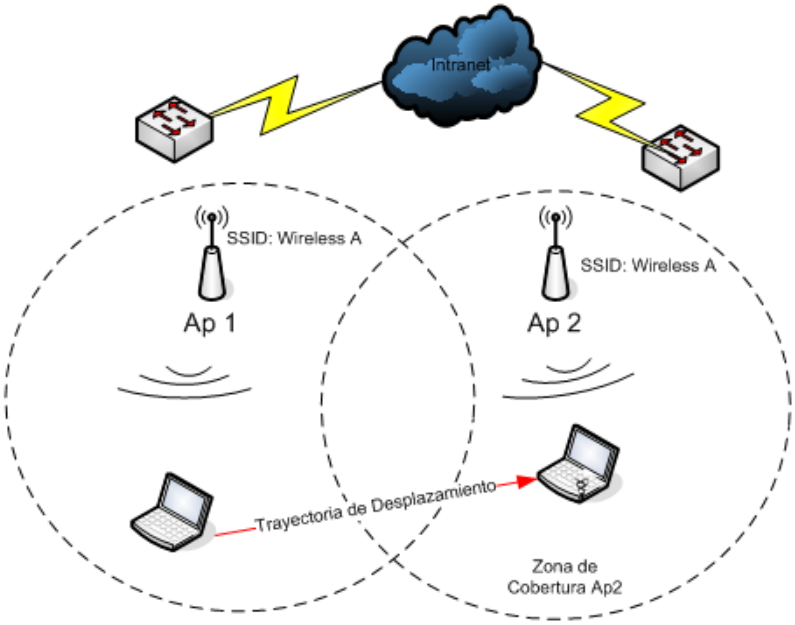



**Figura 34.** Condiciones para el Roaming

En ella vemos la zona de superposición y la trayectoria de desplazamiento indicada por la flecha roja (ver Figura 34) y cómo es posible desplazarse de AP1 a AP2, sin perder la señal WIFI. El usuario está conectado al comienzo al AP1 y en un determinado momento pasa a recibir la señal del AP2 [44].

Cuando utilizamos AP inalámbricos, éstos emiten intermitentemente paquetes denominados *Beacon*s. Cuando una terminal se aleja demasiado de un AP, "pierde la señal", es decir que deja de percibir estos *Beacon*s que le indican la presencia del AP, pero si hay superposición de canales, se comienzan a captar los *Beacon*s del otro AP, hacia el cual se está dirigiendo, a la vez que se van perdiendo gradualmente los del anterior con lo que se efectúa el *roaming*. Para que esto se haga de una manera correcta y sin cortes deben ajustarse los parámetros internos de la tarjeta de radio de

manera adecuada a la velocidad que se mueve terminal móvil. Además una vez que se envía un paquete de datos en las redes inalámbricas *Wifi*, la estación receptora envía un "OK.", denominado ACK. Si la estación emisora se aleja demasiado de la transmisora, es decir que sale del radio de cobertura, no captará los ACK enviados. Los equipos de *Wifi* incorporan un algoritmo de decisión que debe determinar en qué momento se desconectan del AP1 y se conectan al AP2 [44].

### 2.7.2 Triangulación

La triangulación mediante GPS consiste en averiguar la distancia de cada una de las tres señales respecto al punto de medición. Conocidas las tres distancias se determina fácilmente la propia posición relativa respecto a los tres satélites. Además es indispensable conocer las coordenadas o posición de cada uno de los satélites. De esta forma se obtiene la posición absoluta o coordenada reales del punto de medición [45].

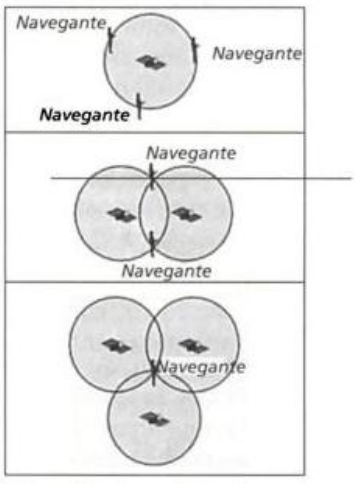



**Figura 35.** Triangulación para hallar la posición mediante satélites GPS

El cálculo de la propia posición, usando señales GPS, se realiza por triangulación, lo que significa que sabiendo la distancia de tres puntos fijados, podemos obtener la propia posición. El receptor mide la distancia desde el satélite 1,

lo que representa que el navegante está en algún lugar del círculo que rodea al satélite 1. A continuación, el satélite mide la distancia al satélite 2. El receptor está en algún lugar de los círculos que rodena a los satélites 1 y 2. Solo hay dos posiciones en las que el receptor puede estar y son donde los dos círculos se intersecan. A continuación, el receptor mide la distancia del satélite 3 y, del mismo que antes, sabe que su posición esta donde los tres círculos intersecan y esto ocurre en un solo punto. De esta forma se calcula la posición del navegante (ver Figura 35) [46].

Este proceso fácilmente se lo realiza por medio del cálculo de la potencia recibida para el cálculo de las distancias desde el receptor, punto del equipo Access Point, hasta el receptor, módulo *wifi* conectado al equipo *Raspberry Pi*, dibujando los círculos y verificando la intersección de los mismos.

# CAPITULO III

# DISEÑO E IMPLEMENTACIÓN

## 3.1 DEFINICIÓN DEL PROBLEMA

Una vez detectado la red inalámbrica dentro del entorno de la institución educativa, se requiere determinar las características de funcionamiento, configuraciones y parámetros necesarios para la implementación y uso del software *Kismet* sobre la minicomputadora *Raspberry Pi*, con el fin de validar y analizar el desempeño del prototipo mediante el análisis de tráfico de las redes inalámbricas y georeferenciación de los AP cliente en la red *wireless* de la Universidad de las Fuerzas Armadas - ESPE.

## 3.2 PROPUESTA DEL PROTOTIPO

El modelo del prototipo propuesto para el sistema de análisis de tráfico de redes 802.11 pretende implementar en una ambiente de pruebas, mediante la utilización de la minicomputadora *Raspberry Pi*, la instalación de programas bajo la plataforma *Raspbian* y componentes necesarios para la puesta en funcionamiento de un sistema de analizador de tráfico de red para el monitoreo y administración, así como para determinar la ubicación de los AP dentro de la red.

## 3.3 DETERMINACIÓN DE LOS PARÁMETROS DEL PROTOTIPO

Para determinar los parámetros de utilización del equipo prototipo fue necesario realizar pruebas en todo el campus de la Universidad, en donde el equipo detectará y analizará las redes inalámbricas del campus así como la ubicación georeferencial de los AP.

En base a estas pruebas se tiene los siguientes parámetros de empleo del equipo:

- El equipo prototipo dispone de equipos eléctricos y electrónicos sensibles al agua, por esta razón el equipo no puede ser empleado en momentos en los que exista lluvia.
- El equipo prototipo es un dispositivo móvil que necesita de una persona que esté a cargo de su cuidado al momento de realizar su análisis.
- El equipo prototipo necesita de un adaptador de energía o batería; ya que al ser un sistema portable no requiere de lugares específicos para su funcionamiento, ni de ser conectado a la red eléctrica para su empleo.

## 3.4 PROCEDIMIENTO DE UTILIZACIÓN DEL PROTOTIPO

Para la utilización del equipo prototipo es necesario determinar el lugar donde sea desea emplear el equipo dentro del espacio abierto del campus de la Universidad de las Fuerzas Armadas - ESPE.

El procedimiento de utilización del equipo tiene dos etapas definidas:

1. La primera es una etapa de identificación y análisis, en donde el equipo se encuentra ubicado en todo el espacio abierto del campus para el monitoreo y administración de la red así como para determinar el análisis de *roaming* del cliente dentro de la red de la Universidad de las Fuerzas Armadas – ESPE; para esto el equipo funciona empleando el uso de la placa reducida *Raspberry Pi* y un módulo *GPS*.
2. La segunda es la etapa de análisis de resultados, en este caso el equipo se encuentra dentro de una oficina y es aquí junto a una computadora donde se revisan cada uno de los archivos generados por *Kismet* para identificar georeferencialmente los AP y determinar diferentes parámetros de desempeño de la red.

## 3.5 IMPLEMENTACIÓN

Para la realización de la prueba utilizaremos los siguientes dispositivos:

- Raspberry Pi Modelo B+ 512 MB de RAM
- Tarjeta de memoria SD de 4 GB o más grande
- Adaptador de red inalámbrico USB capaz de inyección de paquetes (Tp-Link TL-WN722N)
- Receptor GPS USB (GlobalSat BU-353S4 USB receptor de navegación GPS)
- Adaptador de alimentación USB de 5V - 2A (batería con puertos USB (PowerGen® 8400mAh)) y cable micro USB


**Foto 1.** Dispositivos necesarios para el proyecto

### 3.5.1 Configuración GPS

El objetivo de este proyecto es recoger datos sobre redes inalámbricas dentro un área dada; pero una lista de redes inalámbricas, sin importar el grado de detalle, no es muy útil si no se puede encontrar nunca esa red de nuevo. Es por eso que la mayoría

de las herramientas de wardriving apoyan alguna forma de localización por GPS que permite asociar una red descubierta con su ubicación física.

Kismet adquiere su apoyo GPS de *gpsdrive* usando *gpsd*. Una vez gpsd ha sido instalado (ítem 2.3.3.2), este programa se conecta al dispositivo GPS y ofrece los datos a cualquier programa mediante una conexión TCP por el puerto 2947. Se necesita habilitar las funciones de GPS en Kismet. Para habilitar el soporte GPS, se requiere editar el archivo de configuración *kismet.conf* y buscar la línea:

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

Se necesita cambiar por:

```
gps=true
```

Una vez instalado DSGP se descomenta las líneas apropiadas para que coincida con lo siguiente [17]:

```
# Do we use a locally serial attached GPS, or use a gpsd server, or
# use a fixed virtual gps?
# (Pick only one)
gpstype=gpsd
# Host:port that GPSD is running on. This can be localhost OR remote!
gpshost=localhost:2947
```

### 3.5.2 Configuración Kismet

Para la captación de redes se usará *Kismet*, este se puede configurar en modo automático en tiempo de ejecución, puesto que no se ha encontrado mucha documentación para modificar el fichero de configuración de la última versión *(/usr/local/etc/kismet.conf*).

Una vez instalado y modificado el fichero como lo indica el ítem 2.3.3.1.1; en la terminal escribiremos el comando: *sudo Kismet* y le damos Intro. Nos aparecerá la siguiente ventana:

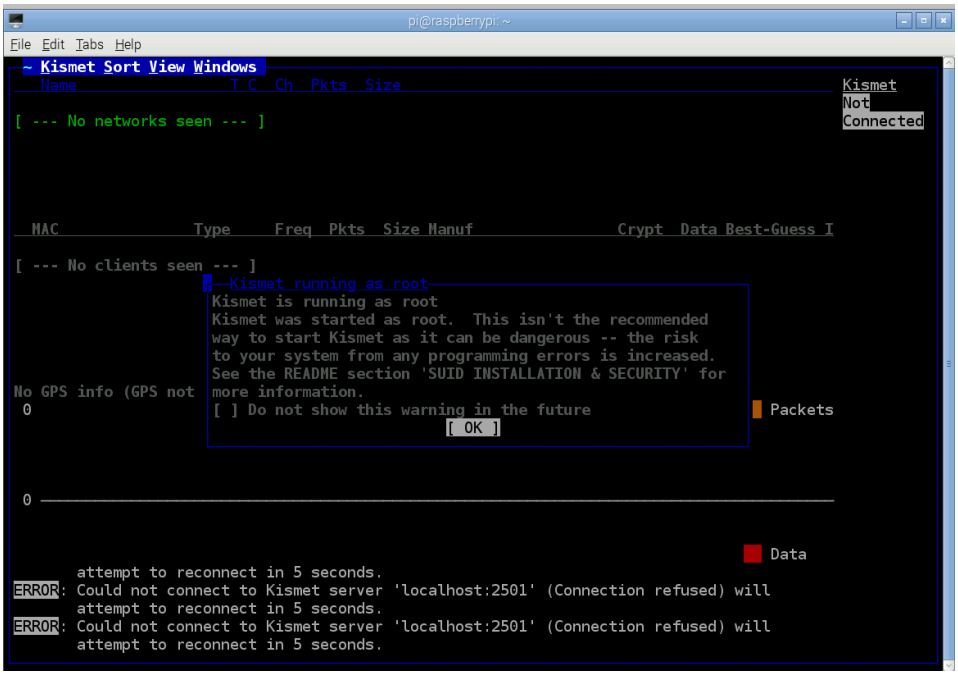



**Figura 36.** Ventana inicial de Kismet

En el Figura 36, nos indica un mensaje que dice que se está ejecutando Kismet desde el usuario root. En la siguiente Figura, se muestra el mensaje pidiendo ejecutar el servidor de Kismet automáticamente, pulsaremos Yes.

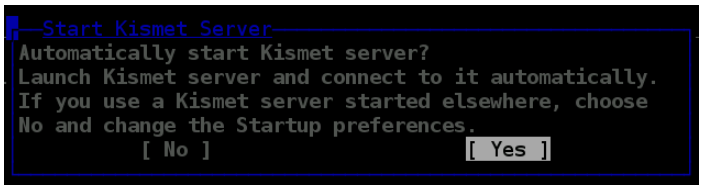



**Figura 37.** Solicitud de inicio automático Kismet server

Después de arrancar el servidor la pantalla a mostrar será la siguiente:

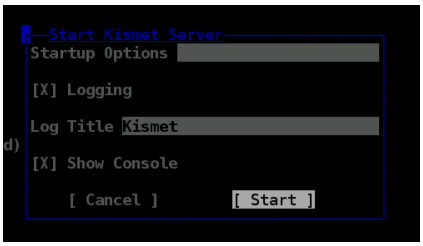



**Figura 38.** Start Kismet Server

Pulsamos Start y nos aparecerá la consola del servidor de Kismet

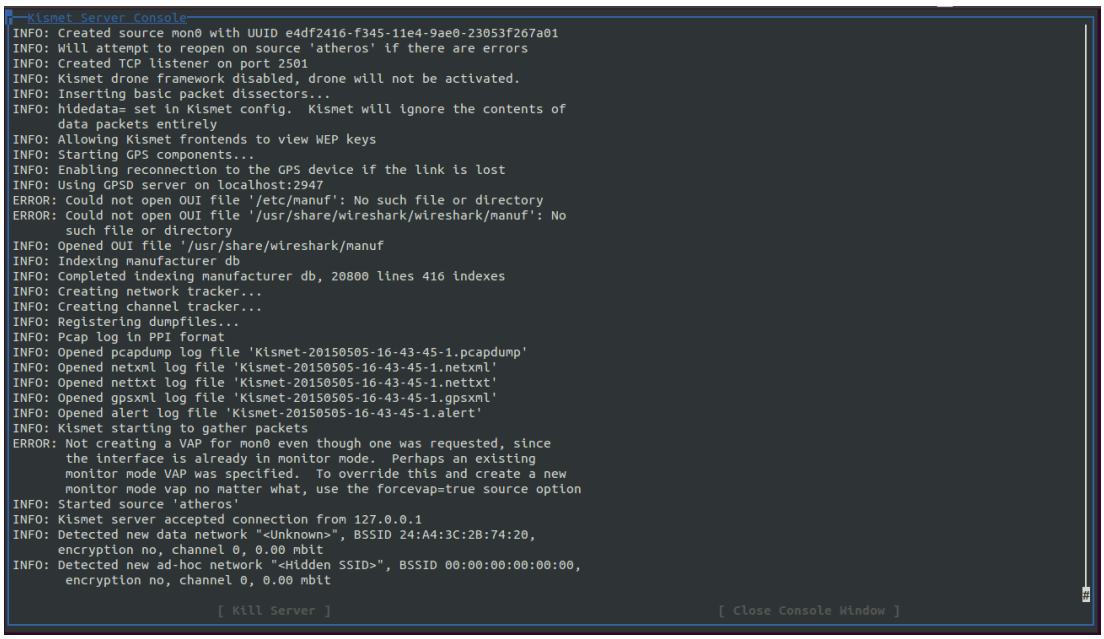



**Figura 39.** Consola Servidor Kismet

Dentro de las líneas más importantes que se verifican en los mensajes de Info se muestra:

INFO: Opened pcapdump log file 'Kismet-20150505-16-43-45-1.pcapdump'

INFO: Opened netxml log file 'Kismet-20150505-16-43-45-1.netxml'

INFO: Opened nettxt log file "Kismet-20150505-16-43-45-1.nettxt'

INFO: Opened gpsxml log file 'Kismet-20150505-16-43-45-1.gpsxml'

INFO: Opened alert log file 'Kismet-20150505-16-43-45-1.alert'

# CAPITULO IV

# VALIDACIÓN Y PRUEBAS

Este capítulo contempla la preparación del escenario de pruebas en el entorno de red del campus universitario; y puesta en marcha de los programas, software y hardware, con el fin de establecer los parámetros necesarios para la correcta implementación del prototipo de sistema de análisis de tráfico de redes 802.11, además de las características de funcionamiento y sus limitaciones con el fin de obtener un análisis de las respuestas obtenidas tanto en *Kismet* como *Wireshark*.

## 4.1 PROCESO DE CAPTURA

Una vez establecidas y obtenidas las herramientas necesarias, se procede a la realización de las capturas. El proceso de captura es la etapa donde se recogen todos los datos necesarios para su posterior análisis. Para ejecutar las capturas se dispuso de la mini computadora *Raspberry Pi B+*, un dispositivo USB inalámbrico capaz de trabajar en la banda de 2,4 y 5GHz, además de un módulo usb GPS junto al software de análisis de tráfico *Kismet*, capaz de recopilar todas las tramas IEEE 802.11; para la etapa de verificación y análisis de resultados se dispone de un ordenador portátil bajo el sistema operativo Linux.

El método de captura, consiste en ejecutar el software *Kismet* recorriendo el campus de la universidad, capturando paquetes de datos de redes inalámbricas bajo los estándares IEEE 802.11a/b/g/n.


**Foto 2.** Prototipo de Sistema de Análisis de tráfico de redes 802.11

Las capturas fueron realizadas a pie, a una velocidad moderada de 6Km/h, para poder capturar el máximo número de redes. De acuerdo al tiempo o entorno en el que se realice la captura, éstas contendrán más o menos cantidad de redes capturadas.

Se definió un escenario por sus características de infraestructura. Los escenarios de este trabajo son:

- Zonas HotSpot (HotS): Campus universitarios y centros comerciales.
    - Entorno 1: Laboratorio de Electrónica
    - Entorno 2: Recorrido interno campus universitario.

En este escenario, se encontrarán AP distribuidos de forma más eficiente con configuraciones homogéneas más elaboradas y conviviendo con redes inalámbricas de ambas bandas (2,4GHz y 5GHz) [29].

## 4.2 ANÁLISIS DE DESEMPEÑO

Durante el proceso de ejecución del proyecto, se encontró múltiples inconvenientes al momento de visualizar los resultados obtenidos con el archivo

*.pcapdump*, ya que, se presentan en las tramas mensajes de error como: "*Malformed Packet"*; por esta razón se realiza una serie de procesos y análisis con el fin de determinar la razón para la obtención de estos paquetes con error.

Una vez comprobada la instalación de *Kismet* y analizada la configuración del fichero *kismet.conf*, se pretende revisar las características y funcionalidades de la *Raspberry Pi*, ya que en muchas ocasiones es necesario vigilar el uso del CPU o el uso de memoria RAM para determinar su funcionamiento.

### 4.2.1 Desarrollo de pruebas

Se han realizado una serie de pruebas utilizando el adaptador inalámbrico Atheros (ítem 2.4.1.1) en un computador instalado el software Kismet, además utilizando otro modelo de tarjeta *Raspberry Pi* en el mismo ambiente de trabajo.

