

UNIVERSIDAD LUTERANA SALVADOREÑA
FACULTAD DEL HOMBRE Y LA NATURALEZA
LICENCIATURA EN CIENCIAS DE LA COMPUTACION



MATERIA: ANÁLISIS DE SISTEMAS

PRIMER AVANCE DEL PROYECTO:
ANALIZADOR FORENSE DE WIFI CON LA HERRAMIENTA
KISMET

CATEDRÁTICO: JOSÉ LUIS ALVARADO AGUILAR

PRESENTADO POR:

Estudiantes
PÉREZ MOLINA, CARLOS MAURICIO
AYALA BARDALES, REINA BEATRIZ
PINEDA MOLINA, RONAL FELIPE
ALFARO RAMIREZ, MAURICIO ENRIQUE

San Salvador, 11 de noviembre de 2017.

ÍNDICE

INTRODUCCIÓN.....	3
.....	3
.....	3
OBJETIVOS.....	4
OBJETIVO GENERAL.....	4
OBJETIVOS ESPECÍFICOS.....	4
.....	4
¿Qué es la herramienta KISMET?.....	5
CARACTERÍSTICAS.....	5
CONCLUSIÓN.....	8

INTRODUCCIÓN

En el presente proyecto se propone el uso de la Herramienta **Kismet** la cual sirve para detectar la presencia de redes wireless, incluidas las que estén ocultas. Puede descubrir y reportar el rango de IP usado por una red wireless particular, como también los niveles de señal. Kismet también puede captar todos los conductores de paquetes de todas las redes wireless, puedes utilizar Kismet para localizar a través de las herramientas wireless networks, optimizar la señal para puntos de accesos y clientes y detectar intrusiones en las redes.

Esta herramienta tiene varios usos como:

- Detectar otras redes que pueden causar interferencias a la nuestra.
- También nos sirve para WarDriving, es decir, detectar todos los APs que están cerca.

Para valorarnos a nosotros mismos, al saber si lo llegamos a usar correctamente, que tenemos ciertas habilidades con linux y somos capaces de compilar programas, de instalar programas y de configurarlos correctamente. Y más cuando los resultados con poco trabajo son tan agradecidos y refrescantes.

El desarrollo de este proyecto, nos permite aprender y aplicar sobre el uso de la herramienta **KISMET** para el aprendizaje educativo de los estudiantes y que conozcan una de las herramientas más populares dentro de la área de la tecnología.

OBJETIVOS

OBJETIVO GENERAL

Saber que es KISMET y como se utiliza en la informática forense como herramienta para analizar las

OBJETIVOS ESPECÍFICOS

-Utilizar la herramienta Kismet en un computador con sistema GNU/Linux O windows desde la conexión wlan o.

-Obtener información adicional que sirva para el análisis de la informática forense.

¿Qué es la herramienta KISMET?

Es una aplicación capaz de rastrear y detectar diferentes dispositivos que se conectan a la señal wifi, que sin darse cuenta el propietario del servicio podría estar siendo interrumpido por usuarios no aceptados dificultando o disminuyendo la velocidad del servicio de internet.

Actúa como un detector de redes wifi un sistema de detección de intrusos, KISMET también se utiliza para para detectar el SSID de una red WLAN. Esa utilidad WI-FI soporta la decodificación WEP mientras funciona el sistema. En los casos en que el SSID no puede ser revelado por el sondeo, el envío de tramas de disociación forjados puede exponer el SSID con una solicitud de reasociación

