PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

TEMA: "ANÁLISIS DE VULNERABILIDADES DE SEGURIDADES EN REDES INALÁMBRICAS DENTRO DE UN ENTORNO EMPRESARIAL QUE UTILIZAN CIFRADO AES Y TKIP, WPA PERSONAL Y WPA2 PERSONAL DEL DMQ"

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS

AUTOR: SERRANO FLORES ANDRÉS GUILLERMO

DIRECTOR: ING. FRANCISCO RODRÍGUEZ

Quito, 2011

DEDICATORIA

Quiero dedicar este trabajo a mis padres Guillermo y Carmita; a mi padre por apoyarme en todos los años de estudio de ésta carrera y por brindarme esa seguridad al saber que siempre contaré con él en cualquier circunstancia, convirtiéndose así en mi mejor amigo; a mi madre por brindarme su conocimiento y guiarme al momento de elaborar la presente disertación de grado, siendo así una de las personas claves que me ayudó a mantener la perseverancia y constancia a lo largo de esta investigación.

No puedo olvidar tampoco a mis hermanos Alexandra y Adrián que se que en cualquier momento puedo contar con ellos.

AGRADECIMIENTO

Quiero comenzar estar líneas agradeciendo a mi Director de Tesis, el Ing. Francisco Rodríguez, quien fue la persona en ayudarme a encontrar el tema de tesis de grado, y con su gran experiencia profesional, me ayudó a desarrollarla y llegar a culminarla obteniendo el resultado final de ésta investigación; igualmente quiero agradecer a mis correctores, la Ing. Suyana Arcos y el Ing. Alfredo Calderón, quienes me apoyaron en todo momento en la elaboración de la misma.

También quiero agradecer a las empresas “ELECDOR S.A.” y “ENCAJAS PACKING & DESIGN”, en donde me abrieron sus puertas para poder realizar el estudio de esta investigación, me brindaron el acceso a sus redes inalámbricas y así poder comprobar la seguridad de las mismas, el cual es el tema de mi disertación de grado.

Finalmente, y no por eso menos importante, a mi familia, a mis padres por su apoyo incondicional durante toda mi vida, quienes siempre me han permitido desarrollarme en lo que me gusta hacer; y a mis hermanos, de quienes se que en cualquier circunstancia de la vida, estarán para apoyarme.

INTRODUCCIÓN

En el texto a continuación se pretende, como punto inicial, dar a conocer la importancia y el auge que las redes inalámbricas están teniendo en la actualidad, ya que existe un incremento considerable en pequeñas, medianas y grandes empresas, donde optan en su mayoría para el acceso de estaciones móviles hacia el internet, y también, pero en menor proporción, para la transmisión de datos. Se puede aclarar, que optando por esta tecnología de transmisión por ondas de radio, se puede llegar a tener las mismas funcionalidades que con una red cableada, minimizando los costos y con una mayor flexibilidad y versatibilidad.

Se hará un breve conocimiento de la topología y el modo de funcionamiento básico de este tipo de redes para tener una mayor percepción a la hora de instalar una WLAN, que a pesar de tener ventajas como las mencionadas, todavía posee debilidades en el ámbito de la seguridad que todavía no se ha llegado a resolver de forma satisfactoria. La transmisión de datos por señales de radio plantea de por si un serio reto a la seguridad, se debe de proveer de mecanismos principalmente basadas en criptografía o cifrado para garantizar la confidencialidad de lo que se está enviando y recibiendo dentro de una WLAN.

Al revisar la necesidad de garantizar la seguridad cuando se utiliza transmisión por radio, se pasara a analizar a que tipos de ataques se encuentran expuestas las redes inalámbricas y la forma de llevar a cabo dichos ataques, se tiene la colaboración de dos pequeñas empresas que permitirán realizar pruebas y practicar con sus dispositivos de WLAN, de los que se obtendrá las diferentes datos que servirán para el estudio y desarrollo de este documento. Se utilizaran dos herramientas de software que se encuentran en Internet para romper el encriptado de la red (CommView for WiFi y suite Aircrack-ng).

Se detallaran el funcionamiento de los intentos realizados de garantizar la seguridad antes mencionada. En primera instancia se analizara el mecanismo de cifrado WEP (Wired Equivalent Protocol) y se constatara las deficiencias que presenta, ya que diversos estudios han demostrado que no ofrece garantías sólidas de seguridad. Posteriormente como alternativa se pasara a

detallar el funcionamiento de otros estándares, el WPA (Wi-Fi Protected Access) Personal y WPA2 Personal, basados en el estándar 802.11i que intenta solucionar las debilidades del sistema de cifrado por WEP y que en principio ofrece mejores mecanismos para el cifrado de datos y autentificación de usuarios. Se debe tener en cuenta que no debe ser suficiente el utilizar las técnicas de encriptado que ofrecen los diferentes dispositivos inalámbricos para mantener la seguridad una red WiFi, sino que se deben implementar mecanismos adicionales que protejan y garanticen la seguridad de éste tipo de redes.

Finalmente, luego de haber analizado las medidas de protección y los ataques que se pueden llevar a cabo en una red inalámbrica, se pasará a recopilar todas estas ideas a modo de tutorial, que permita configurar adecuadamente la WLAN, no solamente a la configuración del punto de acceso o del router, sino también en el diseño de la red inalámbrica en sí.

INDICE

DEDICATORIA ..... **II**

AGRADECIMIENTO ..... **II**

INTRODUCCIÓN ..... **III**

1. Redes Inalámbricas **1**

1.1 Crecimiento de las redes inalámbricas 2

1.2 Normativa IEEE 802.11 4

1.2.1 Estándar 802.11 5

1.2.2 802.11a 5

1.2.3 802.11b 6

1.2.4 802.11g 7

1.2.5 802.11n 7

1.3 Topologías 8

1.3.1 Redes "ad-hoc" 9

1.3.2 Redes de infraestructura 10

2. Seguridad en Redes Inalámbricas **13**

2.1 Protocolos de seguridad 13

2.1.1 EAP (Extensible Authentication Protocol) 13

2.1.2 SSID (Service Set Id) 16

2.2 WEP (Wired Equivalency Privacy) 17

2.3 WPA (Wi-Fi Protected Access) 18

2.4 WPA2 18

2.5 Cifrados AES y TKIP 19

2.5.1 AES (Advanced Encryption Standard) 19

2.5.2 TKIP (Temporal Key Integrity Protocol) 20

3. Cifrados WEP, WPA, WPA2 ..... **22**

3.1 WEP 22

3.1.1 Funcionamiento 22
3.1.2 Vulnerabilidades WEP 24
3.1.3 Alternativas a WEP 27
3.2 WPA 28
3.2.1 Funcionamiento 29
3.2.2 WPA vs WEP 31
3.3 WPA2 31
3.3.1 Estándar 802.11i 32
3.3.2 Características 32

4. Software para comprobación de vulnerabilidad 34
4.1 CommView for WiFi 34
4.1.1 Uso de la herramienta 35
4.2 Suite Aircrack-ng 43
4.2.1 Airodump-ng 44
4.2.2 Airdecap-ng 47
4.2.3 WZCook 48
4.2.4 Aircrack-ng 48

5. Estudio de Casos 56
5.1 Electrificaciones del Ecuador S.A. (Elecdor S.A.) 57
5.1.1 Misión 57
5.1.2 Visión 58
5.1.3 Valores 58
5.1.4 Atacando la red 60
5.2 EN CAJAS Packing & Design 70
5.2.1 Misión 71
5.2.2 Visión 71
5.2.3 Valores 71
5.2.4 Atacando la red 73
5.3 Consejos básicos para que la red WiFi sea segura 78

5.3.1 Seguridades básicas..... 79
5.3.2 Consejos para contraseñas seguras..... 80
5.3.3 Soluciones adicionales de protección..... 82

CONCLUSIONES 85
RECOMENDACIONES 88
GLOSARIO DE TÉRMINOS 90
REFERENCIAS DE INTERNET 99
BIBLIOGRAFÍA 101
ANEXOS 103

INDICE DE FIGURAS

CAPÍTULO I

Figura 1.01 Redes inalámbricas en el mundo 1
Figura 1.02 Logo WiFi 2
Figura 1.03 Router Linksys WAP54G 4
Figura 1.04 Tarjeta inalámbrica Linksys 4
Figura 1.05 Access Point D-Link 4
Figura 1.06 Logo WiFi Certified 4
Figura 1.07 Redes ad-hoc 9
Figura 1.08 Redes estructuradas 10