- Escenario 1: Se ha realizado el análisis de Kismet con la última versión disponible inmersa en la Raspberry Pi B+, ejecutándose durante 15 minutos dentro del entorno del Laboratorio de Electrónica de la institución educativa; del archivo generado por la herramienta con el nombre Kismet-20150505-16-43-45-1.pcapdump (5.8Mb) se obtiene los siguientes resultados:

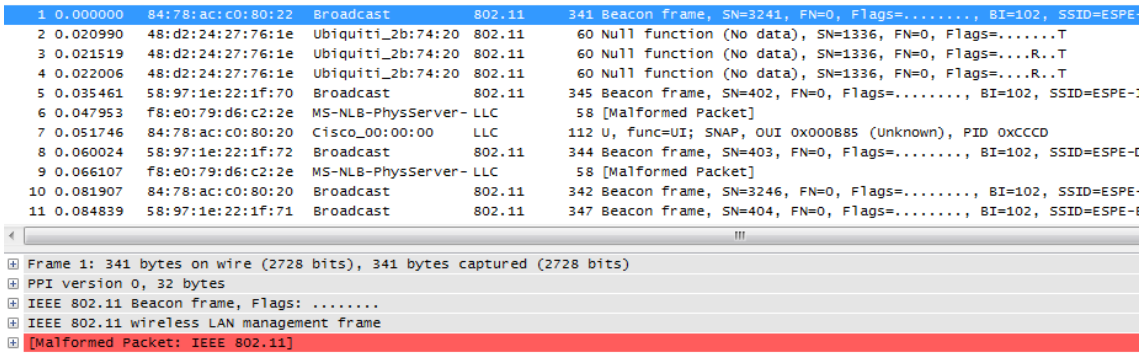



**Figura 40.** Archivo .pcapdump - Malformed Packets Raspberry Pi B+

En la Figura 41, se puede verificar que de 49219 paquetes totales capturados se tiene 11976 paquetes malformados IEEE 802.11, de lo cual nos proporciona 24.33% de la trama con error.

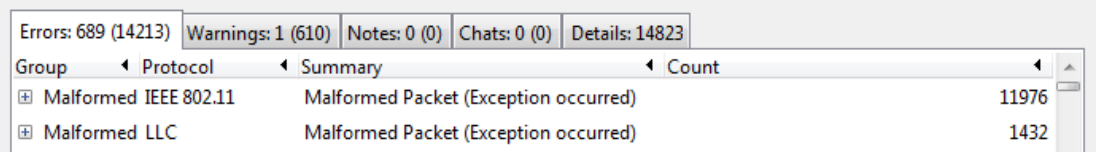



**Figura 41.** Detalles de Error: Malformed IEEE 802.11

Dentro de las estadísticas del tráfico WLAN capturado, se resume el tráfico de la red inalámbrica capturada.

Network Overview

| BSSID | Ch. | SSID | % Packets | Beacons | Data Packets | Probe Req | Probe Resp | Auth | Deauth | Other | Protection |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Broadcast | 3 | <Broadcast> | 1,02 % | 0 | 0 | 18 | 0 | 0 | 0 | 0 | |
| D-LinkIn_8b:65:5a | 6 | CIM2014 | 6,24 % | 97 | 0 | 2 | 11 | 0 | 0 | 0 | |
| Apple_fd:b6:93 | 6 | CIM2014 | 2,84 % | 50 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Apple_13:33:9f | 11 | EDDmac | 1,48 % | 26 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Ubiquiti_29:b0:a1 | 1 | eduroam test | 0,06 % | 0 | 0 | 0 | 1 | 0 | 0 | 0 | |
| Broadcast | 2 | ESPE | 0,57 % | 0 | 0 | 10 | 0 | 0 | 0 | 0 | |
| 84:78:ac:c0:80:23 | 1 | ESPE-ADMINISTRATIVOS | 0,62 % | 9 | 0 | 2 | 0 | 0 | 0 | 0 | |
| 58:97:1e:22:1f:73 | 1 | ESPE-ADMINISTRATIVOS | 1,14 % | 20 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 58:97:1e:b2:4d:03 | 11 | ESPE-ADMINISTRATIVOS | 5,68 % | 94 | 0 | 0 | 6 | 0 | 0 | 0 | |
| Cisco-Li_a0:3f:80 | 6 | ESPE-DEEE | 1,36 % | 23 | 0 | 1 | 0 | 0 | 0 | 0 | |
| 84:78:ac:c0:80:22 | 1 | ESPE-DOCENTES | 0,79 % | 11 | 0 | 3 | 0 | 0 | 0 | 0 | |
| 58:97:1e:22:29:62 | 1 | ESPE-DOCENTES | 0,06 % | 1 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 58:97:1e:22:1f:72 | 1 | ESPE-DOCENTES | 0,96 % | 15 | 0 | 0 | 2 | 0 | 0 | 0 | |
| 58:97:1e:b2:4d:02 | 11 | ESPE-DOCENTES | 6,24 % | 91 | 0 | 0 | 15 | 3 | 0 | 1 | |
| 58:97:1e:22:1f:71 | 1 | ESPE-ESTUDIANTES | 0,57 % | 8 | 0 | 2 | 0 | 0 | 0 | 0 | |
| 84:78:ac:c0:80:21 | 1 | ESPE-ESTUDIANTES | 0,85 % | 11 | 0 | 2 | 2 | 0 | 0 | 0 | |
| 58:97:1e:b2:4d:01 | 11 | ESPE-ESTUDIANTES | 6,92 % | 107 | 0 | 0 | 15 | 0 | 0 | 0 | WEP |
| 58:97:1e:22:1f:70 | 1 | ESPE-INVITADOS | 0,91 % | 13 | 0 | 3 | 0 | 0 | 0 | 0 | |
| 58:97:1e:b2:4d:00 | 11 | ESPE-INVITADOS | 6,13 % | 94 | 0 | 0 | 13 | 1 | 0 | 0 | |
| 84:78:ac:c0:80:20 | 1 | ESPE-INVITADOS | 0,57 % | 10 | 0 | 0 | 0 | 0 | 0 | 0 | |
| Cisco_00:00:00 | 1 | ESPE-INVITADOS | 0,17 % | 0 | 3 | 0 | 0 | 0 | 0 | 0 | |
| 58:97:1e:22:1f:75 | 1 | ESPE-ZONA-LIBRE | 1,25 % | 13 | 0 | 6 | 3 | 0 | 0 | 0 | |
| 84:78:ac:c0:80:25 | 1 | ESPE-ZONA-LIBRE | 0,57 % | 7 | 0 | 0 | 2 | 0 | 0 | 1 | |
| 58:97:1e:b2:4d:05 | 11 | ESPE-ZONA-LIBRE | 7,09 % | 112 | 0 | 0 | 12 | 1 | 0 | 0 | |
| D-Link_a7:d0:1e | 1 | ITURVAS | 0,91 % | 11 | 0 | 0 | 4 | 0 | 0 | 1 | |
| Broadcast | 4 | LabMov | 0,06 % | 0 | 0 | 1 | 0 | 0 | 0 | 0 | |
| Broadcast | 4 | LabMov | 0,06 % | 0 | 0 | 1 | 0 | 0 | 0 | 0 | |
| Apple_1c:d2:5e | 11 | MacBook Pro de MISAHAEL | 2,50 % | 27 | 0 | 0 | 15 | 0 | 0 | 2 | |
| Ubiquiti_68:bb:83 | 2 | PUNTONET TERRACOTA | 0,11 % | 0 | 0 | 0 | 2 | 0 | 0 | 0 | |
| Ubiquiti_68:ab:4a | 8 | PUNTONET TERRACOTA 3 | 0,34 % | 6 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 78:54:2e:5a:cb:ea | 9 | RED_SNNA | 1,42 % | 11 | 0 | 6 | 8 | 0 | 0 | 0 | |
| D-Link_c9:e6:45 | 7 | RED_SNNA | 9,36 % | 165 | 0 | 0 | 0 | 0 | 0 | 0 | |
| IntelCor_94:f5:39 | 11 | RedClu | 0,28 % | 0 | 0 | 1 | 4 | 0 | 0 | 0 | |
| c8:b3:73:14:dd:f9 | 6 | SAT | 7,49 % | 122 | 0 | 3 | 7 | 0 | 0 | 0 | |
| D-LinkIn_45:9b:0c | 8 | TrabajaYnoEnvidies | 0,06 % | 1 | 0 | 0 | 0 | 0 | 0 | 0 | |
| 78:54:2e:57:88:ae | 4 | WFRAB | 10,27 % | 139 | 0 | 12 | 29 | 1 | 0 | 0 | WEP |
| 78:54:2e:0e:46:51 | 4 | wfrab1 | 8,34 % | 113 | 0 | 5 | 29 | 0 | 0 | 0 | |
| Ubiquiti_84:f9:5d | 10 | www.ubnt.com | 4,71 % | 48 | 0 | 3 | 32 | 0 | 0 | 0 | |
| Apple_ff:94:73 | 6 | \020\000\020\000\003\000\003\000\ | 0,06 % | 0 | 0 | 0 | 0 | 0 | 0 | 1 | |

**Figura 42.** Porcentajes de tráfico correspondientes a cada SSID detectado

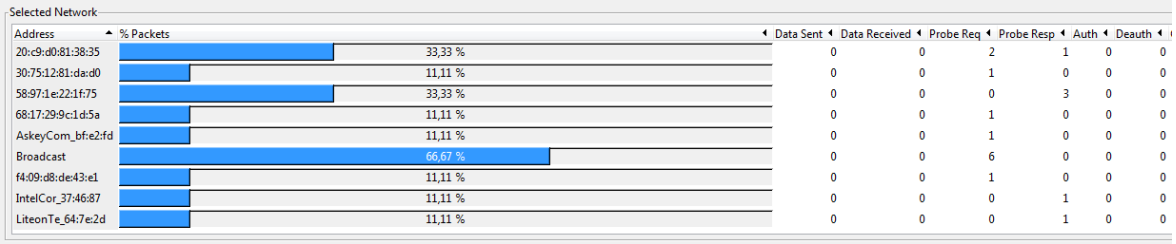



**Figura 43.** Porcentajes de tráfico de clientes, red: “ESPE-ZONA-LIBRE”

Cada fila de la lista muestra los valores estadísticos para exactamente una red inalámbrica.

Con esta herramienta *Statistics/WLAN Traffic*, se puede apreciar los porcentajes de tráfico recolectados en un intervalo de quince minutos, en la figura 42 se puede observar que un 7,09% del tráfico pertenece al SSID de ESPE-ZONA-LIBRE con BSSID de 58:97:1e:b2:4d:05. Por otro lado se puede apreciar que dentro del SSID de interés (Figura 43) los que generan mayor tráfico son la MAC del AP (20:c9:d0:81:38:35) junto a la MAC del BSSID (58:97:1e:22:1f:75) con un 33,33%, la MAC del BSSID (ff:ff:ff:ff:ff:ff) con un 66,67%, porcentajes que pertenecen a su partición en los diferentes tipos de tramas de datos (tomando el papel de destino u origen).

Durante la ejecución de Kismet, se monitoreaba el procesamiento y uso de CPU de la tarjeta Raspberry Pi mediante el comando *top*, el cual proporciona una vista dinámica de la actividad del procesador en tiempo real; puede mostrar una lista de las mayoría de tareas intensivas de CPU en el sistema, rendimiento del equipo, consumo de la RAM, etc. Al ejecutar *top*, se abre un monitor de recursos del sistema y aparece una interfaz en modo texto que se va a ir actualizando cada tres segundos [47].

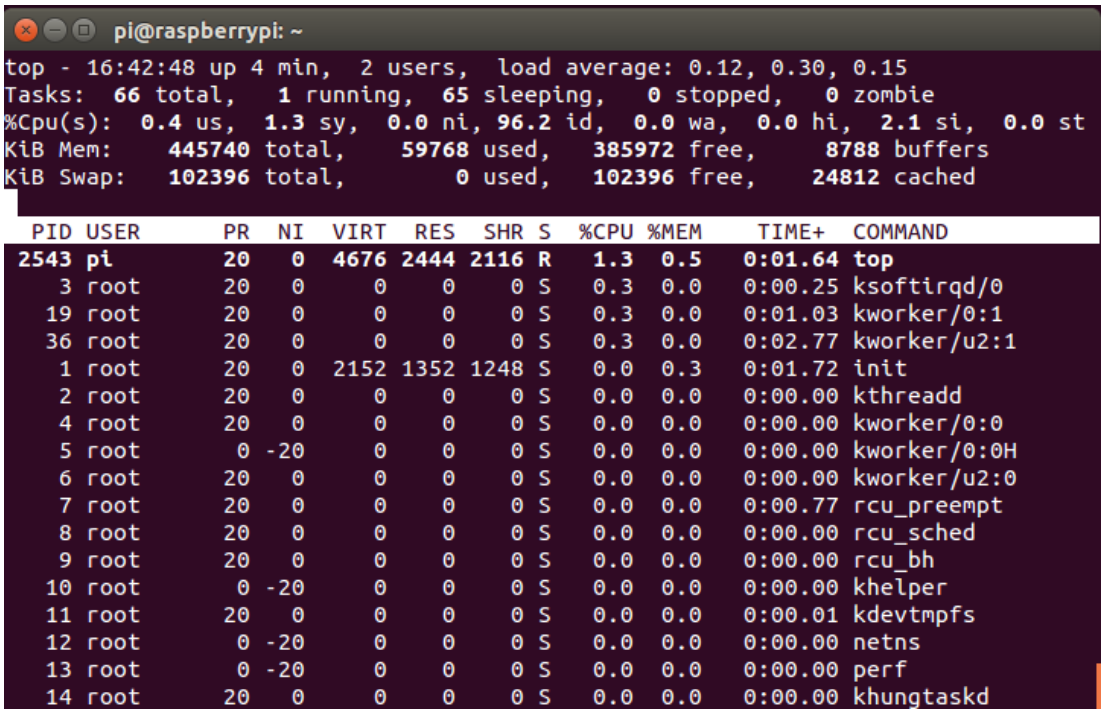



**Figura 44.** Procesamiento CPU Raspberry Pi B+

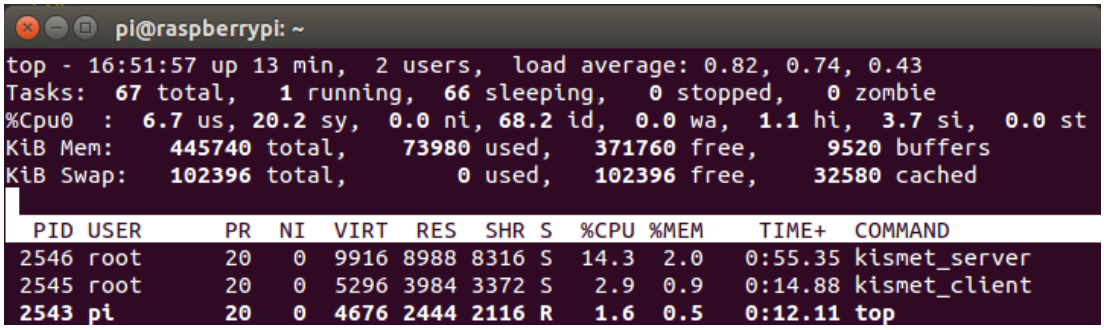
La pantalla que se muestra tiene un número de diferentes campos; en la primera línea se puede observar el tiempo de actividad y carga media del sistema, donde se muestra la hora, el tiempo que lleva encendida la máquina; número de usuarios; carga media por segundo en intervalos del último minuto, últimos 10 y 15 minutos respectivamente. La segunda línea muestra el total de tareas y procesos, los cuales pueden estar en diferentes estados. También se verifica el %CPU, el cual muestra el uso de la CPU por usuario (us), kernel (sy), tiempo de CPU en procesos inactivos (id), etc, [47].

Por debajo de la cabecera de la información se visualiza una tabla que muestra los procesos actuales que se ejecutan en la Raspberry Pi. La información incluye su identificación, el usuario que se inició por, su actual uso de la CPU y uso de memoria RAM, junto con la cantidad de tiempo de procesador se ha consumido. Aquí se podrá ver el proceso o aplicación y garantizar su funcionamiento.

En muchos casos se tiene conflictos con la información otorgada de %CPU y *load average*. Los parámetros de %CPU y *load average* son dos valores completamente diferentes, por lo cual es fundamental tener claro ambos temas; básicamente, *load average* es la media ponderada de los procesos en la cola de ejecución de más de 1, 5 y 15 minutos; es decir estos números representan el número medio de procesos del sistema que durante los últimos 1, 5 y 15 minutos han estado esperando por algún recurso del sistema (CPU, acceso a disco, red, etc.). En general, se desea que este número sea inferior al número de CPU(s)/núcleos que tiene; en términos de porcentaje de utilización, 1.0 representa el 100% de un solo núcleo de la CPU. Algo más de 1,0 representa la cantidad de procesos que están esperando en la cola para ser ejecutado. Cuanto menor es el valor mejor; números altos pueden representan un problema de sobrecarga de la máquina.

Se determina que un valor máximo promedio de carga de utilización de 70% es saludable. Una vez que estés constantemente por encima del 70%, se necesita comenzar a determinar la raíz del problema, a planificar la expansión o bien optimizar el software. Eso significa 0.70 por núcleo de CPU. Por otro lado %CPU es exactamente eso, el porcentaje de la CPU que está siendo utilizado por el proceso.

En nuestro caso una vez ejecutado *Kismet* durante 15 minutos, se observa el continuo incremento de valores en el parámetro *load average* de 1 y 5 minutos, sobrepasando el valor de 0,7 recomendable.



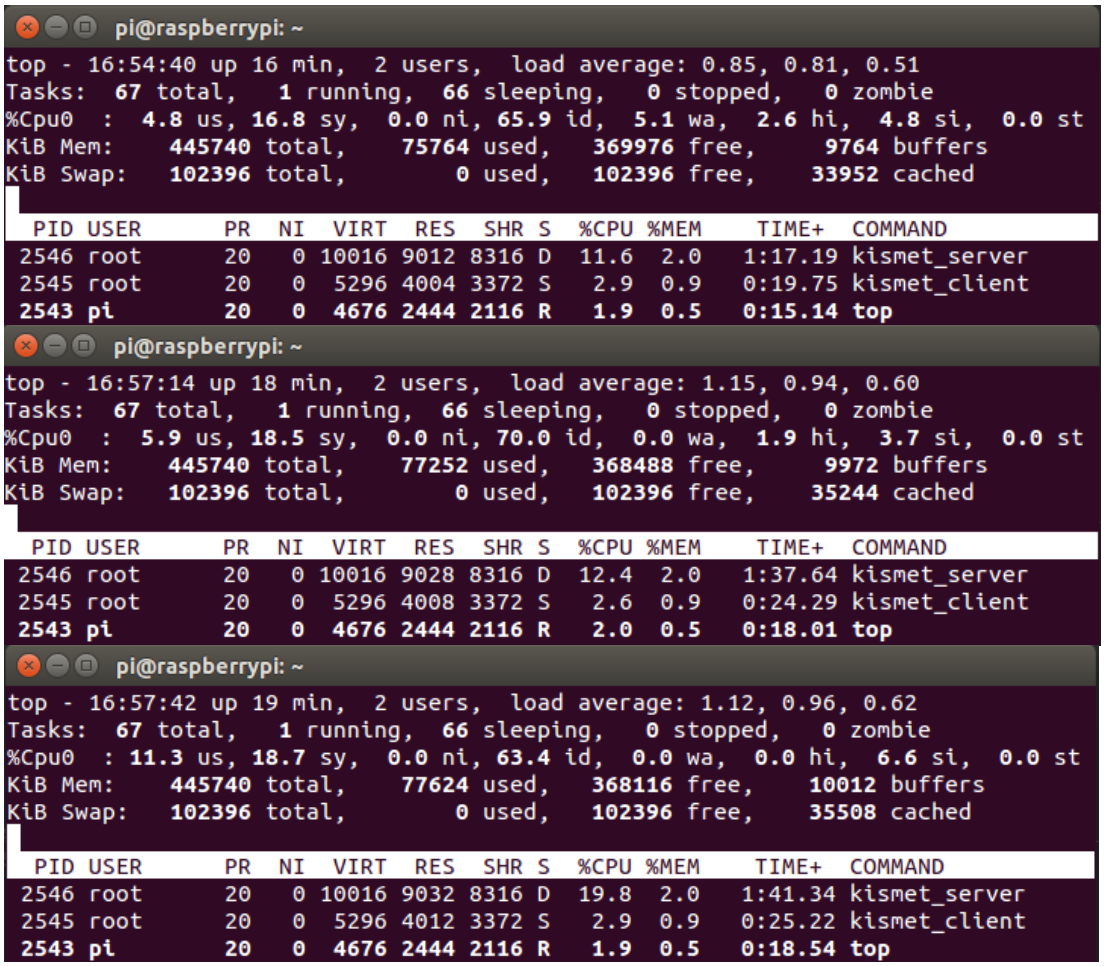



**Figura 45.** Load Average Raspberry Pi B+ durante 15 minutos

Para entender lo que *load average* significa en realidad, se tiene en nuestro caso un sistema de un solo CPU, los números nos dicen que:

En el último 1 minuto: El ordenador estaba sobrecargado en un 12% en promedio. En promedio, 0.12 procesos estaban esperando por la CPU. (1.12)
En los últimos 5 minutos: La CPU inactivo durante 4% del tiempo. (0.96)
Durante los últimos 15 minutos: El ordenador estaba sobrecargado por 38% en promedio. En promedio, 0.38 procesos estaban esperando por la CPU. (0.62).