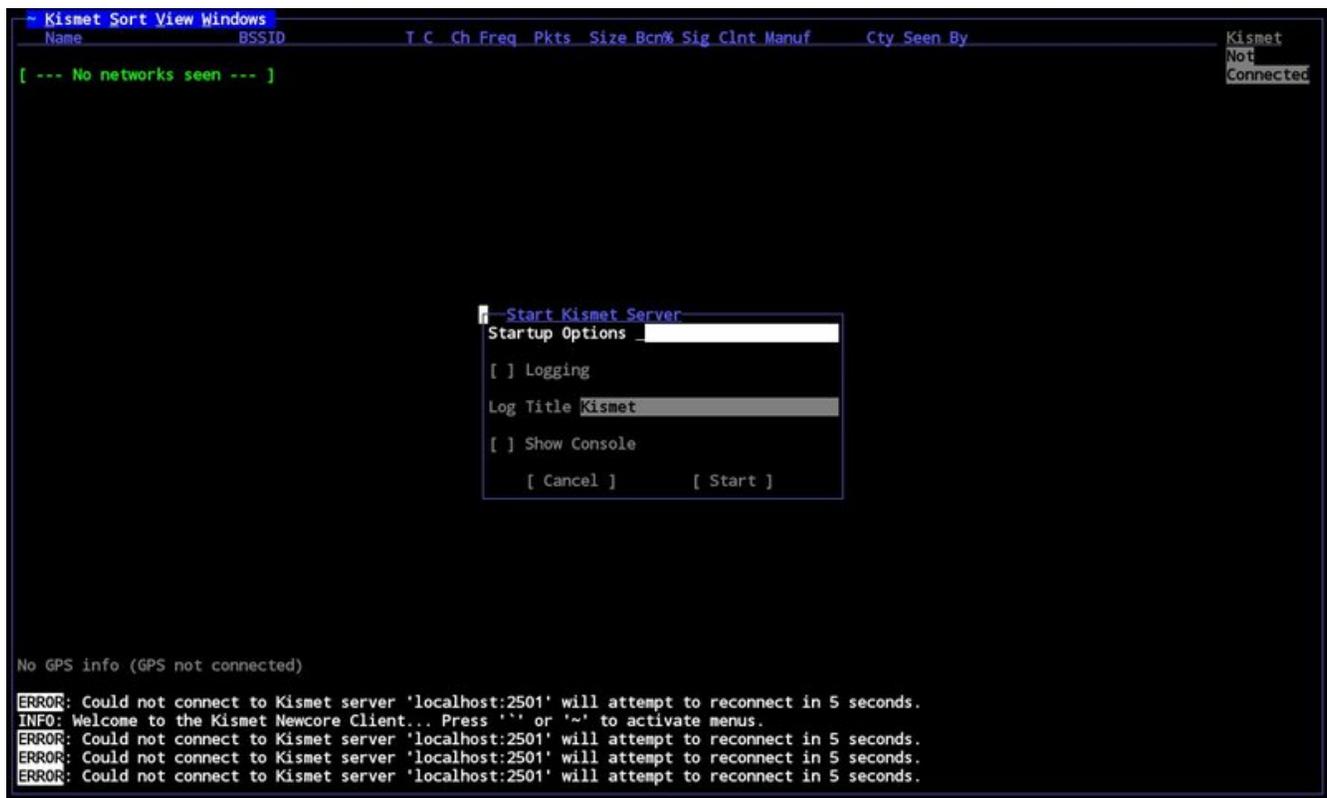
Kismet es un sniffer, un husmeador de paquetes, y un sistema de detección de intrusiones para redes inalámbricas 802.11. Kismet funciona con cualquier tarjeta inalámbrica que soporte el modo de monitorización raw, y puede rastrear tráfico 802.11b, 802.11a, 802.11g y 802.11n. El programa corre bajo Linux, FreeBSD, OpenBSD, y Mac OS X. El cliente puede también funcionar en Windows.

Kismet se diferencia de la mayoría de los otros sniffers inalámbricos en su funcionamiento pasivo. Es decir que lo hace sin enviar ningún paquete detectable, permitiendo detectar la presencia de varios puntos de acceso y clientes inalámbricos, asociando unos con otros.