CAPÍTULO II

Figura 2.01 Autenticación EAP 14

CAPÍTULO III

Figura 3.01 Cifrado WEP 24
Figura 3.02 Arquitectura 802.1x/EAP 30

CAPÍTULO IV

Figura 4.01 CommView for WiFi 34
Figura 4.02 Guía de instalación del controlador wireless 35
Figura 4.03 Ventana de adaptadores disponibles para su instalación 36
Figura 4.04 Configuración inicial CommView for WiFi 37
Figura 4.05 Configuración Reglas CommView for WiFi 37
Figura 4.06 Explorador de redes WiFi 38
Figura 4.07 Redes WiFi encontradas 38
Figura 4.08 Selección red WiFi 39
Figura 4.09 Captura de tráfico de la red seleccionada 39
Figura 4.10 Creación de archivo de captura de paquetes 40
Figura 4.11 Access Point encontrados con sus clientes asociados 40
Figura 4.12 Visor de Registros CommView for WiFi 41
Figura 4.13 Configuración de Opciones Generales 41
Figura 4.14 Exportar registros 42

Figura 4.15 Creación de archivo con extensión .CAP 42
Figura 4.16 Aircrack-ng en modo gráfico 43
Figura 4.17 Aircrack-ng 49
Figura 4.18 Obtención clave con cifrado WEP 50
Figura 4.19 Obtención clave con cifrado WPA 52

CAPÍTULO V

Figura 5.01Computador portátil HP 56
Figura 5.02 Tarjeta USB Linksys 56
Figura 5.03 Logo Elecdor S.A 57
Figura 5.04 Red estructurada Elecdor S.A 60
Figura 5.05 Router Linksys WPA54G 61
Figura 5.06 Configurando CommView for WiFi en Elecdor S.A 61
Figura 5.07 Explorador de redes WiFi 62
Figura 5.08 Selección de red WiFi 62
Figura 5.09 Captura de red WiFi 63
Figura 5.10 Archivo CommView de captura de la red 63
Figura 5.11 Visor de Registros de captura de datos 64
Figura 5.12 Guardando captura obtenida 64
Figura 5.13 Usando Aircrack-ng 65
Figura 5.14 Red de la empresa usando la tarjeta inalámbrica USB 68
Figura 5.15 Ingreso de clave WiFi de la red 69
Figura 5.16 Se agrega automáticamente la red WiFi de la empresa 69
Figura 5.17 Propiedades de la red WiFi 70
Figura 5.18 Logo EN CAJAS 71
Figura 5.19 Red estructurada EN CAJAS 72
Figura 5.20 Router D-Link DIR-280..... 73
Figura 5.21 Explorador de redes WiFi 74
Figura 5.22 Selección de red WiFi 74
Figura 5.23 Captura de red WiFi 75
Figura 5.24 Visor de Registros de captura de datos 75
Figura 5.25 Guardando captura obtenida 76
Figura 5.26 Usando Aircrack-ng 76

INDICE DE CUADROS

CAPÍTULO I

Cuadro 1.01 Principales Estándares 802.11 – Cuadro Comparativo 8

CAPÍTULO II

Cuadro 2.01 Nivel de Soluciones 802.1X/EAP – Cuadro Comparativo..... 16
Cuadro 2.02 Puerta XOR – Tabla de verdad 17

CAPÍTULO III

Cuadro 3.01 WPA vs WPA2 – Tabla comparativa 33

CAPÍTULO IV

Cuadro 4.01 Opciones Airodump-ng 46
Cuadro 4.02 Opciones Airdecap-ng 47

CAPÍTULO V

Cuadro 5.01 Requerimientos de Hardware 56
Cuadro 5.02 Router de la empresa Elecdor S.A 61
Cuadro 5.03 Router de la empresa EN CAJAS 73
Cuadro 5.04 Cuadro Resumen Ataques de Red 78

INDICE DE CAPTURAS

CAPÍTULO IV

Captura 4.01 Puntos de acceso encontrados con Airodump-ng 45
Captura 4.02 AP encontrados de la captura de registros .CAP 50
Captura 4.03 Clave encontrada de red con cifrado WEP 51
Captura 4.04 AP encontrados de la captura de registros .CAP 53
Captura 4.05 Clave encontrada de red con cifrado WPA 53
Captura 4.06 Opciones Aircrack-ng 54

CAPÍTULO V

Captura 5.01 Redes encontradas durante la captura de paquetes de datos 66
Captura 5.02 Selección de red a descifrar 67
Captura 5.03 Clave encontrada de la red WiFi de Elecdor S.A 68
Captura 5.04 Selección de red a descifrar 77
Captura 5.05 Clave encontrada de la red WiFi de EN CAJAS 77

CAPÍTULO I

1. Redes Inalámbricas

Recientemente, el uso de redes inalámbricas ha incrementado en pequeñas y medianas empresas, locales de centros comerciales y en diversos negocios, gracias a su bajo costo de instalación, su fácil configuración y la capacidad de diferentes dispositivos que pueden interconectarse entre sí vía inalámbrica en la actualidad.

El crecimiento y evolución del uso de redes Wi-Fi ha sido tan importante que el estudio a continuación indicará las diferentes tecnologías que usa, tanto como sus ventajas y desventajas.

Figura 1.01 Redes inalámbricas en el mundo

Fuente: http://educacionmiguel.blogspot.es/1216605480/

El significado de Wi-Fi no es abreviatura de Wireless Fidelity, no es un acrónimo ni tiene significado. El término "Wi-Fi" y el logotipo fueron creados por la agencia pública Interbrand Corporation a petición de la WECA (Wireless Ethernet Compatibility Alliance), utilizando una palabra que fuese corta, comercial y fácil de recordar, pareciéndose mucho al estilo ying-yang, que es un concepto basado en la dualidad de todo lo existente en el universo.

Figura 1.02 Logo WiFi

Fuente: http://www.wi-fi.org/index.php

Wi-Fi Alliance certificó el estándar 802.1x basado en servidores RADIUS y más tarde el estándar 802.11i basado en WPA y WPA2, para mejorar el nivel de seguridad.

1.1 Crecimiento de las redes inalámbricas

Durante éstos últimos años, las redes inalámbricas han tomado un protagonismo cada vez más fuerte, basta con indicar que al adquirir una WNIC (tarjeta de red inalámbrica) y conectada en un PC, se puede verificar en cualquier lugar donde nos situemos, la WNIC detecta la existencia de algún AP asociado a una red inalámbrica, o simplemente al revisar con un dispositivo móvil (laptop, celulares, iPhone, iPad, etc.) que posea Wi-Fi (Wireless Fidelity), se distinguirá redes inalámbricas cercanas con y sin seguridad.

Varios motivos han favorecido en el incremento de este tipo de tecnología para la transmisión de información entre estaciones móviles, entre ellas:

- ✓ **Reducción de costos en el hardware necesario:** solamente se necesita uno o varios puntos de acceso dependiendo del área de cobertura que se quiera que alcance la red, y disponer de tarjetas inalámbricas para cada uno de los dispositivos que formen parte de la

red. Estos puntos de acceso se conectarían al resto de la LAN cableada, así como al resto del Internet por medio del sistema de distribución (DS) en una topología ESS (Extended Service Set). Se podría reducir mayormente los costos en equipamiento en el caso que se quiera montar una red "ad-hoc" o BSS, en la que solo haría falta las tarjetas de red inalámbricas para los equipos debido a que uno de ellos, (PC de sobremesa) podría de disponer de una tarjeta de red Ethernet con conexión a Internet, de modo que haría el papel de router para la red.

- ✓ **Movilidad:** los usuarios pueden conectarse a Internet sin necesidad de disponer una conexión física con cables, por lo tanto permite la movilidad de los usuarios dentro del área de cobertura de la WLAN manteniendo el ancho de banda y sin perder conexión.

- ✓ **Instalación rápida:** debido a que no se debe realizar un cableado estructurado a través de paredes, techos, etc., e instalando tomas de acceso, conexiones, etc.

- ✓ **Flexibilidad:** es posible instalar nuevas WLANs o cambiar la configuración ya existente, de una manera rápida y sencilla.

- ✓ **Escalabilidad:** se puede hacer una instalación empezando por pequeñas redes "ad-hoc" de unas pocas estaciones, e ir ampliándolas sucesivamente, hasta llegar a hacerlas muy grandes por medio de la utilización de puentes inalámbricos, utilizados para la interconexión de WLANs en emplazamientos diferentes y situados a una distancia considerable (generalmente no más de 10 KM) pudiendo suponer un ahorro frente al alquiler de circuitos telefónicos.

Figura 1.03 Router Linksys WAP54G

Fuente: http://www.linksysbycisco.com/LATAM/es/products/Adapters

Figura 1.04 Tarjeta inalámbrica Linksys

Fuente: http://www.linksysbycisco.com/LATAM/es/products/Routers

Figura 1.05 Access Point D-Link

Fuente: http://www.dlink.com/solutionFlashes/?type=1

1.2 Normativa IEEE 802.11

Existen varios estándares de la norma IEEE 802.11 aprobados hasta la actualidad. A continuación se resumen aquellos que se han considerado más relevantes para el desarrollo de este documento:

Figura 1.06 Logo WiFi Certified

Fuente: http://www.wi-fi.org/secure_your_wi-fi

1.2.1 Estándar 802.11

En 1997 se publicó originalmente el estándar IEEE (el Instituto de Ingeniería Eléctrica y Electrónica) - (Institute for Electrical and Electronic Engineering IEEE) 802.11, que especifica 2 velocidades de transmisión teóricas de 1 y 2 Megabit por segundo (Mbit/s) que se transmiten por señales infrarrojas (IR) en la banda ISM a 2.4GHz.