En todo el conjunto de las pruebas realizadas, en la figura 45 se puede verificar el %CPU que está siendo utilizado por el proceso *Kismet* un valor singularmente alto como un porcentaje de una sola CPU como es nuestro caso para *Raspberry Pi B+*.

Para nuestro primer caso de prueba se verifica que el inconveniente recae en el sobre procesamiento del CPU.

Para validar esta información, se ha logrado la adquisición de la nueva tarjeta Raspberry Pi 2 modelo B, en el cual se ha instalado el mismo sistema operativo y versión de Kismet usada con el primer equipo, se busca validar el primer resultado ya que la nueva tarjeta tiene varias CPU (para nuestro caso 4).

- Escenario 2: La segunda prueba a realizar es utilizando la tarjeta Raspberry Pi 2 modelo B, en el mismo entorno de red; se determina el procesamiento y uso de CPU antes, durante y al finalizar la ejecución de Kismet; del archivo generado por la herramienta con el nombre Kismet-20150514-10-01-29-1.pcapdump (7.23Mb) se obtiene también una serie de paquetes malformados:

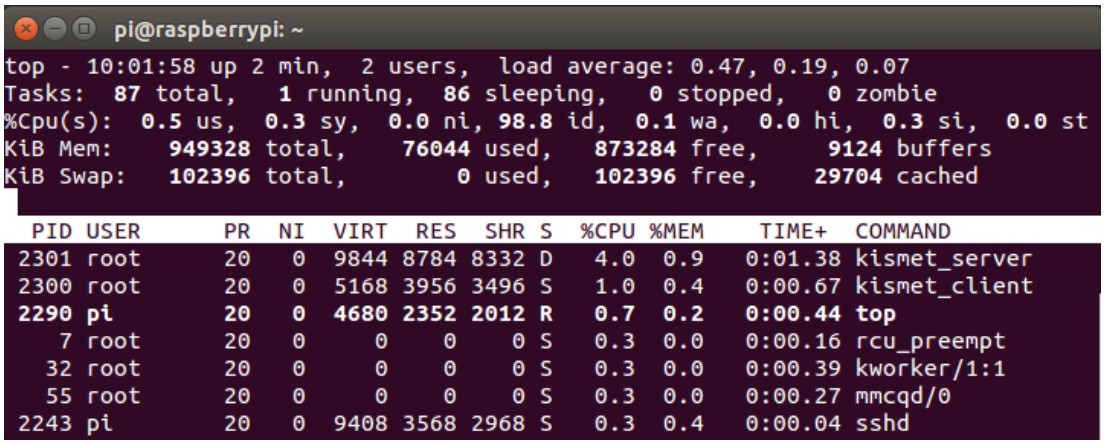
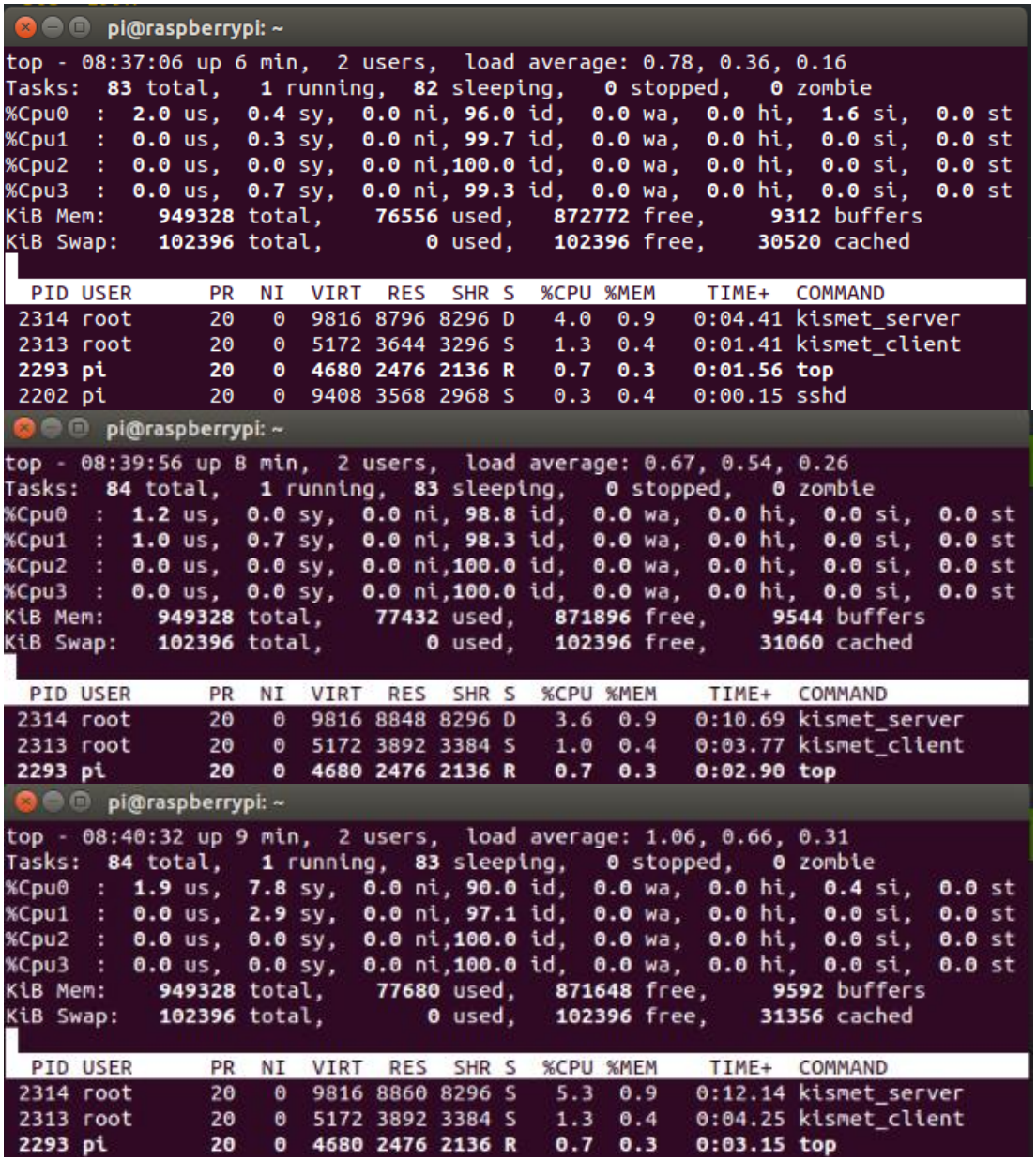



**Figura 46.** Procesamiento CPU Raspberry Pi 2

Es importante tener en cuenta que en un sistema con varias CPU o una CPU multi-core, los números de carga media funcionan diferentes; por ejemplo, si tiene un promedio de carga de 2 en un sistema de un solo CPU, esto significa que su sistema estaba sobrecargado por el 100% de todo el período de tiempo, un proceso estaba usando la CPU mientras otro proceso estaba esperando. En un sistema con 2 CPU, esto sería el uso completo dos procesos diferentes utilizaban dos CPU diferentes todo el tiempo. En los sistemas multi-núcleo, puede tener porcentajes mayores que 100%.

Por ejemplo, si 3 núcleos están en uso 60%, superior mostrará un uso de CPU de 180%.

En la siguiente figura se verifica un incremento no muy elevado de los valores de *load average* para lo cual en este caso se descarta que el proceso de malformación de paquetes obtenidos sea por sobre procesamiento de la CPU.



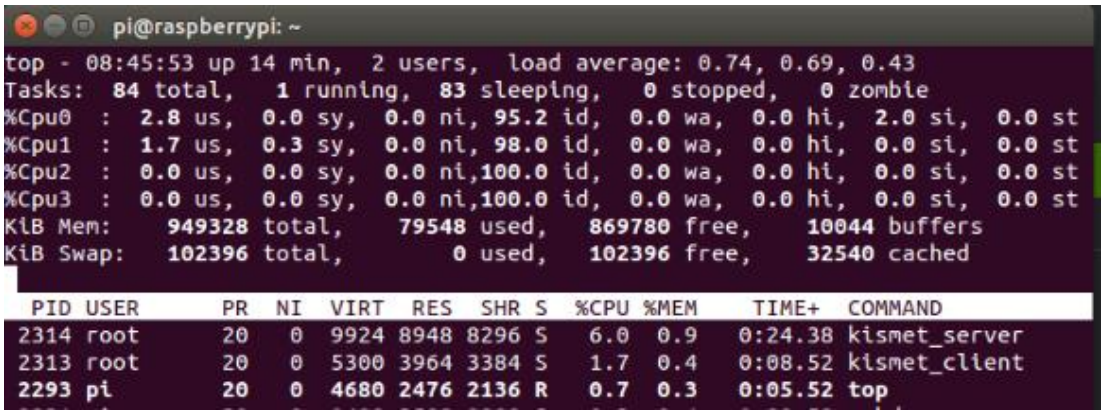



**Figura 47.** Load Average Raspberry Pi 2

En este caso al descartar que el problema de la aparición de paquetes malformados sea el procesamiento y uso del CPU de la tarjeta, se presenta una nueva hipótesis la cual recae en la incompatibilidad del módulo usb wifi Tp-Link. Para esto se realiza una tercera instancia de pruebas mediante el uso de un ordenador con sistema operativo Linux en el cual se instala Kismet y se utiliza el mismo módulo inalámbrico.

- Escenario 3: En las pruebas realizadas con el computador usando el módulo usb wifi sobre el mismo ambiente de trabajo, del archivo generado por la herramienta con el nombre Kismet-20150514-08-18-57-1.pcapdump (12.3Mb) se obtiene los siguientes resultados:

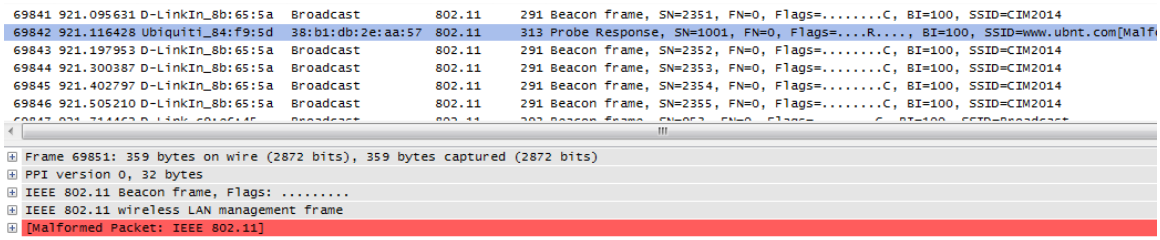



**Figura 48.** Archivo .pcapdump generado mediante Linux-Pc y atheros

Se verifican paquetes malformados en la trama IEEE 802.11, dentro de los cuales algunos se detallan como paquetes Data, se descarta este error ya que

simbolizan ser paquetes encriptados, se presentan las tramas de gestión (*beacon*, *probe request*, etc), como paquetes malformados.

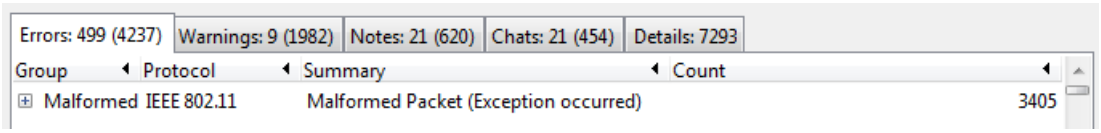



**Figura 49.** Malformed Packets - Linux-Pc y Atheros

- Escenario 4: Debido a las pruebas realizadas con las otras tarjetas *Raspberry Pi B+* y *Pi 2 modelo B*, se tiene como hipótesis que el módulo usb inalámbrico Atheros es el causante de los resultados de tramas malformadas, por lo cual se adquiere un nuevo dispositivo usb inalámbrico de marca Alfa con chipset Ralink (RT3070) sobre la minicomputadora *Raspberry Pi B+* y dentro del mismo entorno de red; del cual se obtiene el archivo generado por la herramienta con el nombre Kismet-20150514-10-29-01-1.pcapdump (10.3Mb), los siguientes resultados:

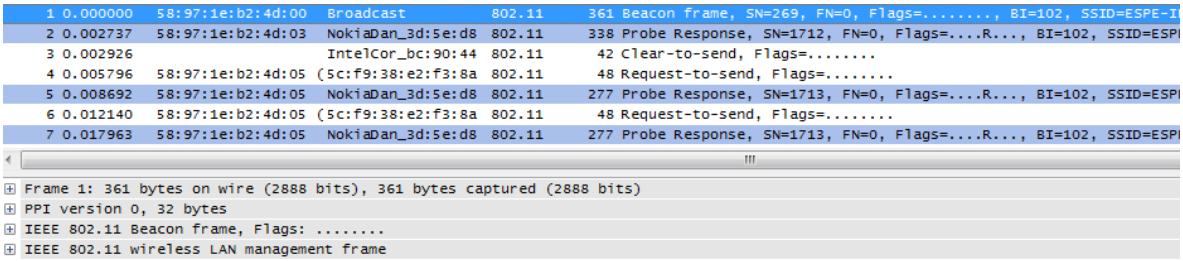



**Figura 50.** Archivo .pcapdump - Raspberry Pi B+ y usb wifi Alfa

En las Tablas 8 y 9, se tiene un resumen del procesamiento del CPU de las tarjetas *Raspberry Pi B+* y *Raspberry Pi 2 modelo B* además de los cuatro escenarios de pruebas realizadas con el software *Kismet* para el sistema de análisis de tráfico de redes 802.11.

**Tabla 8.**

*Load average* Raspberry Pi B+ y Raspberry Pi 2 modelo B

| | Tiempo de Captura (min) | Load average | | | Tiempo de Captura (min) | Load average | |
|---|---|---|---|---|---|---|---|
| | | 1 | 5 | | | 1 | 5 |
| **Raspberry Pi B+ y USB inalámbrico Atheros (TP-LINK TL-WN722N)** | 4 | 0.12 | 0.30 | **Raspberry Pi 2 modelo B y USB inalámbrico Atheros (TP-LINK TL-WN722N)** | 4 | 0.90 | 0.48 |
| | 6 | 0.66 | 0.40 | | 6 | 0.78 | 0.36 |
| | 12 | 1.05 | 0.75 | | 12 | 0.65 | 0.68 |
| | 15 | 0.79 | 0.77 | | 15 | 0.50 | 0.65 |
| | 16 | 0.85 | 0.81 | | 16 | 0.74 | 0.70 |
| | 17 | 1.05 | 0.89 | | 17 | 0.37 | 0.65 |
| | 18 | 1.15 | 0.94 | | 18 | 0.25 | 0.59 |
| | 20 | 0.90 | 0.95 | | 20 | 0.04 | 0.42 |

**Tabla 9.**

Resultados de los cuatro escenarios de prueba

| | TIEMPO DE CAPTURA (min) | TOTAL DE PAQUETES | PAQUETES MALFORMADOS | % ERROR |
|---|---|---|---|---|
| **Raspberry Pi B+ y USB inalámbrico Atheros (TP-LINK TL-WN722N)** | 15 | 49219 | 11976 | 24.33 |
| **Raspberry Pi 2 modelo B y USB inalámbrico Atheros (TP-LINK TL-WN722N)** | 15 | 32494 | 7906 | 24.33 |
| **Pc-Linux y USB inalámbrico Atheros (TP-LINK TL-WN722N)** | 15 | 69851 | 3405 | 4,87 |
| **Raspberry Pi B+ y módulo USB inalámbrico Alfa (AWUS036NH)** | 15 | 55941 | 0 | 0 |

Para el análisis de la trama 802.11, se toma el escenario cuatro ya que se tiene un total de 55941 paquetes capturados durante 15 minutos y no se tiene ningún paquete de la trama 802.11 con error.

## 4.3 ANÁLISIS DE DATOS

### 4.3.1 Análisis de resultados emitidos por Kismet

Una vez ejecutado el software *Kismet*, en la pantalla principal se muestran todas las redes que se van localizando.

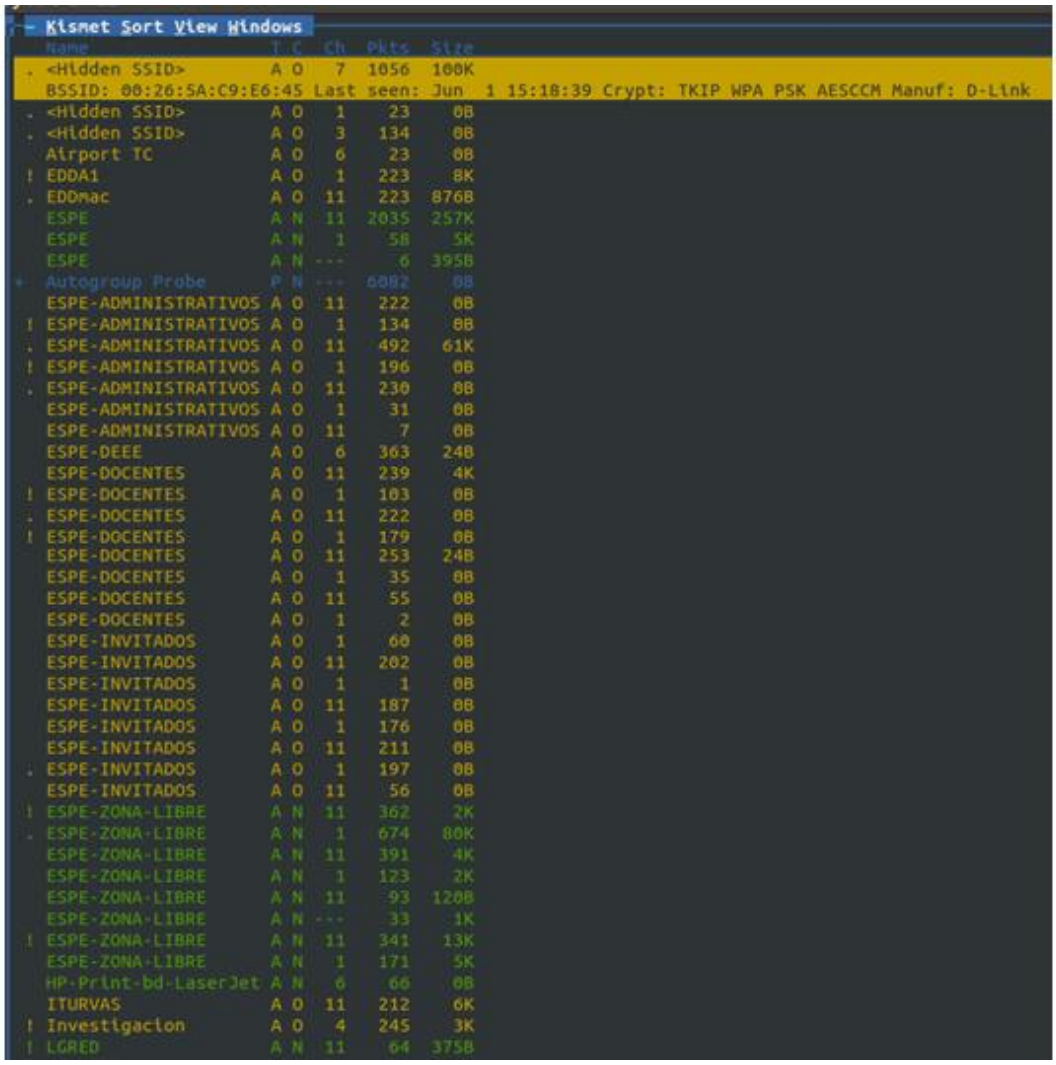



**Figura 51.** Redes detectadas mediante Kismet

Como resultado del análisis se tiene 54 redes detectadas después de un muestreo de 15 minutos, canales 1-3-4-5-6-8-10-11 ocupados. Las redes que aparecen en amarillo tienen activada la seguridad WPA, el código de color rojo es la firma de una red que utiliza su configuración por defecto o de fábrica y las redes en verde no poseen ningún tipo de cifrado, mientras que la red en azul (*Autogroup Probe*) está utilizando encubrimiento SSID o no están transmitiendo el SSID.