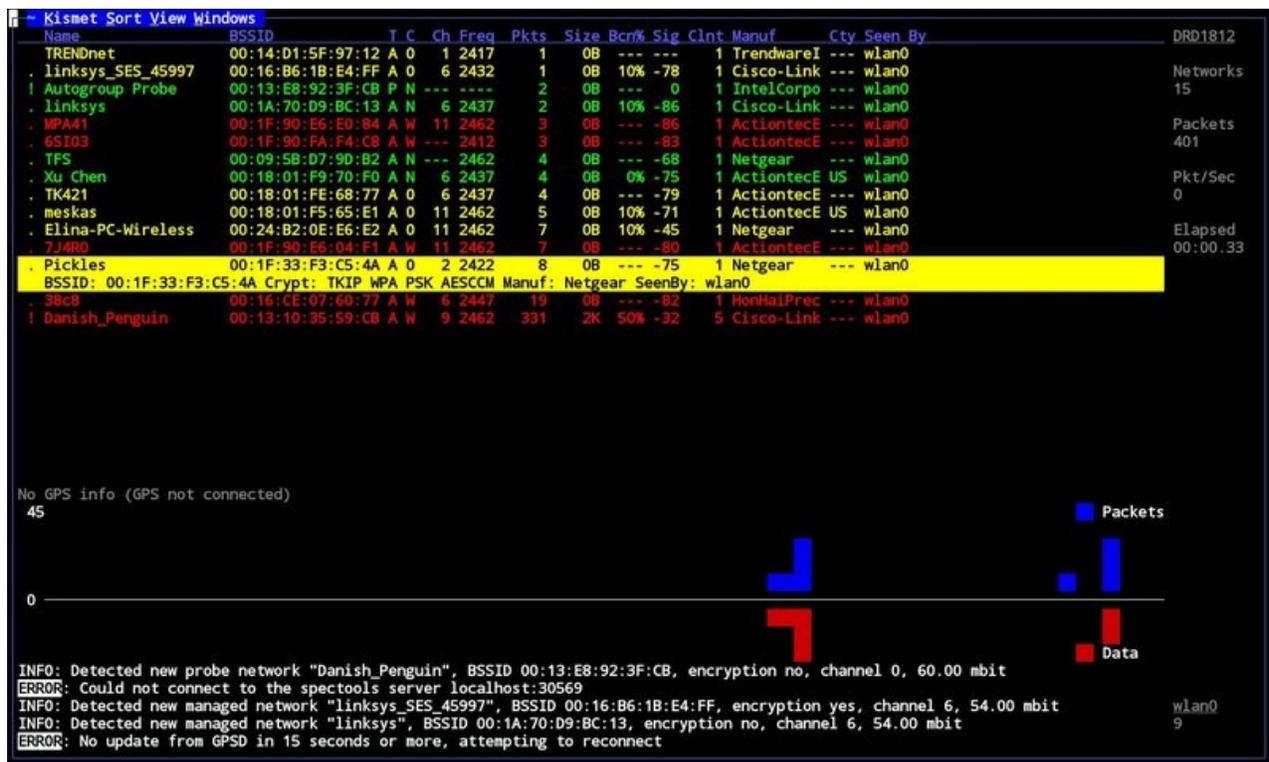
CARACTERISTICAS

Kismet también incluye características básicas de Sistemas de detección de intrusos como detectar programas de rastreo inalámbricos incluyendo a NetStumbler, así como también ciertos ataques de red inalámbricos.

En las siguientes imágenes se muestra la interfaz de usuario y algunas funciones con las que cuenta KISMET.