El estándar original también define el protocolo CSMA/CA como método de acceso. Se ocupa una parte importante de la velocidad de transmisión teórica en las necesidades de esta codificación para mejorar la condición bajo condiciones ambientales diversas, el cual introdujo dificultades de interoperabilidad entre equipos de diferentes marcas. Estas y otras debilidades fueron corregidas en el estándar 802.11b, que fue la primera en alcanzar amplia aceptación entre los usuarios.

1.2.2 802.11a

La revisión 802.11a del estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5Ghz y utiliza 52 subportadoras OFDM con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar practico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s. 802.11a posee 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

Conociendo que la banda de 2.4Ghz tiene gran uso (es la banda usada por los teléfonos inalámbricos y los hornos microondas entre otros dispositivos), al usar la banda de 5Ghz representa una ventaja ya que se presenta con menos interferencia. Sin embargo, el uso de esta banda tiene sus desventajas, dado que restringe el uso de los equipos 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; esto significa también que los equipos que trabajan con este

estándar no tienen un largo alcance como los del estándar 802.11b dado que sus ondas son más fácilmente absorbidas.

1.2.3 802.11b

La revisión 802.11b del estándar original fue ratificada en 1999. Este estándar tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido del estándar original. El estándar 802.aab funciona en la banda de 2.4GHz. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, la velocidad máxima de transmisión en la práctica con este estándar es de aproximadamente de 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

Los productos de la 802.11b aparecieron rápidamente en el mercado, y los diferentes dispositivos fueron fácilmente actualizados para soportar las mejoras del 802.11b. El incremento en el uso del 802.11b junto con sustanciales reducciones de precios causo una rápida aceptación del 802.11b como la tecnología Wireless LAN definitiva.

El estándar 802.11b es usualmente usado en configuraciones punto y multipunto como en el caso de los AP que se comunican con una antena omnidireccional con uno o más clientes que se encuentran en el área de cobertura alrededor del AP.

El rango típico en interiores es de 32 metros a 11 Mbit/s y 90 metros a 1 Mbit/s. Con antenas de alta ganancia externas el protocolo puede ser utilizado en arreglos fijos punto a punto típicamente rangos superiores a 8 Km incluso en algunos casos de 80 a 120 km siempre que haya línea de visión. Esto se hace usualmente para reemplazar el costoso equipo de líneas o el uso de quipos de comunicaciones de microondas.

La tarjetas de 802.11b pueden operar a 11 Mbit/s pero pueden reducirse hasta 5.5, 2 o 1 Mbit/s en el caso de que la calidad de la señal se convierta en un problema. Dado que las tasas bajas de transferencia de información usan

algoritmos menos complejos y más redundantes para proteger los datos son menos susceptibles a la corrupción debido a la atenuación o interferencia de la señal. Sean han hecho extensiones del protocolo 802.11b para incrementar su velocidad a 22, 33, 44 Mbit/s pero estas no han sido ratificadas por la IEEE. Muchas compañías llaman a estas versiones mejoradas 802.11b+. Estas extensiones han sido ampliamente obviadas por los desarrolladores del 802.11g que tiene tasas de transferencia a 54 Mbit/s y es compatible con 802.11b.

1.2.4 802.11g

En junio del 2003, se ratifico un tercer estándar de modulación, el 802.11g. Este utiliza la banda de 2.4GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica de 54 Mbit/s o cerca de 24,7 Mbit/s de velocidad real de transferencia, similares a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias.

Los equipos que trabajan bajo el estándar 802.11g llegaron al mercado muy rápidamente, incluso antes de su ratificación. Esto se debió en parte a que para construir equipos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar b. Muchos de los productos de banda dual 802.11a/b se convirtieron de banda dual a modo triple soportando a (a, b y g) en un solo adaptador móvil o AP. El estándar 802.11g, a pesar de su mayor aceptación, sufre de la misma interferencia de 802.11b en el rango ya saturado de 2.4 GHz por dispositivos como hornos microondas, dispositivos bluetooth y teléfonos inalámbricos.

1.2.5 802.11n

En enero del 2004, la IEEE anuncio un grupo de trabajo 802.11 para revisar una nueva versión del estándar donde la velocidad real de transmisión tendría que llegar a los 500 Mbps (lo que significa que las velocidades teóricas de

transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b.

En septiembre del 2009, IEEE aprobó finalmente el estándar Wi-Fi de alto rendimiento 802.11n. Esta nueva modificación de la norma 802.11, se diseñó para resolver una necesidad actual de la industria de la comunicación frente a la creciente demanda que hay en los hogares, empresas y WLANs públicas, con el aumento de las transferencias de pesados archivos que llegan con esta próxima generación de aplicaciones multimedia.

El estándar 802.11n, permite unas redes WLAN con un mejor rendimiento, un mejor despliegue de redes WLAN escalables, y una perfecta coexistencia con los sistemas e implementaciones de seguridad**.**

802.11n se construye basándose en las versiones previas del estándar 802.11 añadiendo MIMO (Multiple-Input Multiple-Output). MIMO utiliza múltiples transmisores y antenas receptoras permitiendo incrementar el tráfico de datos.

Principales Estándares 802.11

Protocolo	Año publicación	Frecuencia	Velocidad transmisión	Velocidad transmisión (Max)	Rango (interno)
802.11	1997	2.4-2.5 GHz	1 Mbit/s	2 Mbit/s	?
a	1999	5.15-5.35/5.47-7.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	30 m
b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	30 m
g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	30 m
n	2008	2.4 GHz o 5 GHz	200 Mbit/s	540 Mbit/s	50 m

Cuadro 1.01 Cuadro comparativo

Autor: Andrés Serrano Flores

1.3 Topologías

Según especificaciones del estándar 802.11, se tiene 2 tipos de topologías:

- Redes "ad-hoc"
- Redes de infraestructura

1.3.1 Redes "ad-hoc"

Redes sin infraestructura, es el modelo más simple de red inalámbrica, consiste en colocar varias estaciones de trabajo con una tarjeta inalámbrica próximas, que se encuentren dentro de una misma área.

Es una red formada sin ninguna administración central o no hay un nodo central, sino que consta de nodos móviles que usan una interface inalámbrica para enviar paquetes de datos.

Los dispositivos descubren otros artefactos cercanos para formar la red, el tipo de conexión es establecida por la duración de una sección. Los dispositivos pueden buscar nodos fuera del área de alcance conectándose con otros nodos que se encuentren a su alcance.

Figura 1.07 Redes ad-hoc

Fuente: http://www.debahia.com/tecnologia/wireless_1.html

Se pueden interconectar varios dispositivos de un mismo usuario (celular, IPAD, laptop, etc.); los dispositivos ad-hoc pueden también retransmitir tráfico entre dispositivos que están fuera de su alcance. No se necesita de un router o AP.

Uno de los principales motivos de preocupación en ésta topología de red es la seguridad, uno no sabe si algún usuario está revisando el tráfico mediante un

nodo de reenvío, o si el usuario del otro extremo es realmente la persona que dice ser; la confianza en una red ad-hoc es un problema fundamental.

No es posible confiar en el medio, la única elección que queda es usar la criptografía, lo que obliga en confiar en las claves criptográficas usadas.

1.3.2 Redes de infraestructura

Son redes basada en la existencia de uno o varios AP cada uno de los cuales definirá una celda o BSS (Basic Service Set) y la unión de todas estas celdas definirá lo que se conoce como ESS (Extended Service Set). La interconexión de APs se podrá realizarse por medio de una LAN (Local Area Network) convencional o bien por radio (una interconexión sin cables). Cada una de las celdas a las que dan cobertura los APs permite crear redes que den cobertura en zonas amplias (almacenes, edificios, universidades, etc.) permitiendo a los usuarios, la conexión a la red, desde prácticamente cualquier punto así como la movilidad pudiéndose desplazar por dentro de la red sin perder conectividad.