En los canales 1, 3 y 7 se tiene otra red que no difunde su SSID también con actividad pero sin interferencia entre los canales 1 y 7. En principio se visualiza que no hay canales libres de solapamiento. Esto se puede verificar observando como

Kismet representa los niveles de energía para cada canal mediante la opción del Menú en *Windows* → *Channel Details*.

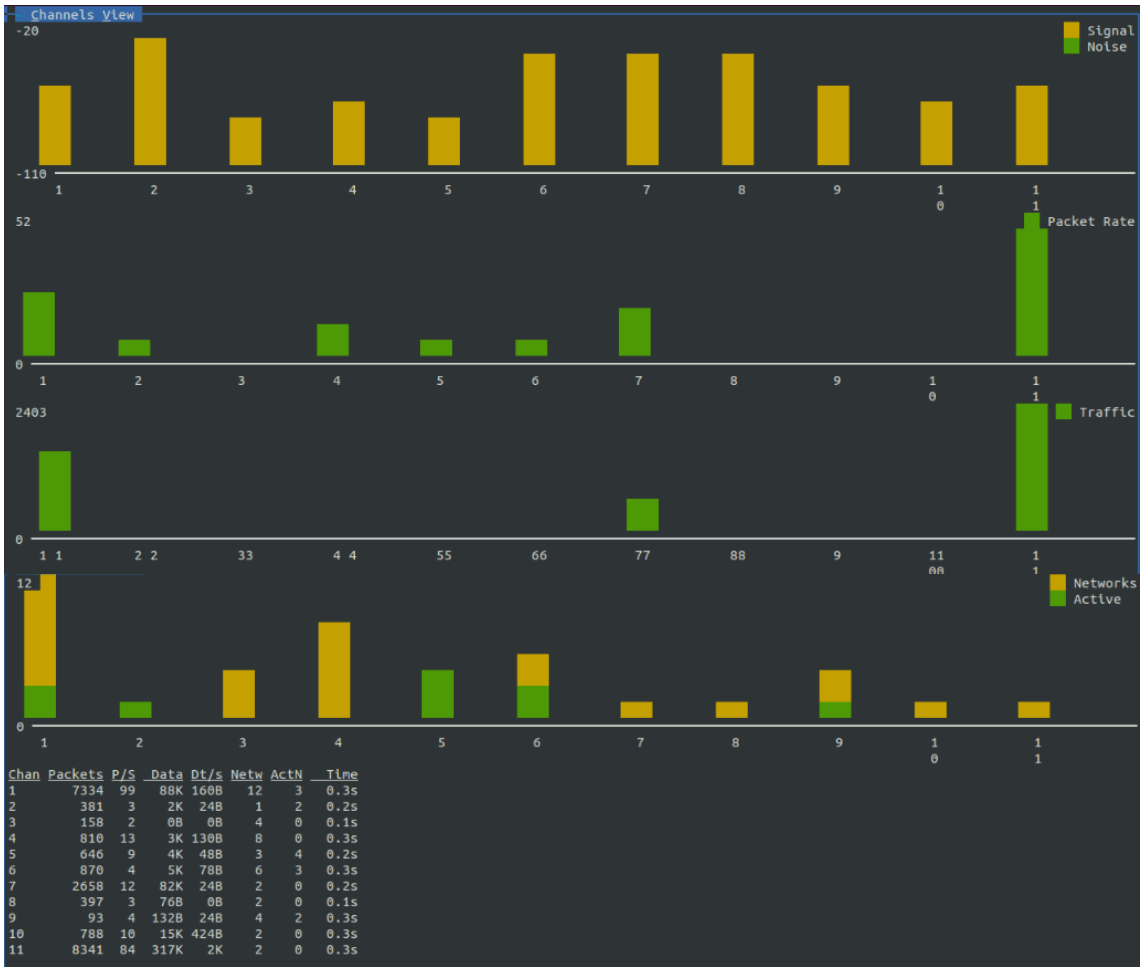



**Figura 52.** Menu Channel Details

Según la Figura 52, se puede configurar un nuevo AP en el canal 3 o 5. Porque aunque se detectan AP's es estos canales su nivel de señal es tan bajo que no constituye una interferencia. Donde se ve mucho peligro es en el canal 6, 7 y 8, se trata de un AP muy cercano, probablemente en la pared contigua de un AP vecino. Esto se sabe por la entidad de la relación señal ruido y el número de canales afectados 6-7-8-9 (4 x 5MHz = 20MHz, ancho de banda de una canal: 22 MHz).

Cuando se agrupa las redes por SSID, se puede seleccionar una red específica y se tiene acceso a otra ventana en la cual se muestra la más completa y detallada información recopilada acerca de la red seleccionada.

Parte de la información interesante que aparece en la pantalla Detalles de la red incluye: SSID, BSSID, número de clientes conectados, MAC address, Channel, Manufacturer of access point (based on MAC address), signal, tipo de encriptación, entre otras.

En la figura 53, se muestra los detalles de un cliente inalámbrico en una red de Infraestructura ESPE-DEEE, el cual indica la dirección MAC (*Basic Service Set Identifier - BSSID*) del AP 00:21:29:A0:3F:80, se identifica el tipo de encriptación de esta red como el cifrado WPA TKIP PSK, etc.

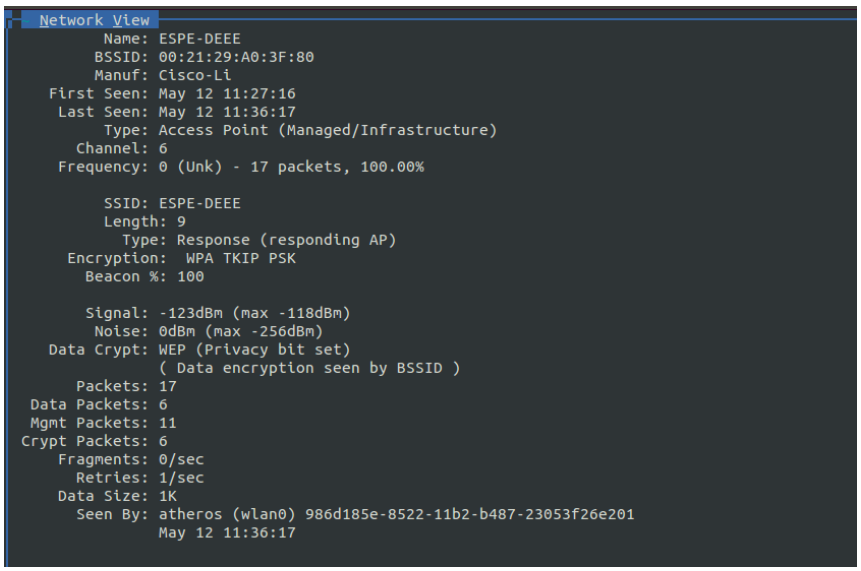



**Figura 53.** Network Details ESPE-DEEE

Es posible que se desee saber qué clientes están conectados a una red. Al poner de relieve el AP y pulsando la tecla *Enter*, se presentará en una nueva ventana una lista de los clientes asociados con la red. La figura 54 proporciona un ejemplo del

listado de los clientes conectados a un AP específico, en nuestro caso a la red ESPE-ZONA-LIBRE.

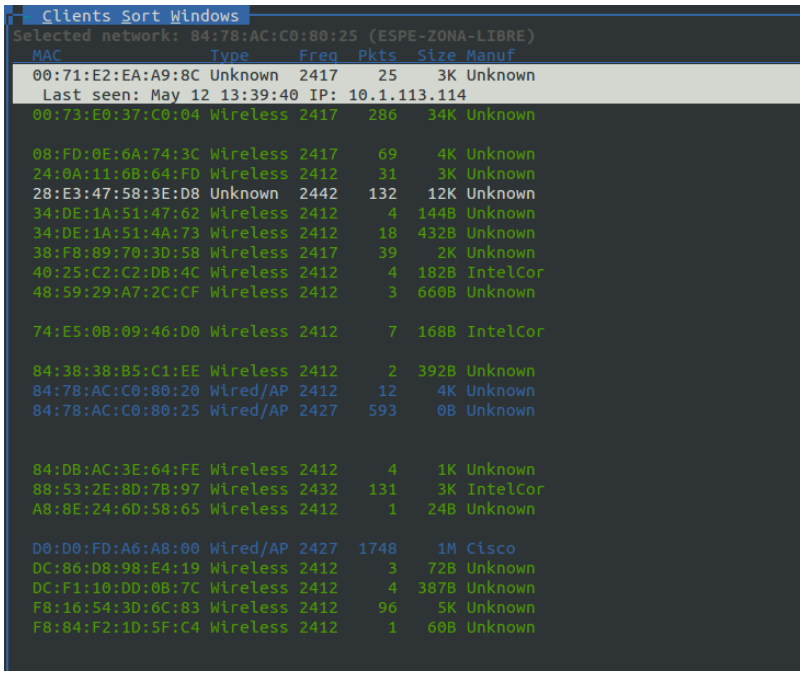



**Figura 54.** Client List - Network: ESPE-ZONA-LIBRE

Cuando un sistema de posicionamiento global apoyado (GPS) se utiliza junto con Kismet, los datos GPS aplicables se mostrarán a lo largo del borde inferior del panel de lista de la red (ver Figura 55).


**Figura 55.** GPS Status Information

Como es típico de coordenadas sin etiquetas norte / sur / este / oeste, latitudes positivos indican norte, mientras que las latitudes negativos indican sur. Del mismo modo, las longitudes positivas indican el hemisferio oriental, mientras que las longitudes negativas indican la occidental. En la Figura 55, nuestras coordenadas son al sur del ecuador, y en el hemisferio occidental (Valle de los Chillos para ser más

precisos). También se incluye una medida de la altitud, velocidad, rumbo, y la calidad de arreglo [18].

En el menú *Windows*, dentro de la opción *GPS Details* se determina la cantidad de satélites junto a la calidad de señal de cada uno. De esta manera se comprueba que Kismet está procesando de manera correcta la información GPS enviada por el módulo GPS USB BU-353S4:

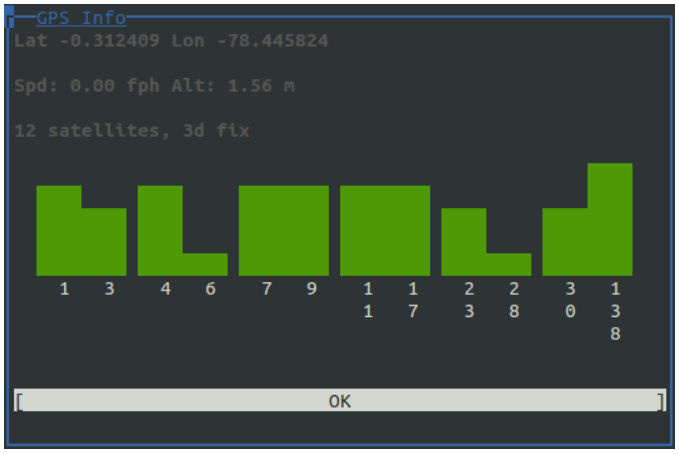



**Figura 56.** Menú GPS Details

Otra importante característica de *Kismet* es tratar de geo-localizar la red. La exactitud de esta información es totalmente dependiente de los datos de localización GPS.

*Kismet* no puede conocer la ubicación de una red, sólo puede conocer el lugar en el que vio una señal para determinar donde la señal es más fuerte. Encerrando en un círculo el lugar sospechoso, mantiene promedios de funcionamiento de la ubicación de la red; hace esto sobre la ejecución del software; por lo tanto, es ventajoso para obtener datos de la muestra a partir de una variedad de ubicaciones y obtener una mejor conjetura [48].

Necesita al menos 3 satélites a la vista para obtener una posición válida. También puede tomar algunos minutos para conseguir una posición válida. Además

se tiene que estar afuera, GPS no funciona dentro de la casa o edificio. Los árboles, casas u otras barreras pueden impedir su receptor GPS de conseguir una posición válida [48].

Para *Kismet* utilizar los datos del GPS, debe tener una forma de recogerla, *Kismet* utiliza el programa *gpsd* para leer los datos de este hardware. Para trazar las ubicaciones de red, se debe utilizar el archivo GPSXML.

Otra opción dentro del menú *Windows,* es la ventana *Alerts* con la cual estas alertas pueden informar al administrador de red gran poder para la determinación de si su red está bajo ataque, o si los problemas son de alguna otra fuente. Mientras que una cierta cantidad y tipos de alertas son normales, otras cantidades excesivas pueden indicar problemas o ataques.

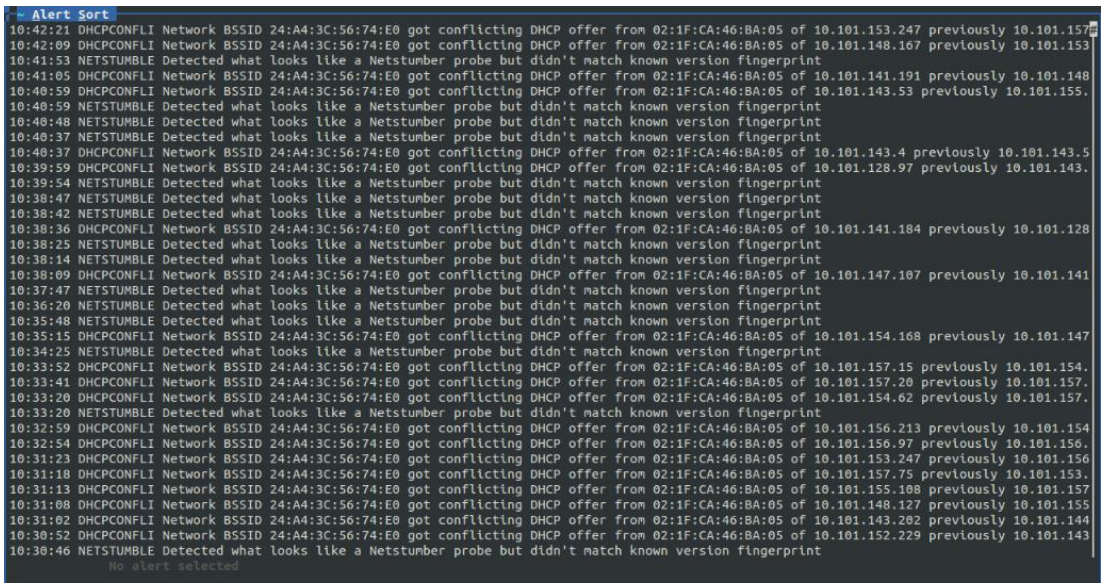



**Figura 57.** Menú Alerts

Adicional se generó un archivo .alert con un total de 43 alertas, las cuales corresponden al SSID ESPE, correspondiente al BSSID 24:A4:3C:56:74:E0 como se indica en la Tabla 10.

**Tabla 10.**

Alertas generadas por Kismet

| Día | Hora | Año | Descripción de la alerta |
|---|---|---|---|
| **Thu May 14** | **10:29:49** | **2015** | NETSTUMBLER 0 24:A4:3C:56:74:E0 8C:BF:A6:AA:3B:4F 01:60:1D:00:01:00 00:00:00:00:00:00 Detected what looks like a Netstumber probe but didn't match known version fingerprint |
| **Thu May 14** | **10:29:49** | **2015** | DHCPCONFLICT 0 24:A4:3C:56:74:E0 02:1F:CA:46:BA:05 FF:FF:FF:FF:FF:FF 00:00:00:00:00:00 Network BSSID 24:A4:3C:56:74:E0 got conflicting DHCP offer from 02:1F:CA:46:BA:05 of 10.101.154.210 previously 10.101.148.127 |
| **Thu May 14** | **10:30:01** | **2015** | DHCPCONFLICT 0 24:A4:3C:56:74:E0 02:1F:CA:46:BA:05 FF:FF:FF:FF:FF:FF 00:00:00:00:00:00 Network BSSID 24:A4:3C:56:74:E0 got conflicting DHCP offer from 02:1F:CA:46:BA:05 of 10.101.148.127 previously 10.101.153.247 |
| **Thu May 14** | **10:30:18** | **2015** | DHCPCONFLICT 0 24:A4:3C:56:74:E0 02:1F:CA:46:BA:05 FF:FF:FF:FF:FF:FF 00:00:00:00:00:00 Network BSSID 24:A4:3C:56:74:E0 got conflicting DHCP offer from 02:1F:CA:46:BA:05 of 10.101.146.118 previously 10.101.143.57 |
| **Thu May 14** | **10:30:24** | **2015** | DHCPCONFLICT 0 24:A4:3C:56:74:E0 02:1F:CA:46:BA:05 FF:FF:FF:FF:FF:FF 00:00:00:00:00:00 Network BSSID 24:A4:3C:56:74:E0 got conflicting DHCP offer from 02:1F:CA:46:BA:05 of 10.101.143.57 previously 10.101.152.229 |
| **Thu May 14** | **10:30:46** | **2015** | NETSTUMBLER 0 24:A4:3C:56:74:E0 90:8D:6C:BA:1F:34 01:60:1D:00:01:00 00:00:00:00:00:00 Detected what looks like a Netstumber probe but didn't match known version fingerprint |

Las alertas que se encuentran en el archivo *kismet.conf,* poseen dos parámetros que son su máximo número de detecciones por unidad de tiempo y cuántas alertas permite en un mínimo de tiempo. A continuación se muestran los ataques que fueron detectados en la Tabla 10 [49]:

**Tabla 11.**

Alertas Kismet según WVE (Vulnerabilidades y Exploits de las Redes Inalámbricas)

| Nombre | Descripción | Tipo de análisis |
|---|---|---|
| ***DHCPCONFLICT*** | Clientes que reciben dirección IP por DHCP y usan otra, indicio de spoofing. | Anomalía |
| ***NETSTUMBLER*** | Detección de Netstumbler | Firma |

La mejor forma de analizar los datos que ha recogido *Kismet* es leer directamente los ficheros de registro donde se guarda la información de las redes inalámbricas.

Del archivo generado por la herramienta con el nombre Kismet-20150514-10-29-01-1.nettxt (809 Kb) se obtiene los siguientes resultados:

```
Network 53: BSSID 58:97:1E:22:1F:72
 Manuf      : Unknown
 First      : Thu May 14 10:29:08 2015
 Last       : Thu May 14 10:43:45 2015
 Type       : infrastructure
 BSSID      : 58:97:1E:22:1F:72
   SSID 1
    Type       : Beacon
    SSID       : "ESPE-DOCENTES"
    Info       : LAB_ELECATOM_2D
    First      : Thu May 14 10:29:08 2015
    Last       : Thu May 14 10:43:45 2015
    Max Rate   : 54.0
    Beacon     : 10
    Packets    : 65
    Encryption : WPA+PSK
    Encryption : WPA+TKIP
    Encryption : WPA+AES-CCM
 Channel    : 1
 Frequency  : 2412 - 95 packets, 98.96%
 Frequency  : 2417 - 1 packets, 1.04%
 Max Seen   : 6000
 Carrier    : IEEE 802.11b+
 Encoding   : CCK
 LLC        : 78
 Data       : 18
 Crypt      : 12
 Fragments  : 0
 Retries    : 0
 Total      : 96
 Datasize   : 2385
 Last BSSTS : 701938504765
    Seen By : alfa (wlan0mon) 09497498-fa24-11e4-b187-8e04841ee201
96 packets
```

**Figura 58.** Archivo .nettxt

Un informe de *Kismet .nettxt* de la Figura 58 ofrece una lista detallada de todos los puntos de acceso inalámbricos y todos sus equipos cliente inalámbricos asociados. Cada punto de acceso inalámbrico de la lista se identifica con un ***"Network Number"*** que se asigna arbitrariamente por la aplicación de software *Kismet*; en este archivo se incluirá SSID encontrados, fabricante del punto de acceso, longitud y latitud, donde se descubrió la red, e incluso los clientes conectados a ella.

Para mayor explicación, se describe la red Network 53 donde se determina ***SSID (Service Set Identifier)*** como *"ESPE-DOCENTES"*, mientras el ***BSSID (Basic Service Set Identifier***) identificado con la dirección MAC *58:97:1E:22:1F:72* correspondiente a un equipo *CISCO*, un valor ***Max Rate*** de 54.0 MB como velocidad máxima soportada en la línea (después de la atenuación); la red posee tipo de encriptación ***WPA (WIFI Protected Access)***, además indica ser una red en modo

"*infrastructure*" (red tipo cliente-servidor, donde los clientes son los ordenadores personales que se conectan al servidor, llamado AP); dentro del total de los 14 canales definidos para el uso de Wifi 802.11 para la banda ISM de 2,4 GHz, la red se encuentra en el canal 1, que se centra en 2412 MHz.