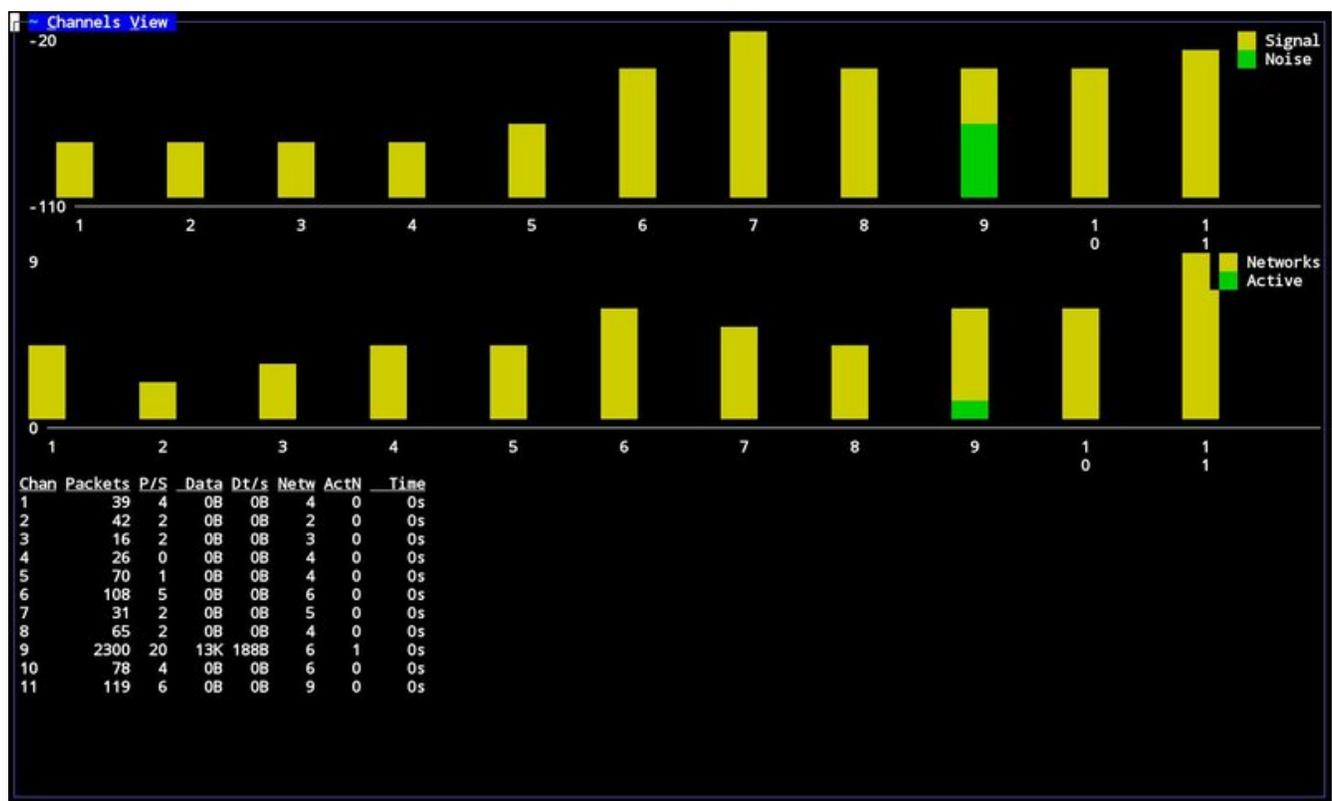
Pantalla de logueo al sistema imagen 1.



Analizando distintos puntos de red, imagen 2.



Transferencia de paquetes desde los dispositivos conectado al mismo router las barras muestran la transmisión de los mismos, imagen 3.



Análisis de los datos transferidos con mas detalle CANAL, PAQUETE, FECHA, TIEMPO entre otros. Imagen 4.

CONCLUSIÓN

Si bien el presente trabajo abordó la importancia de esta herramienta KISMET en el área forense ,donde se da a conocer las diferentes características y capacidad para rastrear y detectar con mayor facilidad y eficiencia diferentes dispositivos que se conectan a la señal wifi y sin que el propietario de esta se de cuenta.

Llegamos a la conclusión de la la importancia del uso de estas nuevas tecnologías para las áreas mas vulnerables y con mayor demanda de nuevas tecnologías que les podría facilitar el proceso de investigación , sin ponerla en riesgo la evidencia recolectada o alterarla , también ayuda a tener una mayor agilidad en los procesos que se realicen sin tener riesgos de perder la evidencia o que la evidencia sea adulterada o manipulada por terceros.