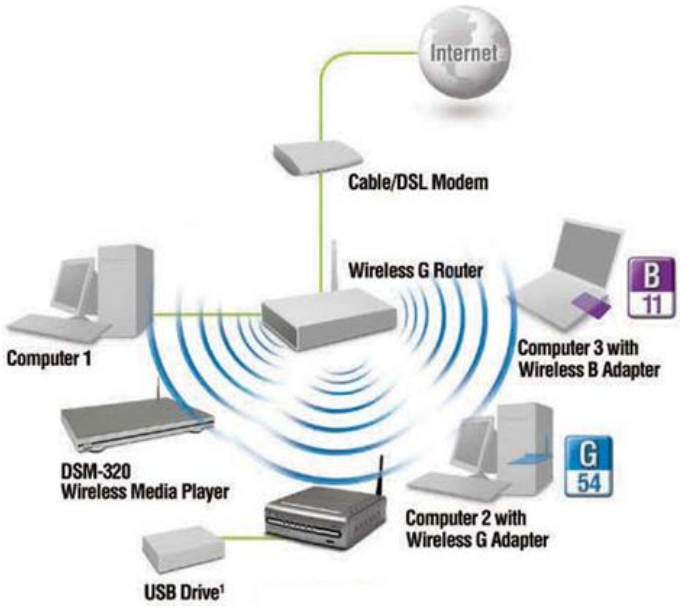


Figura 1.08 Redes estructuradas

Fuente: http://corporacionsiatec.com/proyects/systel/servicios.php?page=1&subpage=1

Las redes inalámbricas son una solución que nos libran de la dependencia de un cableado estructurado que permanece en un lugar fijo, con la capacidad de un movimiento mínimo, y solamente realizar una conexión correcta en los únicos puntos donde existe una toma de conexión de red, de modo que esto se convierte en su mayor ventaja, al permitir movilidad e interconexión sin cables, pero también muestra su mayor problema, como se ha revisado, que es la seguridad.

Primeramente, se debe tomar en cuenta que los ordenadores están frecuentemente enviando información, e incluso anuncian su presencia a cualquier otro dispositivo que pase dentro de su radio de alcance, lo que hace que sea sencilla la manera de espiar la red, por lo tanto, al contrario de una red cableada, donde se necesita un acceso físico al edificio u oficina donde se encuentra la red interna que trata de corromper, las señales de radio utilizadas por los dispositivos sin cables navegan con libertad a través del aire, al alcance de aquel que esté dispuesto a interceptarlas.

Un intruso que quiera aprovecharse de la conexión de red instalada, que trate de revisar los datos que se intercambian entre las estaciones que forman la WLAN, o lo que podría ser peor, que utilice la red como punto de ataque para cometer delitos informáticos contra otros objetivos, lo podrá hacer sin tener un medio físico en el lugar donde esté ubicada dicha red, lo podrá hacer tranquilamente desde casa de un vecino o en algún lugar contiguo, que este a una distancia no demasiado larga a la red objetivo, con el problema adicional de que la intercepción de paquetes de datos no será detectada y el atacante puede actuar sin el conocimiento del administrador de la red, lo que dará más tiempo a la hora de planificar la estrategia de ataque.

Se han desarrollado varias estrategias para intentar evitar estos problemas, la mayoría basadas principalmente en el cifrado de las comunicaciones (WEP, WPA, WPA2). Diversos estudios han demostrado la debilidad de estos mecanismos de seguridad. También existen otro tipo de medidas de protección como el filtrado de direcciones MAC, o bien medidas de protección más robustas basadas en el estándar 802.1x que permite la autenticación y

autorización de usuarios, a través del protocolo extendido de autorización (EAP). Todas estas medias de protección, y algunas adicionales se pasaran a indicarse más adelante analizando las ventajas e inconvenientes de cada una.

CAPÍTULO II

2. Seguridad en Redes Inalámbricas

Si se habla de redes inalámbricas, es necesario hablar de seguridad; una red wireless es más susceptible a ataques de gente inescrupulosa lo que ha provocado la creación de protocolos de seguridad y tecnologías para poder prevenirlos.

2.1 Protocolos de seguridad

Un protocolo de seguridad define las reglas que gobiernan las comunicaciones ya sean éstas telefónicas, de correo electrónico, de radio, etc., o de dispositivos físicos como tarjetas de crédito, pasajes, cédulas, etc., diseñadas para que el sistema pueda soportar ataques de carácter malicioso.

Los protocolos son diseñados bajo ciertas primicias con respecto a los riesgos a los cuales el sistema está expuesto.

2.1.1 EAP (Extensible Authentication Protocol)

Es el *Protocolo de Autentificación Extensible* para llevar a cabo las tareas de autentificación, autorización y contabilidad.

El proceso de Autenticación EAP es el siguiente:

- Supplicant (Suplicante): es el usuario o cliente que desea ser autenticado
- Autenticador: es el elemento intermedio que suministrará el servicio una vez el "supplicant" haya sido autenticado.
- Servidor de Autenticación: es el Servidor responsable de realizar una correcta autenticación del "supplicant".

1. El autenticador envía un paquete de "EAP-Request/Identity" al supplicant tan pronto como detecte que el acoplamiento es activo.

2. El supplicant envía un paquete de "EAP-Response/Identity" al Autenticador, que pasa directamente al servidor de autenticación.

3. El servidor de autenticación envía un desafío al autenticador. El Autenticador desempaqueta el contenido del paquete IP, lo empaqueta de nuevo en EAPOL y lo envía al supplicant.

4. El supplicant responde el desafío vía el autenticador y pasa la respuesta al servidor de autenticación.

5. Si el supplicant proporciona identidad apropiada, el servidor de autenticación responde con un mensaje de éxito al Autenticador, que es pasado así mismo al supplicant. El Autenticador permite a partir de este momento el acceso al supplicant.

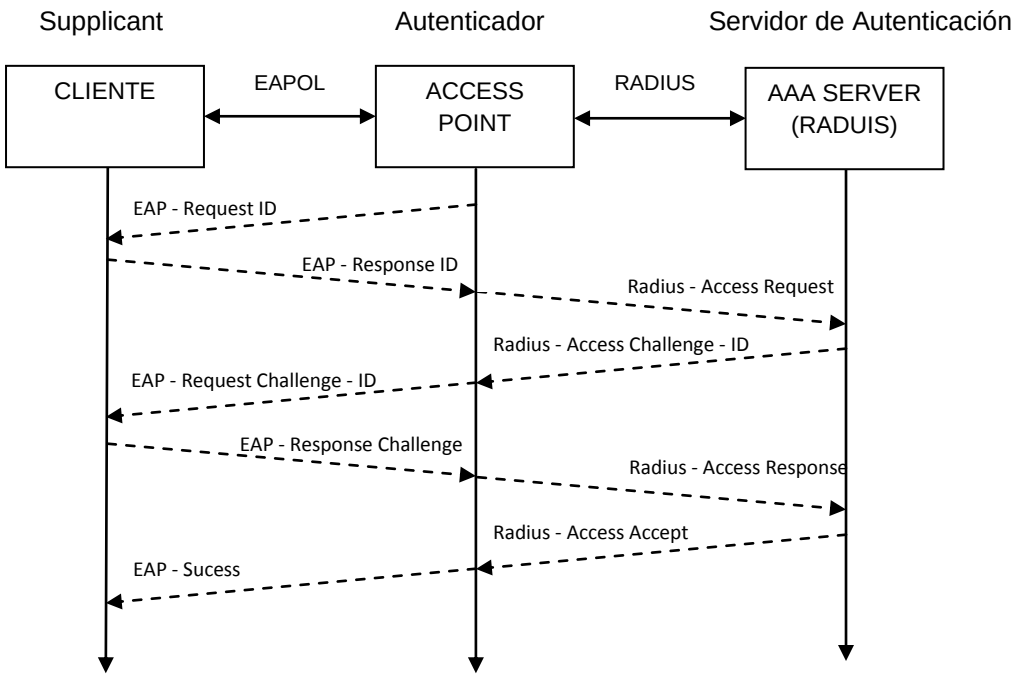


Figura 2.01 Autenticación EAP

Autor: Andrés Serrano Flores

Dicho protocolo permite varios métodos de autenticación como EAP-MD5, EAP-TLS y otros métodos. Las modalidades de autenticación pueden ser por certificados de seguridad o por contraseñas.

2.1.1.1 EAP por contraseñas

- EAP-MD5: utiliza nombre de usuario y contraseña para autenticación. La contraseña es transmitida de forma cifrada a través del algoritmo MD5. No suministra un nivel de protección alto pues puede sufrir ataques de "diccionario", es decir, un atacante puede enviar varias contraseñas cifradas hasta encontrar una válida. No hay modo de autentificar el servidor, y no genera claves WEP dinámicas.

- LEAP: utiliza un usuario y contraseña, y soporta claves WEP dinámicas. Por ser una tecnología propietaria de CISCO, exige que los equipos sean de Cisco y que el servidor RADIUS sea compatible con LEAP.

- EAP-SPEKE: utiliza el método SPEKE (Simple Password-authenticated Expotential Key Change), que permite al cliente y servidor compartir una contraseña secreta, lo que proporciona un servicio de autenticación mutua sin el uso de certificados de seguridad.

2.1.1.2 EAP por certificados de seguridad

- EAP-TLS: requiere la instalación de certificados de seguridad en el servidor y en los clientes. Proporciona autenticación mutua, es decir, el servidor autentifica al cliente y viceversa utilizando el protocolo TLS (Transparent Layer Substrate).