Por último, hay una lista de equipos cliente que están conectados de forma inalámbrica al punto de acceso inalámbrico. Para cada punto de acceso inalámbrico, uno de los clientes en un informe de texto es siempre el propio punto de acceso.

Como se ve en la figura siguiente, se muestran para la Network 53 cinco clientes:

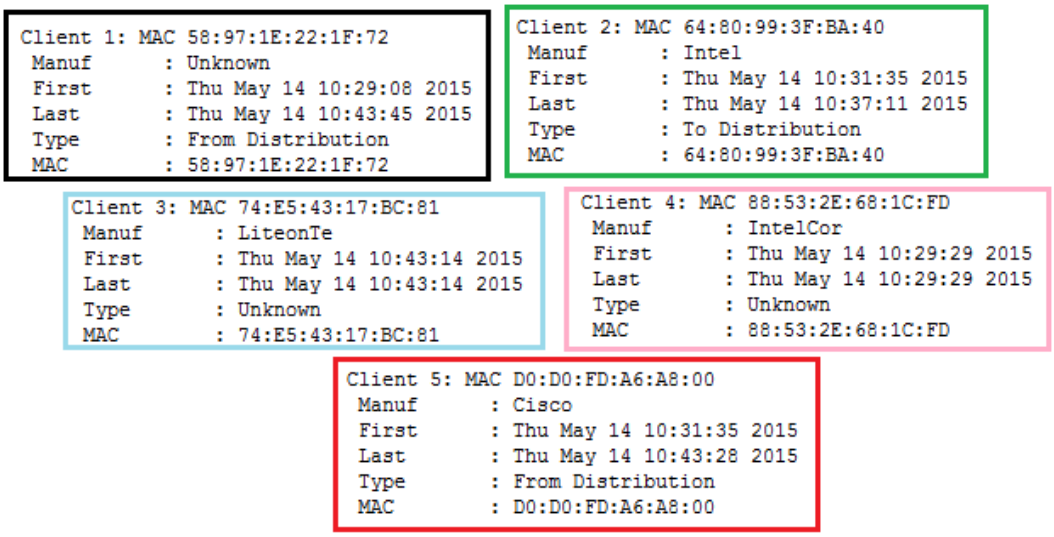



**Figura 59.** Archivo .nettxt - Network 53 Clients

### 4.3.2 Análisis de resultados emitidos por archivo .pcapdump en Wireshark

El estándar 802.11 define una serie paquetes que son usados por los nodos y los AP para establecer la comunicación entre ellos y mantener el link entre ellos. Cada trama tiene un campo de control que define la versión del protocolo 802.11, el tipo de trama y algunos indicadores más. Cada trama tiene también la dirección MAC del origen y del destino, el número de secuencia de la trama y una secuencia de redundancia para detección de errores.

Las tramas de administración o gestión permiten a los nodos establecer y mantener la comunicación entre ellos.

Lo primero que se debe buscar es si los puntos de acceso están enviando tramas *Beacon*. En la siguiente captura de pantalla, se puede ver estas tramas:

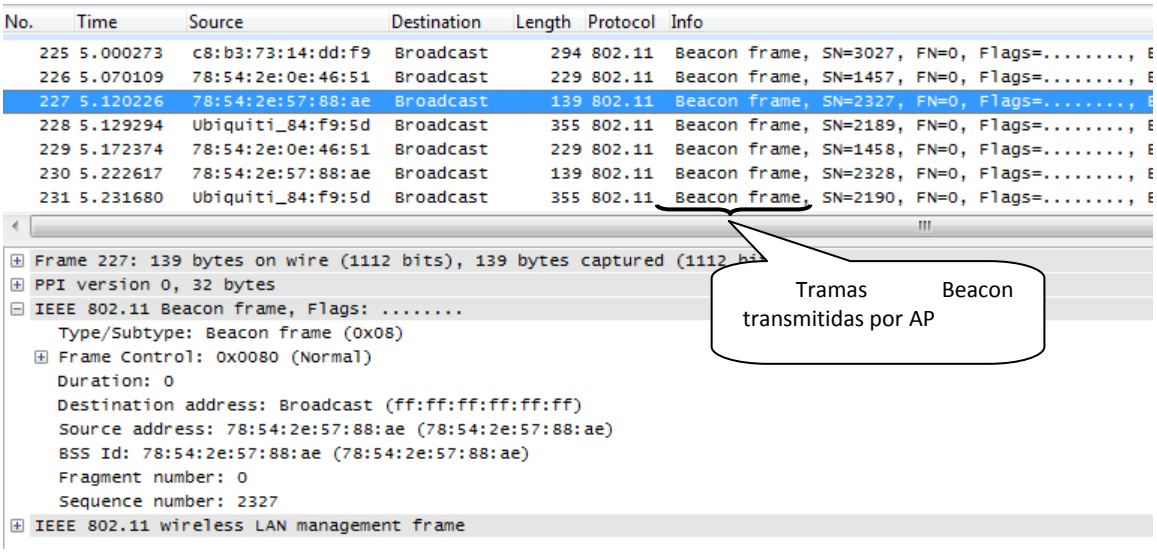



**Figura 60.** Beacon Frames - Wireshark

Antes de empezar la secuencia de transmisión, todas las estaciones que compiten por el medio inalámbrico escuchan una trama *Beacon*. En la figura 61 se presenta la información contenida en esta trama, la cual comienza indicando el número de trama (1), la longitud de la trama capturada (361 bytes), continuando se tiene el campo "*PPI versión 0*" de 32 bytes de longitud, para indicar el canal en que el AP se encuentra operando (2412 MHz), así como el nivel de señal (-37dBm), el nivel de ruido (0dBm) y la velocidad a la que la trama se transmite para este caso es de 1Mbps.

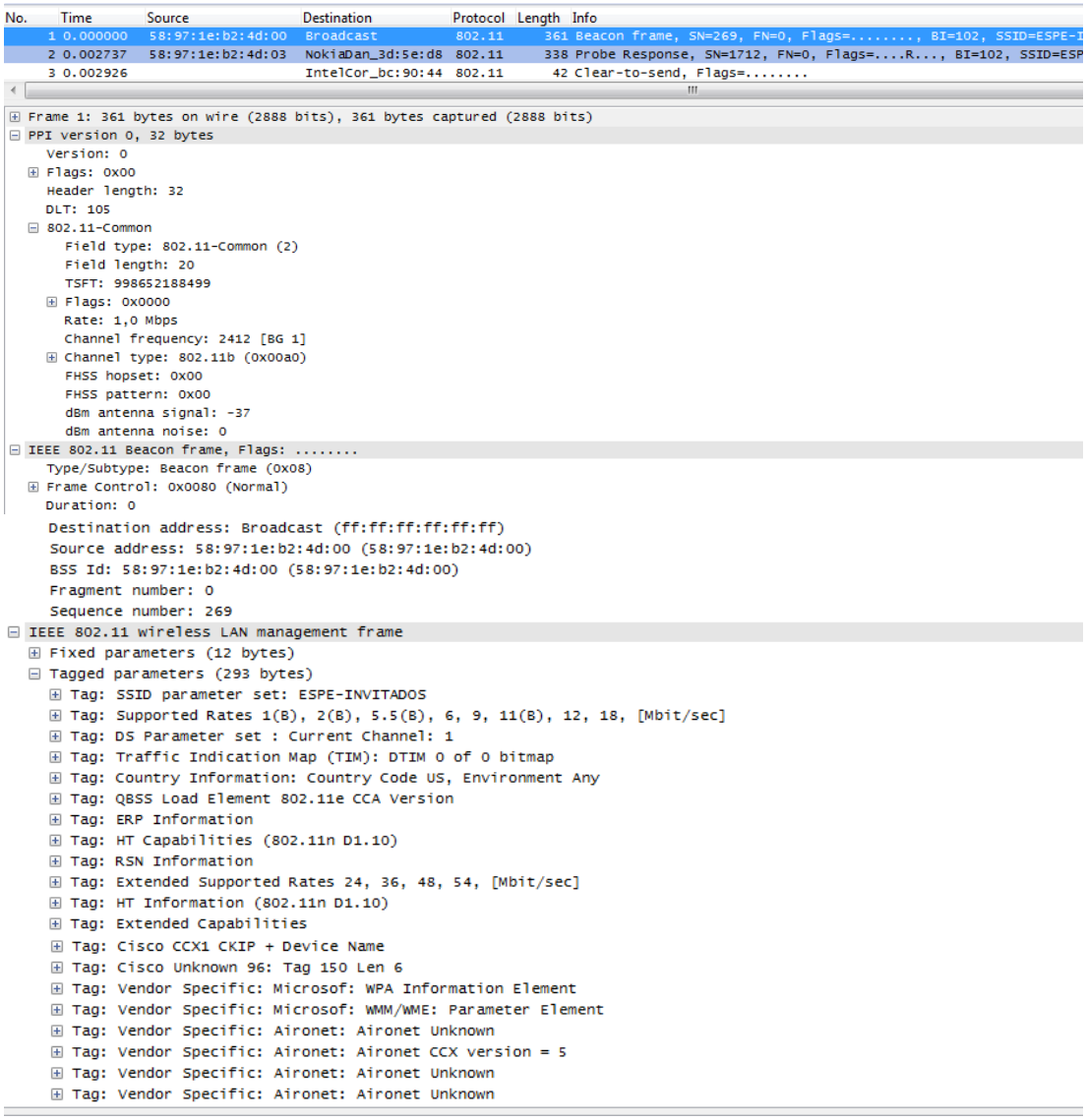



**Figura 61.** Detalle trama Beacon

Continuando con la figura 61 se tiene el campo "*IEEE 802.11 Beacon frame Flags*:" en el cual se indica los campos: control de trama (*frame control*), duración, dirección destino (ff:ff:ff:ff:ff:ff), dirección origen (58:97:1e:b2:4d:00), número de secuencia, numero de fragmentos y el FCS.

A continuación se tiene el campo "*IEEE 802.11 Wireless LAN Management Frame*" el cual está constituido por el subcampo "*Fixed parameters*" de 12 bytes de longitud presenta información del intervalo *Beacon*. Siguiendo, se tiene el campo "*Tagged Parameters*" de 293 bytes de longitud, en este se presenta información del

SSID en "*SSID Parameter Set*" (ESPE-INVITADOS), además se tienen las velocidades soportadas teniendo las de 24, 36, 48 y 54 MBps, seguido del cual se tiene el valor del TIM (*Traffic Indication Map*).

El campo "*HT Capabilities* (802.11n D1.10)" está formado por los siguientes subcampos: el subcampo "*HT Capabilities Info*" se tiene la información para indicar las características opcionales que el AP soporta, indicando de esta manera que el AP no soporta modo de ahorro de energía por multiplexado especial (SM), intervalos de guarda cortos para 40MHz, y la longitud máxima soportada para A-MSDU es de 7935 bytes.

El subcampo "*A-MPDU Parameters*" indica la máxima longitud de A-MPDU es de 65535 bytes, en el subcampo "*Rx Supported modulation and Coding Scheme Set*" se indica que la MCS del transmisor y receptor se establecen de manera similar.

En el subcampo "*HT extended capabilities*", se indica que no se soporta PCO, continuando se tiene el subcampo "*Transmit Beam Forming (TxBF) Capabilities*" el cual indica que no soporta *Beamforming*, de la misma manera el subcampo "*Antenna Selection (ASEL) Capabilities*" indica que no soporta ninguna técnica de selección de antena.

El campo "*HT information* (802.11n D1.10)" contiene información del ancho de banda del canal, si se trabaja con 40MHz indica cual es el canal secundario, además indica que no se opera con RIFS, permite operar PSMP, e informa si se encuentran presentes estaciones que no tienen el formato *Greenfield*, Por último se tiene información específica sobre el fabricante del AP.

Como era de esperarse esta trama está formada de varios campos y subcampos, los cuales son usados para informar a las estaciones vecinas de las características de operación de este AP (58:97:1e:b2:4d:00).

Continuando con el análisis, una estación envía una trama *probe requests* para descubrir redes 802.11 dentro de su alcance. Este es el cliente en busca del AP. Se observa que el destino MAC es todo "ff" que es una dirección de difusión. Además, que el SSID en el paquete también se establece para transmitir. La trama *probe request* se envía en cada canal que el cliente soporta en un intento de encontrar todos los AP. Hasta que el cliente determine qué AP asociar mediante varios factores como velocidad de datos y carga de punto de acceso para seleccionar el AP óptimo que se mueve a la fase de autenticación de la red 802.11 después de conseguir respuestas de AP como *Probe Response*.

En el paquete *Probe Request* se verifica al cliente (IntelCord_68:1c:fd) en busca del AP. Como vemos en la figura 62 el destino MAC y BSSID es todo "ff:ff:ff:ff:ff:ff" lo cual significa que es una dirección de *broadcast*. Este es debido a que el marco seleccionado es un paquete *Probe Request*, que el cliente utiliza como mecanismo para descubrir redes en el área.

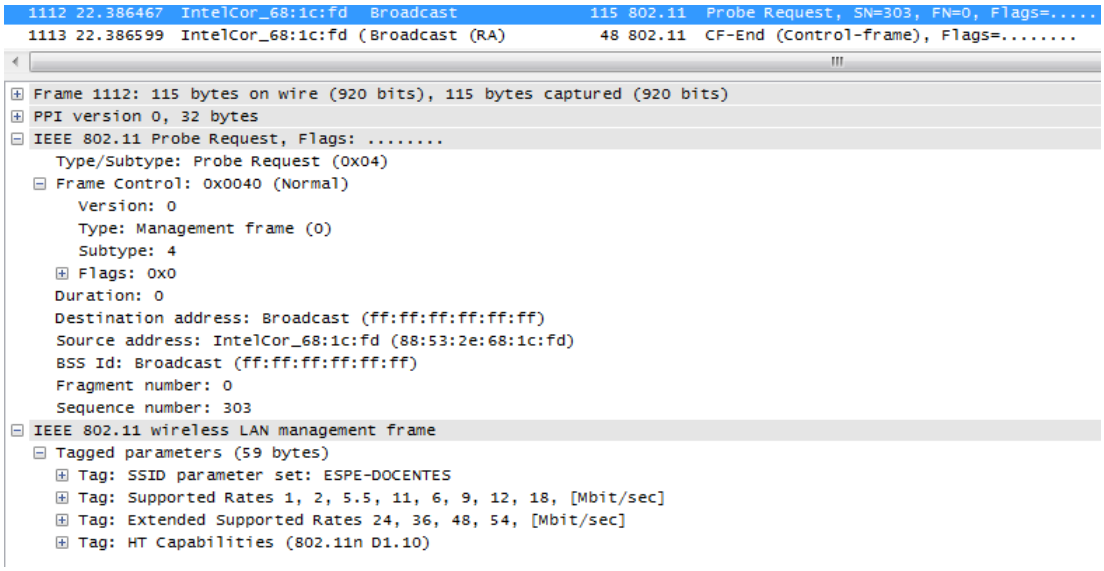



**Figura 62.** Detalle trama Probe Request

Entre la información que se puede contener del paquete (ver Figura 62), se tiene el número de trama (1112), la longitud de la trama capturada (115 bytes), continuando el campo "*PPI versión 0*" de 32 bytes de longitud, donde se verifica el canal en que el AP se encuentra operando (2412 MHz), el nivel de señal (-75dBm), el nivel de ruido (0dBm) y la velocidad a la que la trama se transmite es de 1Mbps.

Continuando, se tiene el campo "*IEEE 802.11 Probe Request Flags*:" en el cual se indica los siguientes campos: control de trama, duración, dirección destino (ff:ff:ff:ff:ff:ff), dirección origen la cual muestra la dirección MAC de nuestro equipo cliente (88:53:2e:68:1c:fd), número de secuencia, numero de fragmentos, etc.

A continuación se tiene el campo "*IEEE 802.11 Wireless LAN Management Frame*" el cual está constituido por el subcampo "*Tagged parameters*" de 59 bytes de longitud, en este se presenta información del SSID en "*SSID Parameter Set*" (ESPE-DOCENTES), dentro de la opción Supported Rates se ven algunas de las velocidades de datos y los tipos de datos extendidos soportados. La WLAN es capaz

de soportar tanto los clientes 802.11b y 802.11g. En la tasa de datos de 1, 2, 5.5, 11, 6, 9, 12 y 18Mbs.

El campo "*HT Capabilities (802.11n D1.10*)" está formado por los siguientes subcampos: el subcampo "HT Capabilities Info" se tiene la información para indica las características opcionales que el AP soporta, indicando de esta manera que el AP soporta modo de ahorro de energía (0x0001) por multiplexado especial (SM), intervalos de guarda cortos para 20MHz, y que la longitud máxima soportada para A-MSDU es de 7935 bytes.

El subcampo "*A-MPDU Parameters*" indica la máxima longitud de A-MPDU es de 65535 bytes, en el subcampo "*Rx Supported modulation and Coding Scheme Set*" se indica que la MCS del transmisor y receptor se establecen de manera similar.

En el subcampo "*HT extended capabilities*", se indica que no se soporta PCO, continuando se tiene el subcampo "*Transmit Beam Forming (TxBF) Capabilities*" el cual indica que no soporta *Beamforming*, de la misma manera el subcampo "*Antenna Selection (ASEL) Capabilities*" indica que no soporta ninguna técnica de selección de antena.

Los AP reciben la trama *Probe Request* para ver si la estación tiene al menos una velocidad de datos soportada en común. Si tienen velocidades de datos compatibles, se envía una trama de respuesta *Probe Response* anunciando el SSID (nombre de red inalámbrica), velocidades de datos soportadas, tipos de cifrado si es necesario, y otras capacidades 802,11 del AP.

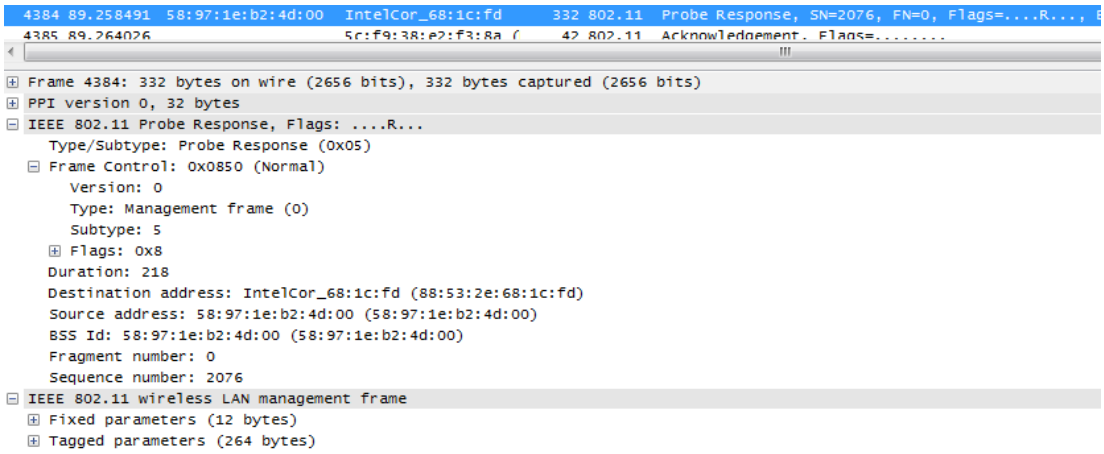



**Figura 63.** Detalle trama Probe Response

Se puede observar en la Figura 63, como este paquete *Probe Response* es una respuesta a la solicitud del sondeo *(probe request*). Donde AP con criterios coincidentes responden al cliente con una trama de respuesta que contiene: una fuente MAC del BSSID como es 58:97:1e:b2:4d:00 la identificación del AP y un destino MAC del cliente (IntelCord_68:1c:fd), información de sincronización, etc.

Continuando, se presenta otro paquete cuando el cliente decide qué AP es el mejor para el acceso y envía una solicitud de autenticación, presentándose en la secuencia 0x0001 (ver Figura 64).

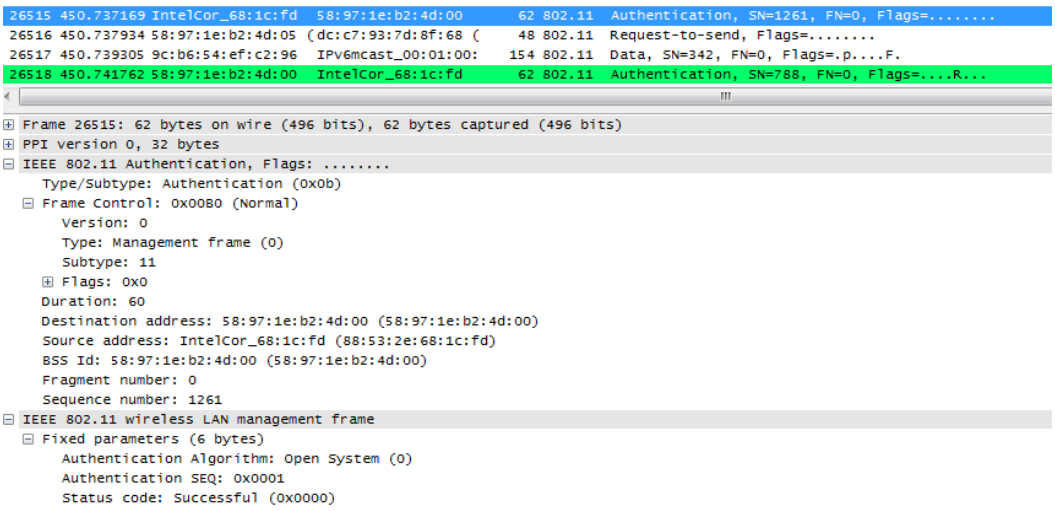



**Figura 64.** Detalle trama Authentication Request

El AP recibe la trama de autenticación y responde a la estación móvil con el conjunto de marco de autenticación para abrir indicando una secuencia de 0x0002. Si un AP recibe cualquier trama que no sea una autenticación o sonda de solicitud desde una estación que no está autenticada responderá con una trama *deauthentication* colocando la estación en un estado no asociado no autenticado. La estación tendrá que comenzar el proceso de asociación de la etapa de bajo nivel de autenticación. En este punto la estación móvil está autenticado, pero todavía no asociado.

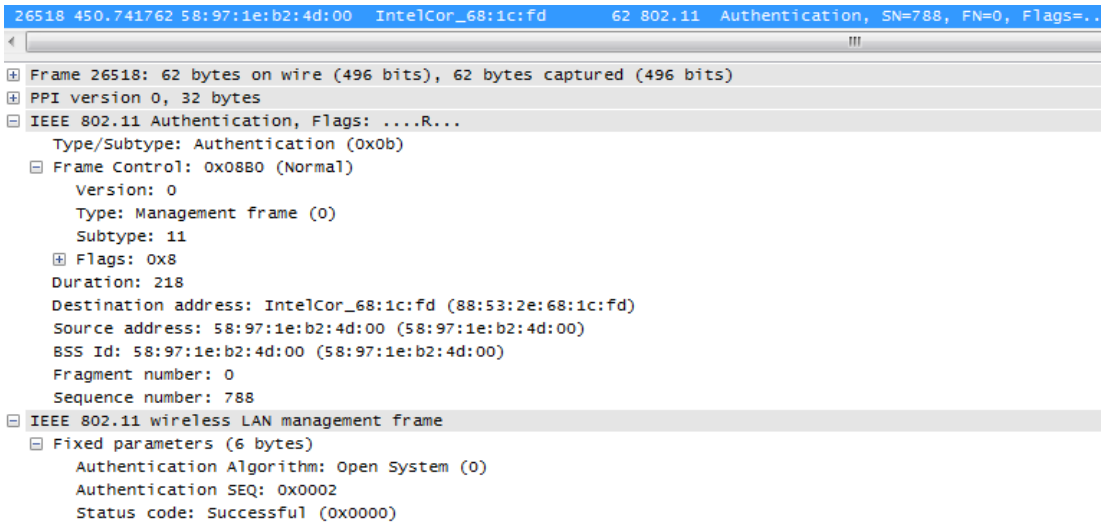



**Figura 65.** Detalle trama Authentication Response

Una vez que una estación determina con cual AP le gustaría asociarse, envía una solicitud de asociación (*association request*) al AP. La solicitud de asociación contiene tipos de cifrado si es necesario y otros capacidades compatibles 802.11. Si un AP recibe una trama de una estación que está autenticado, pero aún no asociado, responderá con un marco de disociación colocando al cliente en un estado autenticado pero no asociado (Figura 66).

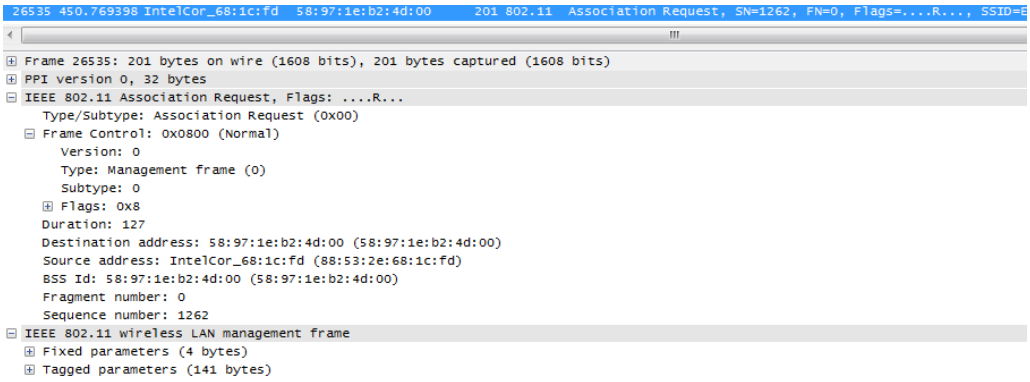



**Figura 66.** Detalle trama Association Request

Si los elementos de la solicitud de asociación coinciden con los de los capacidad del AP, el AP creará un ID de Asociación para la estación móvil en nuestro caso es 0x001d (ver Figura 67) y responde con una respuesta de asociación *(association response)* con la concesión de un mensaje de éxito de acceso de red y de acceso a la estación móvil.

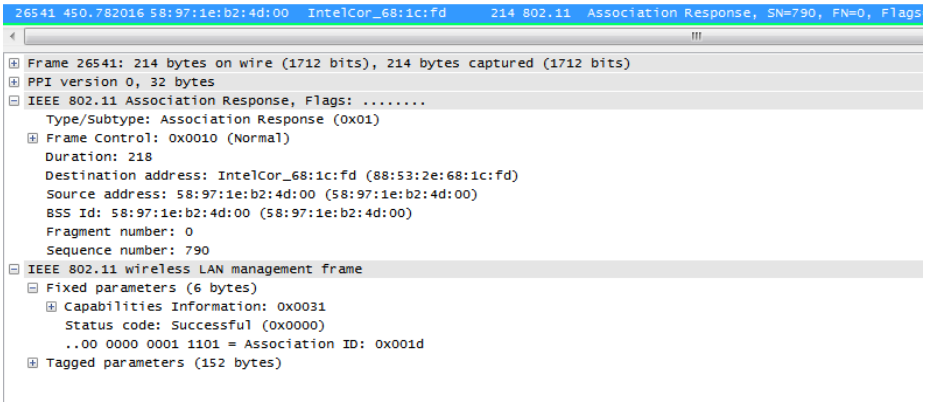



**Figura 67.** Detalle trama Association Request

En este momento, la estación móvil está asociada con éxito al AP y puede comenzar con la transferencia de datos.

Mediante la opción *Protocol Hierarchy*, se muestra la jerarquía de protocolo de los paquetes capturados.

| Protocol | % Packets | Packets | % Bytes | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|---|---|---|---|---|---|---|---|---|
| Frame | 100,00 % | 55941 | 100,00 % | 10001413 | 0,087 | 0 | 0 | 0,000 |
| PPI Packet Header | 100,00 % | 55941 | 100,00 % | 10001413 | 0,087 | 0 | 0 | 0,000 |
| IEEE 802.11 wireless LAN | 100,00 % | 55941 | 100,00 % | 10001413 | 0,087 | 27916 | 1355074 | 0,012 |
| IEEE 802.11 wireless LAN management frame | 17,45 % | 9763 | 27,38 % | 2738231 | 0,024 | 9763 | 2738231 | 0,024 |
| Data | 3,88 % | 2171 | 3,40 % | 339656 | 0,003 | 2171 | 339656 | 0,003 |
| Logical-Link Control | 28,54 % | 15968 | 55,60 % | 5560334 | 0,048 | 0 | 0 | 0,000 |
| Text item | 0,22 % | 123 | 0,08 % | 8118 | 0,000 | 0 | 0 | 0,000 |

**Figura 68.** Protocol Hierarchy

Se desglosan todos los protocolos capturados. Como resultado más de un protocolo se contará para cada paquete.

En la Figura 68 se tiene que el paquete *IEEE 802.11 wireless LAN* alcanza el 100% el cual consta *IEEE 802.11 Wireless LAN Management Frame* y *Data* con un 17.45 y 3.88% respectivamente.

### 4.3.3 Análisis de resultados

El estudio realizado se ha llevado a cabo en las instalaciones de la Universidad de las Fuerzas Armadas - ESPE. El total de AP detectados recae en 55 redes y el total de clientes conectados a estos AP se acerca a los 1198.

A continuación se presentan los resultados obtenidos del análisis realizado.

#### 4.3.3.1 Estándares

El resultado de los estándares utilizados por los AP dentro del entorno del Laboratorio de Electrónica se verifica en el siguiente gráfico.

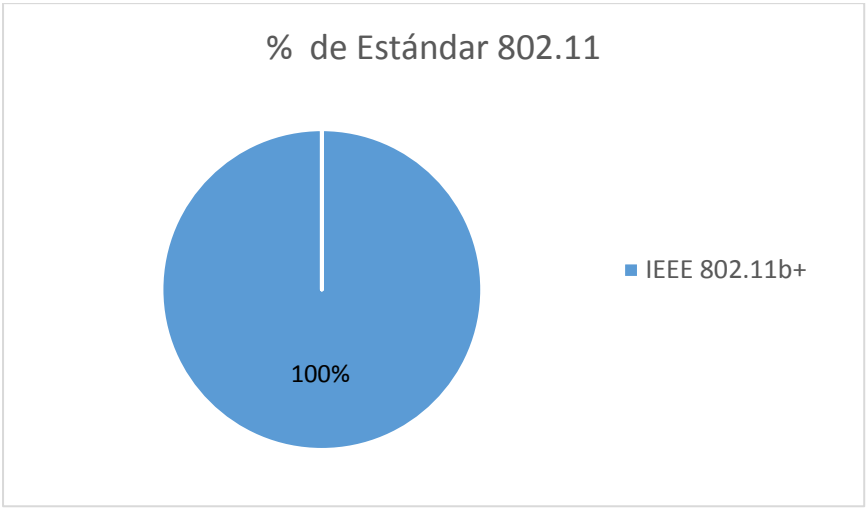



**Figura 69.** Estándares

El total de 100% de los AP detectados trabajan con 802.11b exclusivamente.

En la Figura 70 se muestra las velocidades soportadas por los AP en tanto por ciento, verificándose que el estándar 802.11b está implementado en la infraestructura de la red.

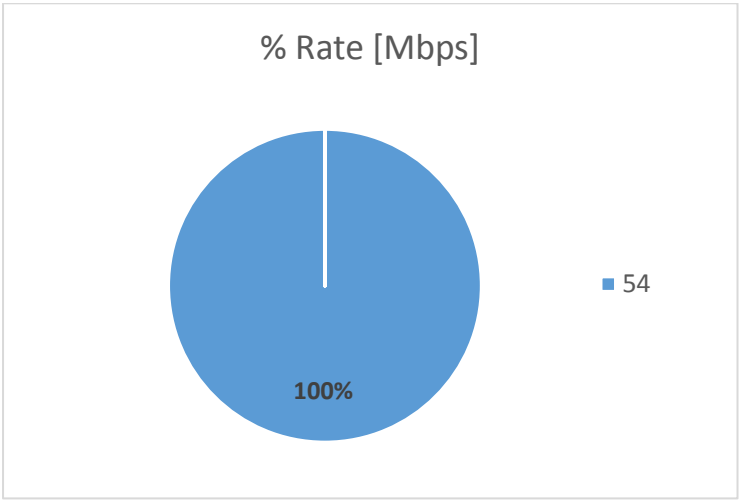



**Figura 70.** Velocidades individuales

#### 4.3.3.2 Canales

Otro parámetro importante de la configuración de los AP son los canales que se fijan para cada red. Para evitar interferencias los AP deberían estar configurados para

trabajar en los canales 1, 6 y 11 con el fin de que no existan solapamientos de frecuencias. En la Figura 71 se puede observar cómo 21 AP de los 55 detectados se encuentran en el canal 1 y 8 de ellos están en el canal 11. El resto de dispositivos están configurados de manera aleatoria sobre el resto de canales, para evitar crear interferencias entre canales.

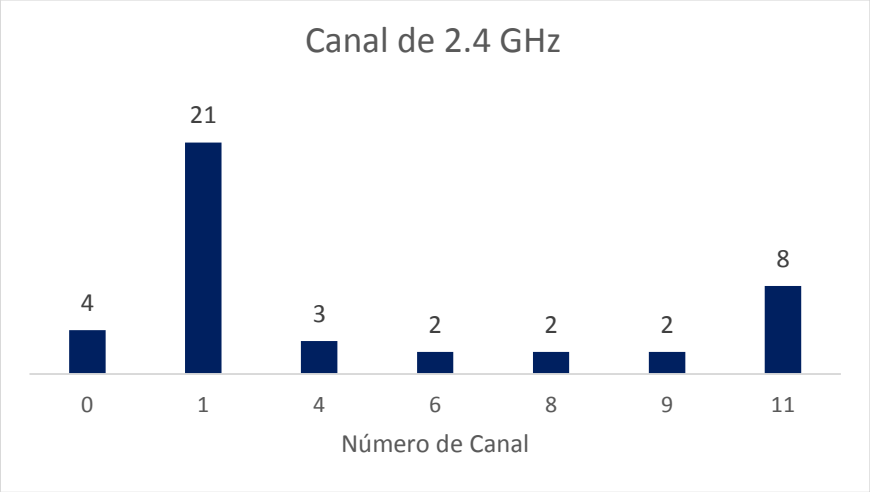



**Figura 71.** Canales 2.4 GHz

Si un AP inalámbrico está unido o parte de un router, todos los dispositivos "de conmutación Ethernet" y cualquier otro dispositivo que están conectados a través de un cable Cat 5/5e/6 al router también se mostrará como un "cliente". En la lista de clientes, el punto inalámbrico y todos los dispositivos que están conectados a él a través de una conexión inalámbrica tendrán un "canal" de 0. Por lo tanto como se verifica en la Figura 71, para cada AP inalámbrico, 4 de los "clientes" dentro del archivo *.nettxt* se verifica que es el mismo AP.

Si un cliente es un cliente inalámbrico real de AP, se muestra un número de canal mayor que cero.

#### 4.3.3.3 Seguridad

En la siguiente Figura, se muestran los distintos mecanismos de encriptación detectados. La mayoría de redes inalámbricas soporta seguridades más robustas como WPA. Un 12% de las WLAN no requieren autenticación siendo AP HotSpot sin encriptación, creadas para ofrecer solamente un servicio de acceso web, dejando las tareas de cifrado para capas superiores (ejemplo navegación HTTPS). Se tiene un pequeño valor de 1% para encriptación WEP, que es un mecanismo de seguridad no fiable.

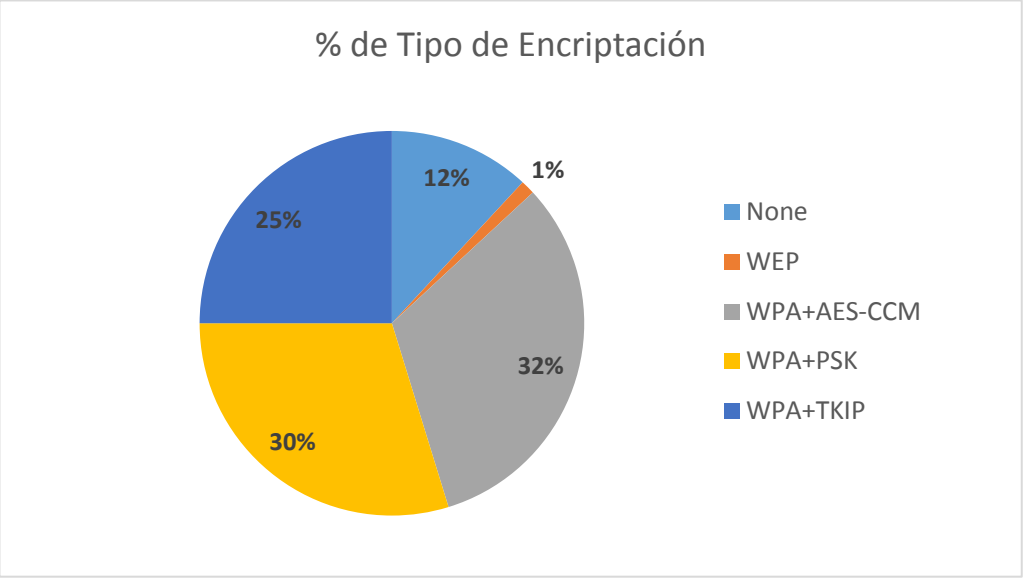



**Figura 72.** Encriptación

#### 4.3.3.4 Modos de Red

En el siguiente gráfico se observa como el modo de red de más del 60% de los AP detectados es probe, la configuración de infraestructura alrededor de 30% típica en la gran mayoría de entornos en los que la finalidad es una conexión compartida a internet a través de un AP, y una red dentro de la configuración Ad-Hoc para la conexión entre dispositivos de forma directa.

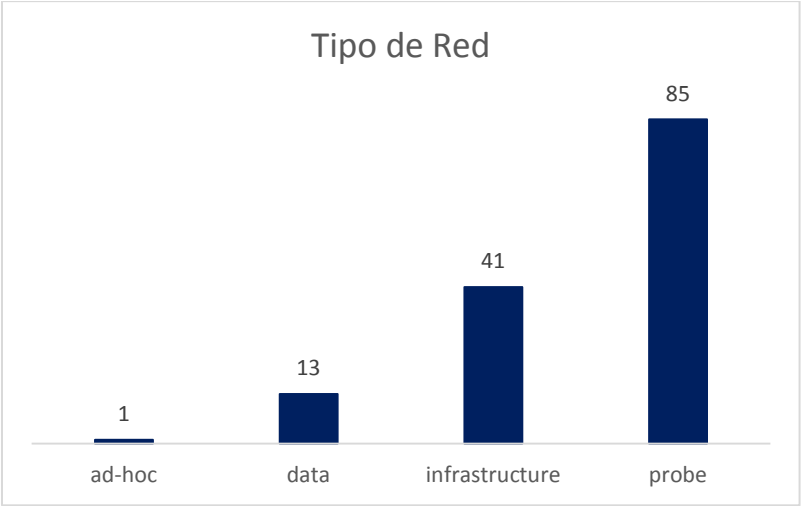



**Figura 73.** Modo operativo de red

Como se define en el Capitulo 2 ítem 2.3.3.1.2.1, el tipo "*probe"*, no es una red ya que *probe* es un cliente que busca (envía *probe request*) para una red y no se ha tenido ninguna respuesta a esas solicitudes, es decir es un cliente que aún no ha sido asociado. Por lo tanto se tiene un total de 55 redes, de las cuales 13 son redes "*data*", *Kismet* no pudo detectar ninguna trama *beacon* o de gestión y por lo tanto aún no pueden decir qué tipo de red es.

#### 4.3.3.5 Fabricantes

Se determina los tipos de fabricantes a nivel comercial en el sector de los AP y clientes de las redes inalámbricas. En el entorno de red estudiado IntelCor y Ubiquiti son los fabricantes con mayores equipos en cuanto a AP, debido a que son de gama más elevada, soportan elevado tráfico y más cantidad de usuarios, por este motivo estos dispositivos se ubican dentro de las características con mayor requerimiento de configuración; también se verifica que existe 70 equipos los cuales no se reconocen el fabricante. En cuanto a clientes, como la gran mayoría son dispositivos como ordenadores portátiles, smartphones, tablets PC, se verifican dispositivos Apple, Inc, LiteonTe detectados y su gran dominio respecto a los demás fabricantes.

Finalmente, en la siguiente gráfica se muestra el ranking de fabricantes de AP y de clientes global.

- IntelCor es el ganador en cuanto a la fabricación de AP seguido de Ubiquiti y HonHaiPr.
- IntelCor es el ganador con diferencia de clientes conectados. Le prosigue la Koreana Samsung Electronics.