- EAP-TTLS: es similar al EAP-TLS; sin embargo, el certificado solamente se instala en el servidor, lo que permite la autentificación del servidor por parte del cliente. La autentificación del cliente por parte del servidor se hace después de establecer una sesión TLS utilizando otro método como PAP, CHAP, MS-CHAP o MS-CHAP v2.

- PEAP: es similar al EAP-TTLS, pues solamente requiere certificados de seguridad en el servidor. Fue desarrollado por Microsoft, Cisco y RSA Security.

Nivel de Soluciones 802.1X/EAP

	EAP-MD5	LEAP (Cisco)	EAP-TLS (MS)	EAP-TTLS (Funk)	EAP-PEAP
Solución de seguridad	Estándar	Patente	Estándar	Estándar	Estándar
Certificados - Cliente	No	N/A	Sí	No (Opcional)	No (Opcional)
Certificados - Servidor	No	N/A	Sí	Sí	Sí
Credenciales de Seguridad	Ninguna	Deficiente	Buena	Buena	Buena
Soporta Autentificación de Base de Datos	Requiere borrar la base de datos	Active Directory, NT Domains	Active Directory	Active Directory, NT Domains, Token Systems, SQL, LDAP	Active Directory
Intercambio de llaves dinámicas	No	Sí	Sí	Sí	Sí
Autentificación Mutua	No	Sí	Sí	Sí	Sí

Cuadro 2.01 Cuadro Comparativo

Autor: Andrés Serrano Flores

2.1.2 SSID (Service Set Id)

SSID es un código alfanumérico que identifica una red inalámbrica. Cada fabricante utiliza un mismo código para sus componentes de fábrica. Para aumentar la seguridad de la red, se debe cambiar este nombre y deshabilitar la opción de "broadcast SSID" al punto de acceso. Cuando el "broadcast SSID" está habilitado, el punto de acceso periódicamente envía el SSID a la red

permitiendo que otros clientes puedan conectarse a la red. En redes de acceso público es deseable que se realice la propagación del SSID, para que cualquier persona pueda conectarse a la red. Como el SSID puede ser extraído del paquete transmitir a través de la técnica de "sniffing" no ofrece buena seguridad para la red. Aún así, se debe alterar el nombre para evitar que otros usen la misma red, accidentalmente.

2.2 WEP (Wired Equivalency Privacy)

Como indica el nombre, este protocolo tiene la intención de suministrar el mismo nivel de privacidad de una red con cable. Es un protocolo de seguridad basado en el método de criptografía RC4 que utiliza criptografía de 64 bits o 128 bits. Ambas utilizan un vector de inicialización de 24 bits. Sin embargo, la clave secreta tiene una extensión de 40 bits o de 104 bits. Todos los productos Wi-Fi soportan la criptografía de 64 bits, sin embargo no todos soportan la criptografía de 128 bits. Además de la criptografía, también utiliza un procedimiento de redundancia cíclica en el patrón CRC-32, utilizado para verificar la integridad del paquete de datos. El paradigma de este tipo de algoritmos es el *One Time Pad*, que funciona aplicando XOR (or-exclusiva) a cada bit de la entrada junto con otro generado aleatoriamente para obtener cada bit de la salida. La ecuación característica que describe el comportamiento de la puerta XOR es $F=A \oplus B$.

Puerta XOR

Entrada A	Entrada B	Salida $A \oplus B$
0	0	0
0	1	1
1	0	1
0	0	0

Cuadro 2.02 Tabla de Verdad

Autor: Andrés Serrano Flores

La base del WEP se encuentra en la operación lógica XOR, que presenta la propiedad de que si se aplica dos veces el XOR a un valor se obtendrá el valor original.

En su primera fase, RC4 desordena una secuencia de números consecutivos, este proceso de inicialización del algoritmo es donde se utiliza la clave WEP. La segunda parte del algoritmo genera la secuencia de números pseudoaleatorios, con el cual el protocolo WEP realizará el XOR con la información que desea encriptar.

El WEP no protege la conexión por completo sino solamente el paquete de datos. El protocolo WEP no es solamente intocable, pues ya existen programas capaces de quebrar las claves de criptografía en el caso de que la red sea monitorizada durante un tiempo considerable como se verá más adelante.

2.3 WPA (Wi-Fi Protected Access)

Fue elaborado para solucionar los problemas de seguridad del WEP. El WPA posee un protocolo denominado TKIP (Temporal Key Integrity Protocol) con un vector de inicialización de 48 bits y una criptografía de 128 bits. Con la utilización del TKIP la llave es alterada en cada paquete y sincronizada entre el cliente y el Access Point, también hace uso de autenticación del usuario por un servidor central.

2.4 WPA2

Es una mejoría del protocolo WPA que utiliza el algoritmo de encriptación denominado AES (Advanced Encryption Standard).

2.5 Cifrados AES y TKIP

Ambos cifrados son utilizados en el protocolo de seguridad WPA/WPA2.

2.5.1 AES (Advanced Encryption Standard)

Como se ha revisado, éste algoritmo es usado en el protocolo de seguridad WPA y es el más conocido entre los usuarios de routers. Este cifrado se puede implementar tanto en sistemas de hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variables, tenemos AES de 128bits, de 192bits y de 256bits.

El resultado intermedio del cifrado constituye una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de bucles de cifrado basado en operaciones matemáticas (sustituciones no lineales de bytes, desplazamiento de filas de la matriz, combinaciones de las columnas mediante multiplicaciones lógicas y suma XOR en base a claves intermedias).

Con referencia a la seguridad, AES tiene 10 rondas para llaves de 128bits, 12 rondas para llaves de 192bits y 14 rondas para laves de 256bits.

En el año 2006, los mejores ataques conocidos fueron el de 7 rondas para claves de 128bits, 8 rondas para llaves de 192bits y 9 rondas para claves de 256bits, esto genera una preocupación entre algunos criptógrafos porque se cree que el margen entre el número de rondas especificado en el cifrador y los mejores ataques conocidos es muy pequeño. Otra preocupación es la estructura de AES, a diferencia de la mayoría de cifradores de bloques, AES tiene una descripción matemática muy ordenada.

Hay que tener en cuenta que AES es usado en los cifrados Wireless de los routers de los hogares u oficinas como método de cifrado (no como clave), ya que en los routers se puede usar una clave estática o una dinámica mediante un servidor RADIUS.

Los algoritmos de cifrado de bloque como AES separan el mensaje en trozos de tamaño fijo, por ejemplo de 64 0 128 bits. La forma en que se gestionan estos bloques de mensaje, se denomina "modo de cifrado".

Por ejemplo, existe el AES-CBC, AES-CFB y AES-OFB

- **CBC (Cipher-block chaining):** a cada bloque de texto plano se le aplica la operación XOR con el bloque cifrado anterior antes de ser cifrado. De esta forma, cada bloque de texto cifrado depende de todo el texto en claro procesado hasta este punto. Como no se dispone de un texto cifrado con el que combinar el primer bloque, se usa un vector de inicialización IV (número aleatorio que puede ser públicamente conocido). La desventaja es que el cifrado es de forma secuencial y por tanto no puede ser paralelizado.

- **OFB (Output feedback):** se generan bloques de flujo de claves, que son operados con XOR y el texto en claro para obtener el texto cifrado. Al igual que con otras unidades de flujo de cifrado, al intercambiar un bit en el texto cifrado produce texto cifrado con un bit intercambiado en el texto plano en la misma ubicación. También se usa un vector de inicialización para el primer bloque.

- **CFB (Cipher feedback):** se hace igual que en OFB, pero para producir el keystream cifra el último bloque de cifrado, en lugar del último bloque del keystream como hace OFB. Un bit erróneo en el texto cifrado genera 1+64/m bloques de texto claro incorrectos (siendo m la longitud del flujo en el que se divide el bloque). El cifrado no puede ser paralelizado, sin embargo el descifrado sí.

2.5.2 TKIP (Temporal Key Integrity Protocol)

Es también llamado hashing de clave WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. WPA tiene TKIP, que utiliza el mismo algoritmo que WEP, pero construye claves en una forma diferente para cada trama.

TKIP es una solución temporal que resuelve el problema de reutilización de clave de WEP. WEP utiliza periódicamente la misma clave para cifrar los datos.

El proceso de TKIP comienza con una clave temporal de 128 bits que es compartida entre los clientes y los puntos de acceso. Combina la clave temporal con la dirección MAC del cliente. Luego agrega un vector de inicialización relativamente largo, de 16 octetos, para producir la clave que cifrará los datos. Este procedimiento asegura que cada estación utilice diferentes streams claves para cifrar los datos. El hashing de clave WEP protege a los vectores de inicialización (IVs) débiles para que no sean expuestos haciendo hashing del IV por cada paquete.

Utiliza el RC4 para realizar el cifrado, que es lo mismo que el WEP. Sin embargo, una gran diferencia con el WEP es que cambia las claves temporales cada 10.000 paquetes. Esto proporciona un método de distribución dinámico, lo que mejora significativamente la seguridad de la red.

Una ventaja de usar TKIP es que las compañías que tienen puntos de acceso basados en WEP y NICs de radio pueden actualizarse a TKIP a través de patches de firmware relativamente simples.

Las mejoras de TKIP, como MIC, proveen claves WEP más fuertes. MIC evita los ataques de bit-flip en paquetes cifrados. Durante un ataque bit-flip, un intruso intercepta un mensaje cifrado, lo altera levemente y lo retransmite. El receptor acepta el mensaje retransmitido como legítimo. El controlador y el firmware del adaptador cliente deben soportar la funcionalidad del MIC, y MIC debe estar activo en el punto de acceso. Las mejoras de TKIP, como MIC y hashing de clave WEP pueden ser activados usando claves WEP estáticas. No necesitan un servidor RADIUS para funcionar.

CAPÍTULO III

3. Cifrados WEP, WPA, WPA2

Entre los cifrados que se utilizan en la actualidad en diferentes routers y AP encontramos: WEP, WPA personal, WPA enterprise, WPA2 personal y WPA2 enterprise.

3.1 WEP

WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable) es el algoritmo opcional de seguridad incluido en la norma IEEE 802.11. Según el estándar, los objetivos WEP son de proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

3.1.1 Funcionamiento

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red, esto genera algunos inconvenientes. La clave está almacenada en todas las estaciones, aumentando la posibilidad de que sea comprometida, y la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que, en la mayoría de ocasiones, conlleva a que la clave se la cambie poco o nunca.

El algoritmo de encriptación utilizado es RC4 con claves (*seed*), según el estándar, de 64 bits. Estos 64 bits están formados por 24 bits correspondientes al vector de inicialización más 40 bits de la clave secreta. Los 40 bits son los que se deben distribuir manualmente. El vector de inicialización (IV), en cambio, es generado dinámicamente y debería ser diferente para cada trama.

El objetivo perseguido con el IV es cifrar con claves diferentes para impedir que un posible atacante pueda capturar suficiente tráfico cifrado con la misma clave y terminar finalmente deduciendo la clave. Como es lógico, ambos extremos deben conocer tanto la clave secreta como el IV. Lo primero se sabe ya que es conocido puesto que está almacenado en la configuración de cada elemento de red. El IV, en cambio, se genera en un extremo y se envía en la propia trama al otro extremo, por lo que también será conocido. Se observa que al viajar el IV en cada trama es sencillo de interceptar por un posible atacante.

El algoritmo de encriptación de WEP es el siguiente:

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).
2. Se concatena el ICV al mensaje que se quiere enviar, y se concatena la clave secreta a continuación del IV formado la semilla (*seed*).
3. El PRNG (Pseudo-Random Number Generator) de RC4 genera una secuencia de caracteres pseudoaleatorios (keystream - Secuencia de RC4), a partir del *seed,* de la misma longitud que los bits obtenidos en el punto 2.
4. Se calcula la OR exclusiva (XOR) de los caracteres del punto 2 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

Algoritmo de Encriptación WEP

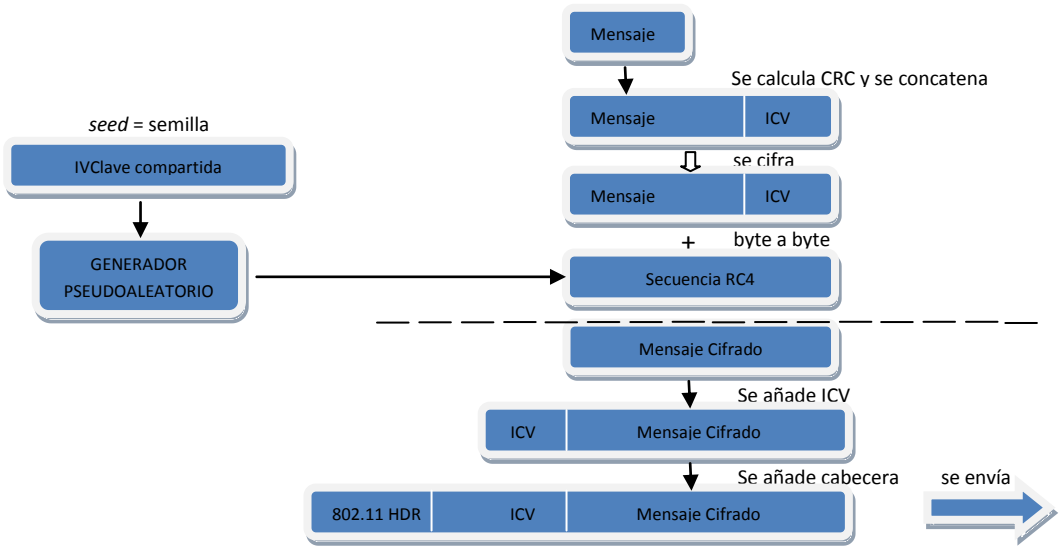


Figura 3.01 Cifrado WEP

Autor: Andrés Serrano Flores

El algoritmo para descifrar es parecido al detallado anteriormente. Debido a que el extremo conocerá IV y la clave secreta, tendrá entonces el *seed* y con ello podrá generar el *keystream*. Realizando el XOR entre los datos recibidos y el *keystream* se obtendrá el mensaje sin cifrar (datos y CRC-32).

3.1.2 Vulnerabilidades WEP

Como se ha revisado, WEP posee algunas vulnerabilidades de seguridad, como la debilidad en el vector de inicialización IV y problemas con el algoritmo de encriptación RC4.

3.1.2.1 Fragilidad en el vector de inicialización IV

La implementación del vector de inicialización (IV) en el algoritmo WEP tiene varios problemas de seguridad. Para recordar, el IV es la parte que varía de la

clave (seed) para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

El estándar 802.11, sin embargo, no especifica cómo manejar el IV; el uso y manejo del IV queda abierto a los fabricantes de los productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama. Y esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún si se tiene en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado (2^24=16 millones aprox.), por lo que terminará repitiéndose en cuestión de minutos u horas. El tiempo será menor cuanto mayor sea la carga de red. Lo ideal sería que el IV no se repitiese nunca, pero como se ve, esto es imposible en WEP. La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencia, aleatoria, etc.) y de la carga de la red. Es trivial saber si dos tramas han sido cifradas con la misma clave, puesto que el IV se envía sin cifrar y la clave secreta es estática.

La longitud de 24 bits para el IV forma parte del estándar y no puede cambiarse. Actualmente existen implementaciones con claves de 128 bits (WEP2), sin embargo, en realidad lo único que se aumenta es la clave secreta (104 bits) pero el IV se conserva con 24 bits. El aumento de la longitud de la clave secreta no soluciona la debilidad del IV.

¿Qué sucede luego de haber capturado varias tramas con igual IV (*keystream*)? Se necesita conocer el mensaje sin cifrar de una de ellas. Al hacer el XOR entre un mensaje sin cifrar y el mismo cifrado, nos dará el keystream para ese IV. Al conocer el keystream asociado a un IV, se puede descifrar todas las tramas que usen el mismo IV. El problema es entonces conocer un mensaje sin cifrar, aunque esto no llega a ser muy complicado, ya

que existen tráficos predecibles o se los puede provocar (confirmaciones de RCP, mensajes ICMP y respuestas de eco, etc.).

Con lo que se ha descrito no se puede deducir la clave secreta, pero sí es posible generar una tabla con los IV de los que se conoce el *keystream*, lo que permitirá descifrar cualquier mensaje que tenga un IV contenido en la tabla.

Sin embargo, se puede llegar a más y deducir la clave secreta. Una vulnerabilidad reciente del protocolo WEP permite deducir la clave total conociendo parte de la clave (precisamente, el IV que es conocido). Para ello se necesita recopilar suficientes IVs y sus *keystreams* asociados obtenidos por el procedimiento indicado.

3.1.2.2 Debilidades en el algoritmo RC4

El protocolo WEP también padece de otros problemas además de los relacionados con el vector de inicialización y la forma de utilizar el algoritmo RC4.

Como se había descrito en párrafos anteriores, uno de los objetivos de WEP es proporcionar un mecanismo que garantice la integridad de los mensajes. Con este fin, WEP incluye un CRC-32 que viaja cifrado. Sin embargo, se ha demostrado que este mecanismo no es válido y es posible modificar una parte del mensaje y a su vez el CRC, sin necesidad de conocer el resto. Esto permitiría, como por ejemplo, modificar algún número de la trama sin que el destino se percatara de ello. En lugar del algoritmo de CRC se recomienda como ICV (*Integrity Check Value*) un algoritmo diseñado para tal fin como SHA1-HMAC.