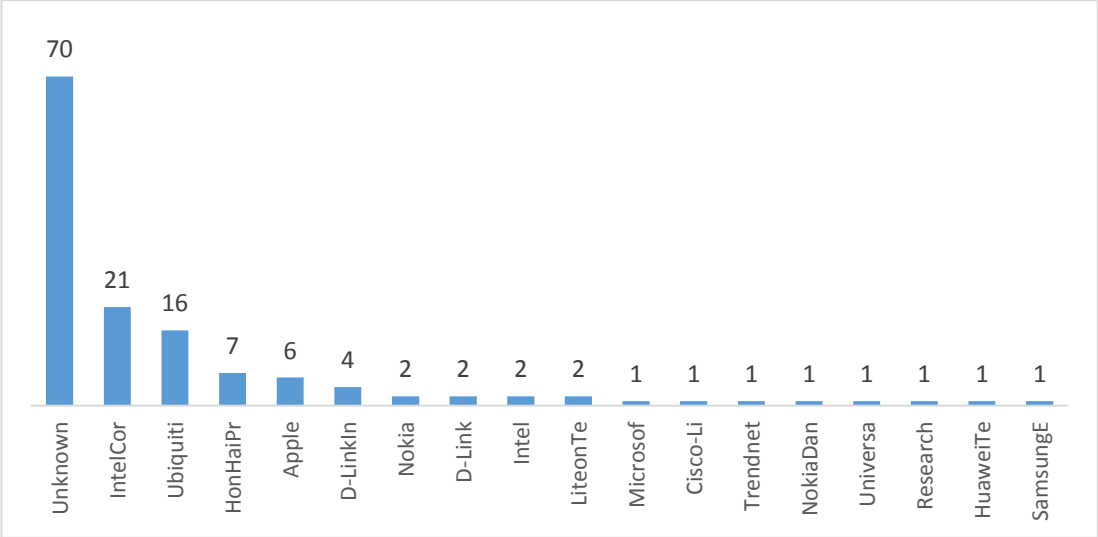



**Figura 74.** Fabricantes AP

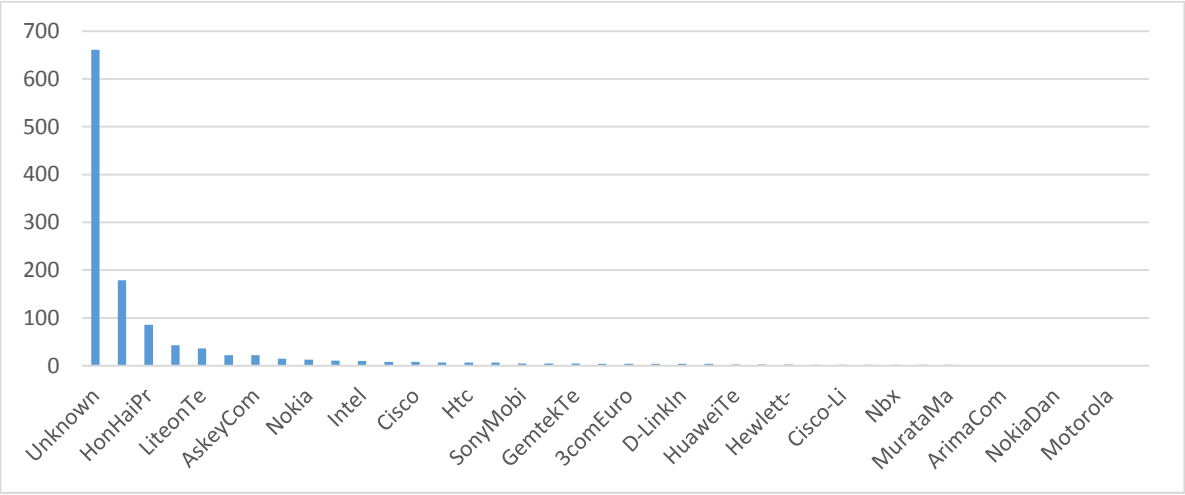



**Figura 75.** Fabricantes de Clientes

#### 4.3.3.6 Porcentaje de tramas de gestión

Las tramas Beacon, Probe Request y Probe Response, explicadas en el ítem 2.6.1.1, son enviadas a tasas de transferencia bajas ya que las tienen que poder recibir todos los dispositivos. Una gran cantidad de transmisiones de estas tramas ocupando el canal puede afectar al rendimiento de este.

La Figura 76 muestra la cantidad de tramas Beacon, Probe Request y Probe Response capturadas. De las pruebas realizadas durante 15 minutos, el total ha sido 55941 tramas capturadas de las cuales se observa que 68 tramas, un 35%, son *Beacon* y los valores tanto de las tramas Probe Request como las Probe Response deberán ser semejantes pero en nuestro estudio no es así ya que se tiene 113 tramas con un 57% y 16 tramas con un 8% respectivamente. Esto repercute seriamente en el rendimiento del canal ya que el medio sólo puede usarse por un equipo a la vez y se reparte a partes iguales entre todos los dispositivos del canal.

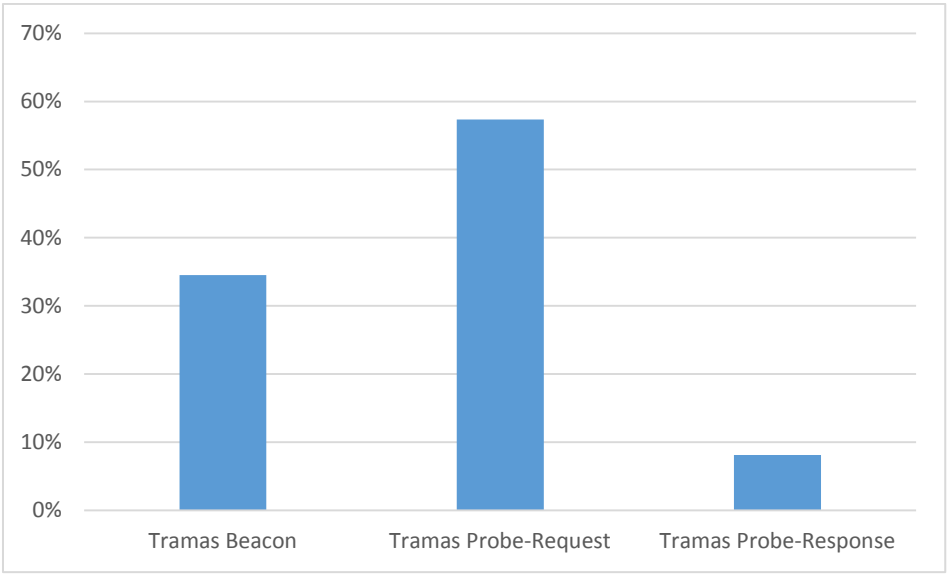



**Figura 76.** Porcentajes cantidad de tramas

#### 4.3.3.7 Porcentaje de AP de acuerdo a la red existente

Dentro del entorno de red analizado se verifica un sin número de redes inalámbricas, y de acuerdo a la infraestructura del campus universitario se puede observar que las redes difieren del equipo y por ende de su BSSID, por lo cual se determina la existencia de varias AP para una SSID especifica.

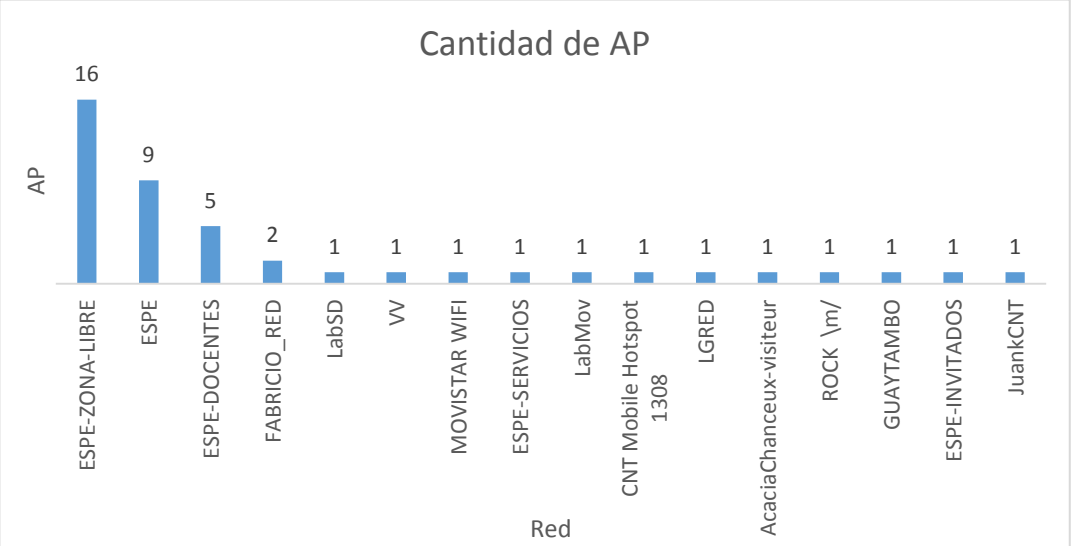



**Figura 77.** Porcentajes cantidad de AP

## 4.4 ANÁLISIS GEOREFERENCIAL DE LOS EQUIPOS ACCESS POINT

Para estimar la ubicación de los equipos AP, se utiliza el archivo de *Kismet* con formato .gpsxml; se lo puede ver en la figura 78. Este archivo en formato xml se lo puede abrir en Excel para utilizarlo como una base de datos, para generar las ubicaciones de latitud, longitud, potencia de recepción en dBm y red, y de esta manera determinar las distancias necesarias en la triangulación de antenas.

Kismet-20150516-09-17-25-1.gpsxml (~/espe_lab) - gedit

Abrir Guardar Deshacer

Kismet-20150516-09-17-25-1.gpsxml

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE gps-run SYSTEM "http://kismetwireless.net/kismet-gps-2.9.1.dtd">

<gps-run gps-version="5" start-time="Sat May 16 09:17:25 2015">

    <network-file>/kismet_arch/Kismet-20150516-09-17-25-1.netxml</network-file>

    <gps-point bssid="84:78:AC:98:60:55" source="84:78:AC:98:60:55" time-sec="1431785862" time-usec="785010"
lat="-0.312451" lon="-78.445854" spd="1.474000" heading="255.563293" fix="3" alt="2567.952881" signal_dbm="-63"
noise_dbm="0"/>
    <gps-point bssid="58:97:1E:B2:4D:03" source="58:97:1E:B2:4D:03" time-sec="1431785862" time-usec="787705"
lat="-0.312451" lon="-78.445854" spd="1.474000" heading="255.563293" fix="3" alt="2567.952881" signal_dbm="-53"
noise_dbm="0"/>
    <gps-point bssid="58:97:1E:22:5A:E0" source="58:97:1E:22:5A:E0" time-sec="1431785862" time-usec="790328"
lat="-0.312451" lon="-78.445854" spd="1.474000" heading="255.563293" fix="3" alt="2567.952881" signal_dbm="-71"
noise_dbm="0"/>
    <gps-point bssid="58:97:1E:22:1F:73" source="58:97:1E:22:1F:73" time-sec="1431785862" time-usec="793236"
lat="-0.312451" lon="-78.445854" spd="1.474000" heading="255.563293" fix="3" alt="2567.952881" signal_dbm="-83"
noise_dbm="0"/>
    <gps-point bssid="58:97:1E:B2:4D:05" source="58:97:1E:B2:4D:05" time-sec="1431785862" time-usec="797282"
lat="-0.312451" lon="-78.445854" spd="1.474000" heading="255.563293" fix="3" alt="2567.952881" signal_dbm="-53"
noise_dbm="0"/>
    <gps-point bssid="84:78:AC:98:60:50" source="84:78:AC:98:60:50" time-sec="1431785862" time-usec="803775"
lat="-0.312451" lon="-78.445854" spd="1.474000" heading="255.563293" fix="3" alt="2567.952881" signal_dbm="-65"
noise_dbm="0"/>
    <gps-point bssid="58:97:1E:22:5A:E2" source="58:97:1E:22:5A:E2" time-sec="1431785862" time-usec="812880"
lat="-0.312451" lon="-78.445854" spd="1.474000" heading="255.563293" fix="3" alt="2567.952881" signal_dbm="-71"
noise_dbm="0"/>
```

**Figura 78.** Archivo .gpsxml

Para calcular las distancias, se utiliza el modelo de espacio libre, mediante el valor de la frecuencia en MHz y la potencia de recepción, con la fórmula:

$$d\ m\ = 10^{\frac{27.55 - 20\log_{10} f\ MHz\ + pot.recepción}{20}}$$

Al momento de calcular las distancias, ya se puede generar el archivo .kmz, mediante el archivo .csv, generado en Excel; para poder ubicar los puntos mediante latitud y longitud en Google Earth, y de esta forma determinar los radios de los círculos para la triangulación para una red *Wifi*.

| | A | B | C | D | E | F | G | H | I | J | K | L |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | <gps-point bssi | source= | time-se | time-use | lat= | lon= | spd= | headi | fix= | alt= | signal_dbr | noise_dbr |
| 2 | 00:21:29:A0:3F:80 | 00:21:29:A0:3F:80 | 1433189466 | 692187 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -63 | 0 |
| 3 | 00:27:22:84:F9:5D | 00:27:22:84:F9:5D | 1433189466 | 843066 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -65 | 0 |
| 4 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189466 | 894341 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -77 | 0 |
| 5 | E4:CE:8F:1C:D2:5E | E4:CE:8F:1C:D2:5E | 1433189466 | 895180 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -73 | 0 |
| 6 | E4:CE:8F:1C:D2:5E | E4:CE:8F:1C:D2:5E | 1433189466 | 897324 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -77 | 0 |
| 7 | 00:26:5A:C9:E6:45 | 00:26:5A:C9:E6:45 | 1433189467 | 391221 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -45 | 0 |
| 8 | 00:26:5A:C9:E6:45 | B8:E8:56:42:8A:56 | 1433189467 | 392041 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -67 | 0 |
| 9 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 392065 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 10 | 00:26:5A:C9:E6:45 | 00:26:5A:C9:E6:45 | 1433189467 | 493651 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -45 | 0 |
| 11 | 00:26:5A:C9:E6:45 | B8:E8:56:42:8A:56 | 1433189467 | 494291 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -65 | 0 |
| 12 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 494306 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 13 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 559812 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 14 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 559834 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 15 | 00:26:5A:C9:E6:45 | 00:26:5A:C9:E6:45 | 1433189467 | 596090 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -45 | 0 |
| 16 | 00:26:5A:C9:E6:45 | B8:E8:56:42:8A:56 | 1433189467 | 596794 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -67 | 0 |
| 17 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 596809 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 18 | 00:26:5A:C9:E6:45 | 00:26:5A:C9:E6:45 | 1433189467 | 698345 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -47 | 0 |
| 19 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 699198 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 20 | 00:26:5A:C9:E6:45 | 00:26:5A:C9:E6:45 | 1433189467 | 800934 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -47 | 0 |
| 21 | 00:26:5A:C9:E6:45 | B8:E8:56:42:8A:56 | 1433189467 | 801786 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -67 | 0 |
| 22 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 801807 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 23 | 00:26:5A:C9:E6:45 | 00:25:64:E2:63:C3 | 1433189467 | 817456 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -47 | 0 |
| 24 | 00:26:5A:C9:E6:45 | 00:26:5A:C9:E6:45 | 1433189467 | 903342 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -47 | 0 |
| 25 | 00:26:5A:C9:E6:45 | B8:E8:56:42:8A:56 | 1433189467 | 904295 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -65 | 0 |
| 26 | 00:00:00:00:00:00 | 00:00:00:00:00:00 | 1433189467 | 904320 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -49 | 0 |
| 27 | 00:26:5A:C9:E6:45 | 00:24:73:6E:DF:C1 | 1433189467 | 931169 | -0.312409 | -78.44582 | 0 | 0 | 3 | 2512.43897 | -47 | 0 |

Hoja1

**Figura 79.** Base de datos (.csv) mediante archivo .gpsxml

En la base de datos (Figura 79) se tiene varios puntos, por lo tanto se toma solamente una dirección MAC (58:97:1E:B2:4D:02), por ejemplo de la red ESPE-DOCENTES. Se debe descartar varios puntos, ya que se debe considerar el error de precisión del equipo GPS, las pérdidas de propagación por obstáculos como paredes, equipos o personas. Finalmente, se debe generar los círculos con las distancias de los puntos escogidos para la triangulación.


**Figura 80.** Archivo .kml en Google Earth (Red: ESPE-DOCENTES, BSSID: 58:97:1E:B2:4D:02)

En la figura 81 se determina el punto, mediante la triangulación de las antenas. Cabe recalcar que estos equipos solo pueden estar dentro de los edificios, por lo tanto también se descartan posibles ubicaciones en exteriores.


**Figura 81.** Ubicación AP (BSSID: 58:97:1E:B2:4D:02) en Google Earth

- Ubicación AP_1: 0°18'44.90" S 78°26'45.36" O

Se puede validar este resultado mediante una verificación en campo para comprobar la ubicación de los equipos, Access Point. Para esto mediante la aplicación móvil *Wifi Analyzer* detectamos el SSID, BSSID y la potencia de la señal del AP determinando que es el encontrado mediante triangulación en el 2do piso de Laboratorio de Electrónica (área de Networking).

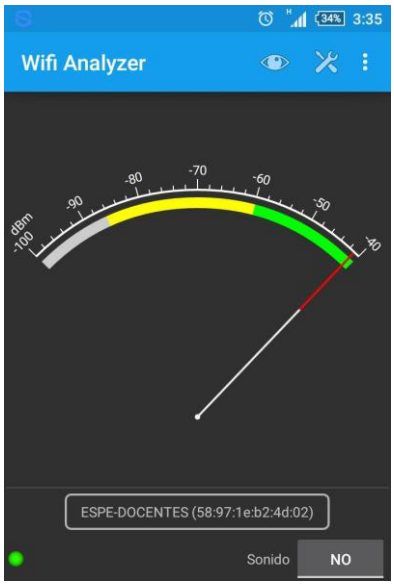



**Figura 82.** Visualización de potencia de la señal BSSID 58:97:1e:b2:4d:02

A continuación, se realiza nuevamente el análisis de la misma red, pero tomando otra dirección MAC (84:78:AC:98:67:12), dando como resultado que la ubicación del equipo se encuentra en los laboratorios de Biotecnología.

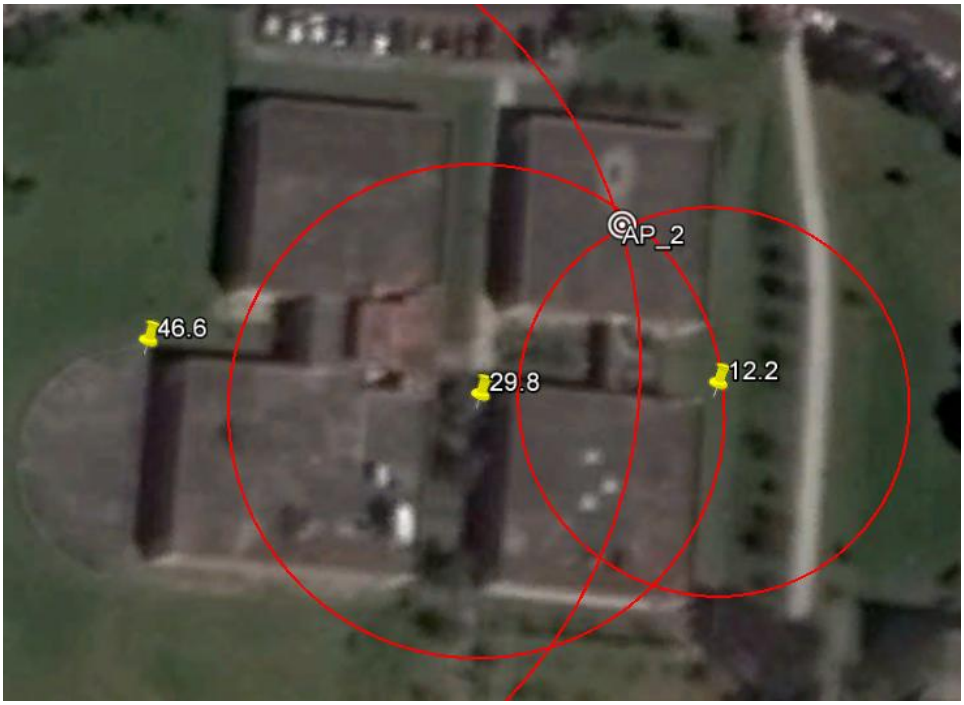



**Figura 83.** Visualización archivo .kml con Google Earth

- Ubicación AP_2: 0°18'43.95" S 78°26'44.40" O

Otro método para mejorar la visualización de la información recogida, es mediante el uso de *GisKismet* el cual es una herramienta inalámbrica de visualización de reconocimiento para representar los datos recopilados mediante *Kismet* de manera flexible. *GISKismet* utiliza SQLite para la base de datos y archivos .kml de GoogleEarth para su representación gráfica [50].

En primer lugar se debe añadir toda la información de los AP que hemos capturado a una base de datos. Para ello se utiliza el script *GisKismet.*

Giskismet permite inclinar el contenido de los archivos .netxml a una base de datos SQLite. Para ello nos situaremos en la carpeta donde se encuentran las capturas y escribiremos el siguiente comando [51]:

**giskismet -X KismetLogFile.netxml**

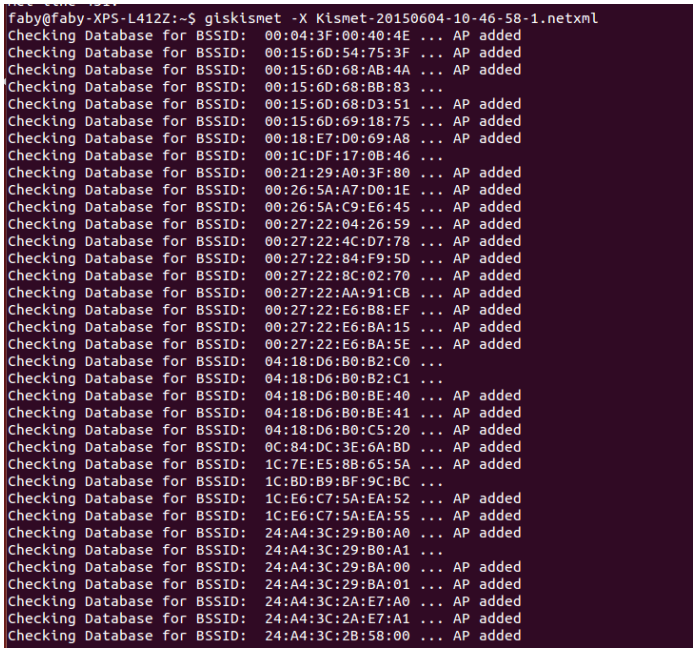



**Figura 84.** Información colocada en un archivo de base de datos

Automáticamente el script iniciara y comprobará uno a uno si los AP están guardados en la base de datos, si no existe añadirá el AP y toda la información relacionada con él, y si existe saltará al siguiente.

Giskismet tiene la posibilidad de convertir en un archivo *.kml* de Google Earth nuestra base de datos, para así visualizar las redes en un mapa del mismo programa.

El comando a introducir para crear ese archivo es el siguiente:

**giskismet -q "select * from wireless" -o output.kml KismetLogFile.netxml**

el parámetro -q indica una búsqueda SQL, la sentencia "select * from wireless" significa que seleccione todo de la base de datos wireless (nombre por defecto), -o indica la salida de un archivo y seguidamente escribiremos el nombre deseado sin olvidar la extensión [14].