El estándar IEEE 802.11 incluye mecanismo de autentificación de las estaciones basado en un secreto compartido. Para ello se utiliza la misma contraseña de WEP en la forma que se describe a continuación:

Una estación que quiere unirse a una red, solicita al punto de acceso autentificación. El punto de acceso envía un texto en claro a la estación y ésta lo cifra y se lo devuelve. El punto de acceso finalmente descifra el mensaje

recibido, comprueba que su ICV es correcto y lo compara con el texto que envió.

El mecanismo anterior de *autentificación de secreto compartido* tiene el problema de enviar por la red el mismo texto sin cifrar y cifrado con la clave WEP (esta clave coincide con la utilizada para asegurar la confidencialidad). El estándar es consciente de esta debilidad y aconseja no utilizar el mismo IV para el resto de transmisiones. Sin embargo, tanto si las implementaciones repiten ese IV como sino la repiten, el mecanismo ofrece información que podría ser aprovechada para romper la clave WEP utilizando las debilidades del vector de inicialización.

WEP no incluye autentificación de usuarios. Lo más que incluye es la autentificación de estaciones descrita (sólo aquellas estaciones que en su configuración tengan almacenada la clave WEP). El sistema de autentificación descrito es tan débil que el mejor consejo sería no utilizarlo para no ofrecer información extra a un posible atacante. En este caso tendríamos una *autentificación de sistema abierto* (sin autentificación).

Entre la larga lista de problemas de seguridad de WEP se encuentra también la ausencia de mecanismos de protección contra mensajes repetidos (*replay*). Esto permite que se capture un mensaje y se introduzca en la red en un momento posterior. El paquete podría ser, por ejemplo, el que contiene la contraseña de un usuario para utilizar un determinado servicio.

Todos los problemas comentados unidos a las características propias de WEP como es la distribución manual de claves y la utilización de claves simétricas, hacen que este sistema no sea apropiado para asegurar una red inalámbrica.

3.1.3 Alternativas a WEP

Las vulnerabilidades explicadas de WEP son motivos más que suficientes para utilizar otros mecanismos de seguridad en redes WLAN.

Aunque no forma parte del estándar, los fabricantes de productos Wi-Fi decidieron ofrecer la posibilidad de utilizar claves del doble de longitud (de 64

bits a 128 bits). WEP utilizado con claves de 128 bits es lo que se conoce generalmente como *WEP2*. Sin embargo, se debe observar que la longitud del vector de inicialización sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la clave secreta (de 40 bits a 104 bits). Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. Con todo lo descrito, se tiene que WEP2 no resuelve los problemas de WEP.

Otra variante de WEP utilizada en algunas implementaciones es *WEP dinámico*. En este caso se busca incorporar mecanismos de distribución automática de claves y de autentificación de usuarios mediante 802.1x/EAP/RADIUS. Requiere un servidor de autentificación (RADIUS normalmente) funcionando en la red. En el caso de que la misma clave (clave secreta + WEP) no se utilice en más de una trama, este mecanismo sería suficiente para compensar las principales debilidades de WEP.

Sin embargo, la solución preferida por las empresas como alternativa a WEP ha sido la utilización de VPNs, de la misma manera que se haría si los usuarios estuviesen conectados remotamente a la oficina. La tecnología de VPNs está suficiente probada y se considera segura, aunque no ha sido diseñada específicamente para redes WLAN.

Los mecanismos diseñados específicamente para redes WLAN para ser los sucesores de WEP son WPA y WPA2 (IEEE 802.11i).

3.2 WPA

WPA (*Wi-Fi Protected Access*, Acceso Protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

Las principales características de WPA son la distribución dinámica de claves, la utilización más robusta del vector de inicialización IV (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

En el cifrado WPA, los datos utilizan el algoritmo RC4 con una clave de 128 bits y un IV de 48 bits. Una de las mejoras sobresalientes es TKIP (Protocolo de Integridad de Clave Temporal).

Otra de las ventajas, además de ofrecer autenticación y cifrado, WPA ofrece mejorar la integridad de la carga útil. La verificación de redundancia cíclica (CRC) utilizada en WEP es insegura porque permite alterar la carga útil y actualizar el mensaje de verificación de redundancia cíclica sin necesidad de conocer la clave WEP; en cambio, WPA utiliza MIC. El MIC de WPA incluye un mecanismo que contrarresta los intentos de ataque para vulnerar TKIP y bloques temporales.

3.2.1 Funcionamiento

WPA puede funcionar en dos modos:

- **Con clave inicial compartida (PSK / Pre-Shared Key):** conocido también como WPA Personal, este modo está orientado para usuarios domésticos o pequeñas empresas. No requiere un servidor AAA, sino que se utiliza una clave compartida en las estaciones y punto de acceso. Al contrario que en WEP, esta clave sólo se utiliza como punto de inicio para la autentificación, pero no para el cifrado de datos.

- **Con servidor AAA, RADIUS normalmente:** conocido también como WPA Enterprise, este es el modo indicado para las empresas. Requiere un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad. Utiliza el estándar IEEE 802.1x, que proporciona un control de acceso a red basado en puertos para la autenticación y distribución de claves. El punto de acceso mantendrá el puerto bloqueado hasta que el usuario se autentifique, para este fin se ocupa el protocolo EAP y un servidor AAA (Authentication Authorization Accounting) como puede ser RADIUS. Si la autorización es positiva, entonces el punto de acceso abre el puerto. El servidor RADIUS puede contener políticas para ese usuario concreto que

podría aplicar el punto de acceso (como priorizar ciertos tráficos o descartar otros).

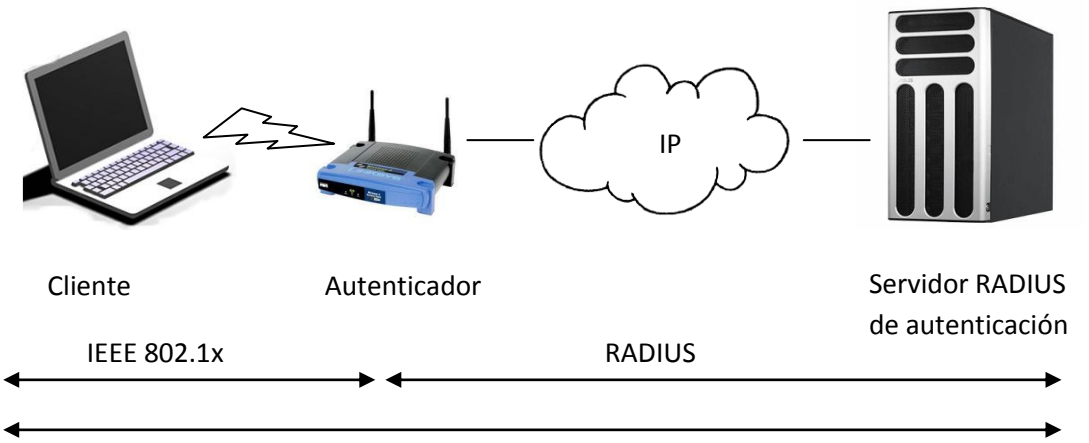


Figura 3.02 Arquitectura 802.1x/EAP

Autor: Andrés Serrano Flores

Los elementos que intervienen en un sistema 802.1x son:

- ✓ Autenticador: generalmente un AP, cuya función es forzar el proceso de autenticación y enrutar en tráfico a los dispositivos adecuados de la red.
- ✓ Solicitante: es el usuario que solicita el acceso a la red.
- ✓ Servidor de autentificación: lleva a cabo la autenticación de las credenciales de usuario.
- ✓ A continuación se muestra la arquitectura típica de un sistema de autenticación 802.1x/EAP.

Entre el Cliente y el AP (Autenticador) el protocolo utilizado es IEEE 802.1x. El protocolo entre el AP y el Servidor de autenticación no está definido en el estándar IEEE 802.1x ni en el estándar IEEE 802.11, en este caso se usa RADIUS. Cuando el cliente se conecta a un AP que soporta 802.1x comienza el intercambio de mensajes de autenticación EAP entre ambos para llevar a cabo la autenticación de usuario contra el servidor de autenticación.

3.2.2 WPA vs WEP

WPA soluciona la debilidad del vector de inicialización (IV) de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia que los fabricantes deben implementar. Los 48 bits permiten generar 2 elevado a 48 combinaciones de claves diferentes, lo cual parece un número suficientemente elevado como para tener duplicados.

El algoritmo utilizado por WPA sigue siendo RC4. La secuencia de los IV, conocida por ambos extremos de la comunicación, se puede utilizar para evitar ataques de repetición de tramas (*replay*).

Para la integridad de los mensajes (ICV), se ha eliminado el CRC-32 que se demostró inservible en WEP y se ha incluido un nuevo código denominado MIC.

Las claves ahora son generadas dinámicamente y distribuidas de forma automática por lo que se evita tener que modificarlas manualmente en cada uno de los elementos de red cada cierto tiempo, como ocurría en WEP.