```
Checking Database for BSSID:  84:78:AC:C0:80:23 ... AP added
Checking Database for BSSID:  84:78:AC:C0:80:25 ... AP added
Checking Database for BSSID:  90:94:E4:B1:B0:62 ... AP added
Checking Database for BSSID:  B0:C5:54:81:46:46 ... AP added
Checking Database for BSSID:  B4:52:7E:78:AC:28 ... AP added
Checking Database for BSSID:  C8:BE:19:61:ED:DA ... AP added
faby@faby-XPS-L412Z:~$ giskismet -q "select * from wireless" -o prueba.kml Kisme
t-20150529-16-57-54-1.netxml
faby@faby-XPS-L412Z:~$
```

**Figura 85.** Creación de archivo .kml

El resultado es un archivo *prueba.kml* que se abre con Google Earth:


**Figura 86.** Georefenciación de AP mediante GisKismet

En el mapa se observa una especie de dianas, cada una corresponde con un AP, el código de colores es simple, el rojo significa que tiene seguridad WEP, el color verde indica que no posee ningún tipo de seguridad y el amarillo WPA.

Si se pulsa sobre una red se visualiza la información asociada a ella:

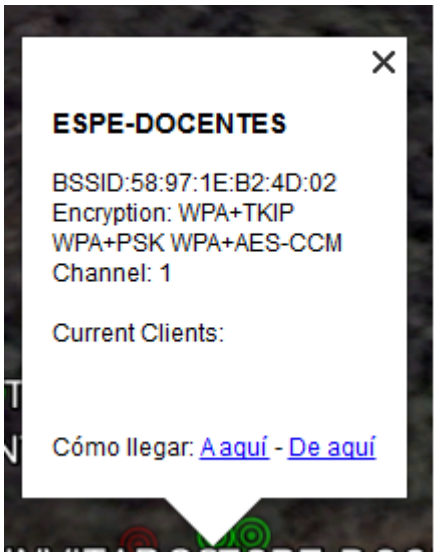



**Figura 87.** Información de la Red

# CAPITULO V

# CONCLUCIONES Y RECOMENDACIONES

## 5.1 CONCLUSIONES

- Se concluye que se es capaz de realizar un sistema de análisis de tráfico de redes 802.11 para el monitoreo y administración de la red, con la utilización del software Kismet y el equipo Raspberry Pi B+ gracias al bajo consumo de potencia, la portabilidad del dispositivo y los bajos costos de software para su desarrollo, permitiendo así un ahorro significativo frente a los analizadores de tráfico de red existentes en el mercado.
- Con el software adecuado y configurado la tarjeta inalámbrica en modo monitor se concluye que es posible capturar la trama MAC en 802.11 ya que las tramas de control, datos y administración son claramente visibles en la captura de la trama 802.11.
- Al realizar las pruebas con la tarjeta Raspberry Pi B+ durante 15 minutos en el entorno del Laboratorio de Electrónica de la institución educativa, se evidencia que de 49219 paquetes totales capturados se tiene 11976 paquetes malformados IEEE 802.11, lo cual nos proporciona 24.33% de la trama con error al utilizar el módulo USB inalámbrico TP-LINK TL-WN722N.
- Debido a las múltiples resultados con el mensaje "*Malformed Packet*" se realiza un análisis paralelo del procesamiento y uso del CPU, con lo cual se concluye que el continuo incremento de valores en el parámetro *load average* de 1 y 5 minutos, sobrepasa el valor de 0,7 recomendable en la teoría, ya que estos valores representan la cantidad de procesos que están

esperando en cola para ser ejecutados representan un problema de sobrecarga de la máquina (procesamiento del CPU de la tarjeta) y por ende influyen en la correcta ejecución y funcionamiento de Kismet.

- Se realiza nuevas pruebas con la tarjeta Raspberry Pi 2 modelo B y el módulo USB inalámbrico TP-LINK TL-WN722N, donde se evidencia que este es más óptimo debido a su capacidad de procesamiento al tener 4 núcleos comparado con Raspberry Pi B+, sin embargo aún se tienen resultados de paquetes malformados.
- Mediante el proceso de análisis del uso y procesamiento del CPU de ambas tarjetas se determina que el procesamiento del CPU de Raspberry Pi B+ ejecutándose el software Kismet alcanza el 100% de procesamiento saturando a la tarjeta Raspberry mientras que la Raspberry Pi 2 modelo B no ocupa ni el 50% de uso o procesamiento del CPU de la Raspberry.
- Con la adquisición de un nuevo módulo USB inalámbrico Alfa AWUS036NH y junto al Raspberry Pi B+, se tiene 0% paquetes malformados, por lo tanto el inconveniente recae en el dispositivo TP-LINK TL-WN722N ya que a pesar de tener más sensibilidad, el dispositivo ALFA tiene 10 veces más potencia que TP-LINK, además es un dispositivo apto para realizar auditorías ya que soporta modo monitor, es compatible con los estándares 802.11a, 802.11b y 802.11n, mantiene siempre una conexión estable, y es ideal para entornos con mucho ruido, por ejemplo, ambientes que tienen muchas redes.

- Mediante el proceso de triangulación de antenas se puede determinar la ubicación del AP mediante el cálculo de la distancia obteniendo de la potencia de recepción del equipo.
- Del análisis de resultados en los laboratorios de Electrónica se determina que existe 55 redes detectadas de las cuales 13 son redes "data", Kismet no pudo detectar ninguna trama beacon o de gestión y por lo tanto aún no pueden decir qué tipo de red es, de infraestructura alrededor de 30% y 1 red se determina como Ad-Hoc.
- De los resultados obtenidos se muestra que todas las redes inalámbricas son del tipo 802.11b ya que al menos existe un cliente de este tipo para que degrade toda la red.
- Como método de solución de análisis inalámbrico, el Raspberry Pi puede satisfacer las necesidades de los administradores de red como iniciativa de seguridad de la institución o empresa; ya que la capacidad de configuración de hardware y software, bajo costo y la portabilidad del equipo hacen de esta herramienta asequible, para su uso con simplemente encenderlo y salir a caminar, andar o conducir.
- Mediante una observación de campo se puede confirmar que la ubicación obtenida mediante el proceso y cálculo de triangulación es igual a la visualizada en la visita por lo tanto se verifica el correcto funcionamiento del GPS junto la ejecución de Kismet.

## 5.2 RECOMENDACIONES

- Para la instalación de Kismet es importante tomar en cuenta las últimas versiones del software además verificar cada uno de los dispositivos de red compatibles con las versiones recientes, ya que en las versiones

anteriores que muchas fuentes de información aún muestran para la configuración (source = *madwifi_g*, ath0, internet). MadWifi ha sido reemplazado por otros drivers ath5k y ath9k, que son parte del núcleo de Linux para dispositivos LAN inalámbricos con chipsets Atheros.

- Para el análisis de las distancias se debe considerar que el mismo equipo GPS tiene errores de precisión también no se considera obstrucciones como paredes, columnas, vehículos, personas por lo tanto se recomienda hacer una estudio más detallado para el análisis de las distancias ya que se considera un modelo de entorno de red ideal.
- Utilizar el prototipo implementado para que Kismet aumente su detección de ataques en capas superiores de la arquitectura de red; y continuar con el análisis de red en la Universidad para ayudar al administrador de la red con todos los parámetros y determinar la eficiencia del diseño de la red creada.

# BIBLIOGRAFÍA

[1] M. Richardson and S. Wallance, Getting Started with Raspberry Pi, 2012.

[2] P. Membrey and D. Hows, Learn raspberry Pi with Linux, 2012.

[3] G. Halfacree and E. Upton, "Raspberry Pi - User Guide," 2012. [Online]. Available: http://www.cs.unca.edu/~bruce/Fall14/360/RPiUsersGuide.pdf. [Accessed Julio 2014].

[4] E. Barahona and P. Gellibert, "Analizador de trádico de Red," 2011. [Online]. Available: https://www.dspace.espol.edu.ec/bitstream/123456789/20042/3/Tesis%20Barahona-Gellibert.pdf. [Accessed Marzo 2015].

[5] "Las 75 Herramientas de Seguridad Más Usadas," [Online]. Available: http://insecure.org/tools/tools-es.html. [Accessed Marzo 2015].

[6] "Analizadores de Red," [Online]. Available: http://fpgalapagar.es/carmenluengo/mod/page/view.php?id=147&inpopup=1. [Accessed Marzo 2015].

[7] "Protocol Analyzers," [Online]. Available: http://www.vias.org/wirelessnetw/wndw_08_06_03.html. [Accessed Marzo 2015].

[8] "Raspberry Pi," [Online]. Available: http://es.wikipedia.org/wiki/Raspberry_Pi. [Accessed Marzo 2015].

[9] "Hardware Raspberry Pi," [Online]. Available:

http://www.raspberryshop.es/hardware-raspberry-pi.php. [Accessed Marzo 2015].

[10] V. Alvarez, "Diseño de dispositivo no invasivo para rastreo y detección de movimiento giratorio de cabeza mediante sistemas microelectromecánicos para control de ordenador personal," 2013. [Online]. Available: http://biblioteca.usac.edu.gt/tesis/08/08_0351_EO.pdf. [Accessed Marzo 2015].

[11] A. Cobo, "Guia Raspberry Pi," 2013 - 2015. [Online]. Available: http://dplinux.net/guia-raspberry-pi. [Accessed Febrero 2015].

[12] "About Debian," 2014. [Online]. Available: https://www.debian.org/intro/about.en.html#what. [Accessed Marzo 2015].

[13] "Welcome to Raspbian," [Online]. Available: http://www.raspbian.org/. [Accessed Marzo 2015].

[14] J. M. García, "Auditoria de redes inalámbricas," 2011-2012. [Online]. Available: https://es.scribd.com/doc/97722405/Proytecto-Final. [Accessed Marzo 2015].

[15] "Instalacion y uso de kismet en sistemas linux. --1era parte--," [Online]. Available: http://foro.elhacker.net/hacking_wireless/instalacion_y_uso_de_kismet_en_sistemas_linux_1era_parte-t420464.0.html. [Accessed Febrero 2015].

[16] "Manual funcionamiento básico del programa más conocido en la auditoria wireless: Kismet," [Online]. Available:

http://hwagm.elhacker.net/htm/kismet.htm. [Accessed Febrero 2015].

[17] C. Scott, "War Pi," 2013. [Online]. Available: http://www.sans.org/reading-room/whitepapers/networkdevs/war-pi-34435. [Accessed Febrero 2015].

[18] F. Thornton, M. J. Schearer and B. Haines, Kismet Hacking, 2008.

[19] "Tplink," 2014. [Online]. Available: http://www.tp-link.com/mx/products/details/?model=TL-WN722N. [Accessed Marzo 2015].

[20] "AWUS036NH - 802.11b/g/n Wireless USB adapter," [Online]. Available: http://www.alfa.com.tw/products_show.php?pc=34&ps=21. [Accessed Abril 2015].

[21] "BU-353-S4," 2014. [Online]. Available: http://usglobalsat.com/p-688-bu-353-s4.aspx#images/product/large/688.jpg. [Accessed Marzo 2015].

[22] "Instalar y configurar Wireshark en Linux," 2012. [Online]. Available: www.tuxylinux.com/instalar-y-configurar-wireshark-en-linux/. [Accessed Marzo 2015].

[23] "Cómo trabajar con ficheros pcap WiFi en Windows," [Online]. Available: https://www.acrylicwifi.com/software/analizador-wifi-acrylic-wifi-profesional/como-trabajar-ficheros-pcap-wifi-windows/. [Accessed Abril 2015].

[24] "Augmented PCAP Next Generation Dump File Format," [Online]. Available: https://github.com/HoneProject/Linux-Sensor/wiki/Augmented-PCAP-Next-Generation-Dump-File-Format. [Accessed Abril 2015].

[25] ".PCAPNG File Extension," [Online]. Available: http://fileinfo.com/extension/pcapng. [Accessed Abril 2015].

[26] "A look at the pcap file format," 2012. [Online]. Available: http://www.kroosec.com/2012/10/a-look-at-pcap-file-format.html. [Accessed Abril 2015].

[27] "Network packet capture and dissecting in Perl 101," 2012. [Online]. Available: http://perl.pt/files/ptpw2012/packet_capture_and_dissecting_101_2x2.pdf. [Accessed Abril 2015].

[28] "Development/LibpcapFileFormat," 2013. [Online]. Available: https://wiki.wireshark.org/Development/LibpcapFileFormat. [Accessed Abril 2015].

[29] X. Tena, "TRABAJO DE FIN DE CARRERA," Diciembre 2013. [Online]. Available: http://upcommons.upc.edu/pfc/bitstream/2099.1/20067/1/memoria.pdf. [Accessed Marzo 2015].

[30] "Introducción a Wi-Fi (802.11)," [Online]. Available: http://es.kioskea.net/contents/789-introduccion-a-wi-fi-802-11-o-wifi. [Accessed Marzo 2015].

[31] O. León and S. Hernán, "NORMAS 802.11a, 802.11b y 802.11g," [Online]. Available: http://dspace.ups.edu.ec/bitstream/123456789/221/8/Tesis.pdf. [Accessed Marzo 2015].

[32] "Capitulo 2: Familia IEEE 802.11," [Online]. Available: http://bibing.us.es/proyectos/abreproy/11579/fichero/f.+Cap%EDtulo+2+-

+Familia+IEEE+802.11.pdf. [Accessed Marzo 2015].

[33] "Tramas 802.11," [Online]. Available: http://www.bdat.net/seguridad_en_redes_inalambricas/x187.html. [Accessed Marzo 2015].

[34] P. Jara and P. Nazar, "Estándar IEEE 802.11 X de las WLAN," [Online]. Available: http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf. [Accessed Abril 2015].

[35] J. C. Chamorro, "DISEÑO DE UNA RED DE ÁREA LOCAL (LAN) INALÁMBRICA PARA LA EX - FACULTAD DE INGENIERÍA ELÉCTRICA," 2001. [Online]. Available: http://bibdigital.epn.edu.ec/bitstream/15000/5235/1/T1816.pdf. [Accessed Marzo 2015].

[36] "802.11 Sniffer Capture Analysis - Management Frames and Open Auth - See more at: https://supportforums.cisco.com/document/101431/80211-sniffer-capture-analysis-management-frames-and-open-auth#sthash.qFkbULn7.dpuf," 2014. [Online]. Available: https://supportforums.cisco.com/document/101431/80211-sniffer-capture-analysis-management-frames-and-open-auth. [Accessed Abril 2015].

[37] "Cisco: Security Setup," [Online]. Available: http://www.cisco.com/c/en/us/td/docs/wireless/access_point/1200/vxworks/configuration/guide/ap120scg/bkscgc8.html. [Accessed Marzo 2015].

[38] "Tipos de autenticación o claves Wifi, Wireless, inalambrico o no cableado," [Online]. Available:

http://www.xnet.ec/b2evolution/blogs/blog5.php/2010/10/17/tipos-de-autenticacion-o-claves-wifi-wireless-inalambrico-o-no-cableado. [Accessed Marzo 2015].

[39] "Autenticación 802.1x," [Online]. Available: http://driveragent.com/c/archive/2f28fdf9/image/28-0-418/Intel(R)-PRO/Wireless-2200BG/2915ABG-Network-Connection?PHPSESSID=hj5b9319ar6deqdjjeb41b41s3. [Accessed Marzo 2015].

[40] "Hacking WiFi: Entendiendo WPA/WPA2 Personal (Parte 11)," [Online]. Available: http://www.flu-project.com/2013/12/hacking-wifi-entendiendo-wpawpa2.html. [Accessed Marzo 2015].

[41] "Configuring 802.1X Port-Based Authentication," [Online]. Available: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_9_ea1/configuration/guide/scg/Sw8021x.html. [Accessed Marzo 2015].

[42] "Seguridad," [Online]. Available: https://rinuex.unex.es/modules.php?op=modload&name=Textos&file=index&serid=39. [Accessed Marzo 2015].

[43] "EAP," [Online]. Available: http://www.bdat.net/seguridad_en_redes_inalambricas/x80.html. [Accessed Abril 2015].

[44] "Roaming," [Online]. Available: http://www.adrformacion.com/cursos/wifi/leccion3/tutorial3.html. [Accessed

Marzo 2015].

[45] "Triangulación," [Online]. Available: http://es.wikipedia.org/wiki/Triangulaci%C3%B3n. [Accessed Abril 2015].

[46] L. Letham, GPS fácil. Uso del sistema de posicionamiento global, 2001.

[47] "Funcionamiento del comando top en Linux," [Online]. Available: https://geekytheory.com/funcionamiento-del-comando-top-en-linux/. [Accessed Abril 2015].

[48] "GpsDrive – Navigation Software for Linux, Mac, and UNIX," [Online]. Available: http://www.gpsdrive.de/documentation/faq.shtml. [Accessed Abril 2015].

[49] A. YACCHIREMA, "ANÁLISIS DE LOS SISTEMAS DE ATAQUE Y PROTECCIÓN EN," [Online]. Available: http://repositorio.espe.edu.ec/bitstream/21000/8380/1/T-ESPE-047801.pdf. [Accessed Mayo 2015].

[50] "GisKismet," [Online]. Available: http://trac.assembla.com/giskismet. [Accessed Abril 2015].

[51] "Wifi Mapping," [Online]. Available: https://www.altamiracorp.com/blog/employee-posts/wifi-mapping. [Accessed Abril 2015].