Para la autentificación, se sustituye el mecanismo de autentificación de secreto compartido de WEP así como la posibilidad de verificar las direcciones MAC de las estaciones por la terna 802.1X / EAP / RADIUS. Su inconveniente es que requiere de una mayor infraestructura: un servidor RADIUS funcionando en la red, aunque también podría utilizarse un punto de acceso con esta funcionalidad.

3.3 WPA2

WPA2 (*Wi-Fi Protected Access 2*, Acceso Protegido Wi-Fi 2) es la versión mejorada del protocolo de seguridad WPA. WPA2 es una certificación de producto que está disponible a través de Wi-Fi Alliance, la cual certifica que el equipo inalámbrico es compatible con el estándar IEEE 802.11i.

La certificación de producto WPA2 sustituye formalmente a la Privacidad Equivalente por Cable (WEP) y al resto de características de seguridad del estándar original IEEE 802.11.

El objetivo de la certificación WPA2 es proporcionar compatibilidad para las características adicionales de seguridad obligatorias del estándar IEEE 802.11i que aún no se incluyen para los productos que admiten WPA.

3.3.1 Estándar 802.11i

En junio del 2004, el estándar 802.11i se ratificó para abordar el problema de la seguridad en redes inalámbricas. El estándar se basa en el algoritmo de cifrado TKIP, como el WEP, pero también admite el AES (Estándar de cifrado avanzado) que es mucho más seguro.

A diferencia del WPA, el WPA2 puede asegurar tanto en redes de infraestructura como en redes ad-hoc.

3.3.2 Características

WPA2 posee las siguientes características:

- WPA2 Enterprise, que utiliza la autenticación IEEE 802.1X y WPA2 Personal, que usa una clave previamente compartida (PSK).
- El estándar de cifrado avanzado (AES), que usa Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), proporciona confidencialidad de datos, autenticación del origen de datos e integridad de los datos en tramas inalámbricas.
- El uso opcional de la memoria caché de la clave maestra en pares (PMK) y de la memoria caché oportunista PMK. En el almacenamiento en caché de PMK, los clientes inalámbricos y los puntos de acceso inalámbricos almacenan en caché los resultados de las autenticaciones 802.1X. De este modo, el acceso es mucho más rápido cuando un cliente inalámbrico vuelve a un punto de acceso inalámbrico en el que el cliente ya se ha autenticado.
- El uso opcional de preautenticación. En la preautenticación, un cliente inalámbrico WPA2 puede realizar una autenticación 802.1X con otros puntos

de acceso inalámbrico en su intervalo cuando todavía está conectado a su punto de acceso inalámbrico.

WPA vs WPA2

	WPA	**WPA2**
Modo Enterprise	Autentificación: 802.1x / EAP	Autentificación: 802.1x / EAP
	Encriptación: TKIP /MIC	Encriptación: AES-COMP
Modo Personal	Autentificación: PSK	Autentificación: PSK
	Encriptación: TKIP /MIC	Encriptación: AES-COMP

Cuadro 3.01 Tabla comparativa

Autor: Andrés Serrano Flores

CAPÍTULO IV

4. Software para comprobación de vulnerabilidad

Al revisar que los dispositivos WiFi en la actualidad que utilizan cifrados WEP y WPA no poseen la seguridad necesaria en lo que se refiere a la contraseña de ingreso a la red wireless, se comprobará de una manera práctica dichas vulnerabilidades, y se usará el software que se encuentra en el Internet: **CommView for WiFi** y el suite **Aircrack-ng**.

NOTA: *Con el software que se encontró en Internet, es posible solamente buscar contraseñas WPA/WPA2 que utilizan cifrado PSK.*

4.1 CommView for WiFi

CommView for WiFi es una poderosa herramienta para el monitoreo y análisis de las redes 802.11 a/b/g/n. Presenta una interfaz amigable para el usuario, fácil y sencilla para equipos con Sistema Operativo Windows (XP, Vista, 7) de 32bits, es uno de los sniffers más completos y mejor valorados para Windows.

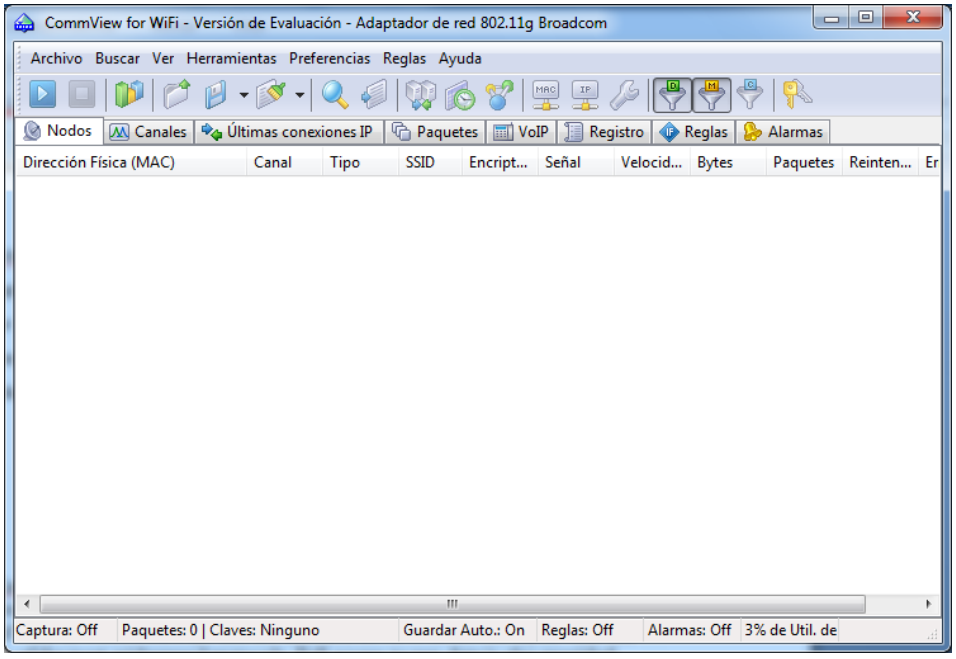


Figura 4.01 CommView for WiFi

Fuente: Software CommView for WiFi

CommView for WiFi es justamente eso, un sniffer con herramientas y funciones que se necesita para capturar los paquetes de las conexiones inalámbricas. Con la herramienta se puede capturar tramas Ethernet y analizar cada una de sus cabeceras y protocolos incluidos: paquetes IP, segmentos TCP, datagramas UDP, protocolos RTP y RTCP, entre otras posibilidades.

4.1.1 Uso de la herramienta

La herramienta CommView for WiFi se puede bajar de la siguiente página web: **http://www.tamos.com/products/commwifi/**

Antes de instalarlo, es necesario sacar los respaldos de los drivers de la tarjeta de red inalámbrica del computador, ya que es obligatorio cargar el driver que proporciona ***CommView***, lo que se puede hacer mediante el asistente del programa o a través del administrador de dispositivos, a continuación se presentará la instalación de los drivers mediante el asistente:

- Instalamos la aplicación, luego ingresamos al menú *Ayuda*, y damos clic en la opción *Guía de instalación del controlador*.

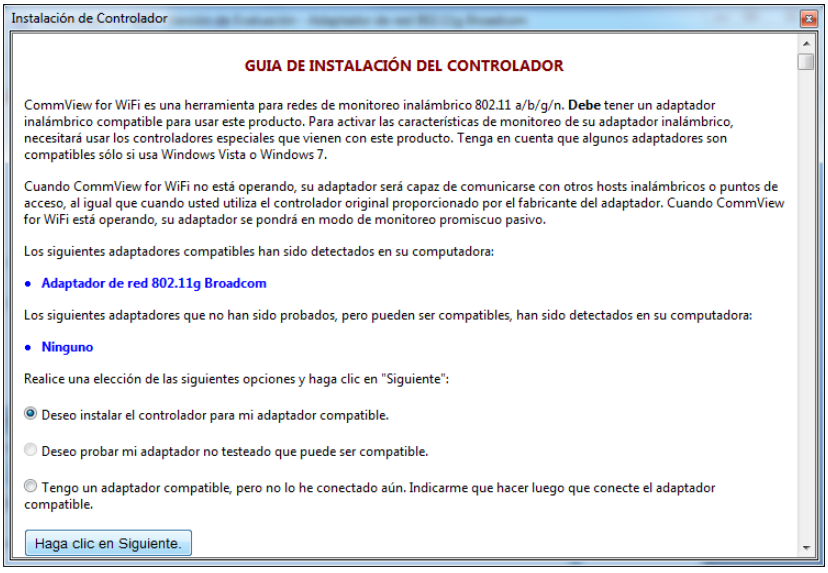


Figura 4.02 Guía de instalación del controlador wireless

Fuente: Software CommView for WiFi

- La ventana mostrará el adaptador que se encuentra instalado en la computadora y presenta una elección por defecto, dejamos seleccionada la primera opción y damos clic en *Siguiente*.

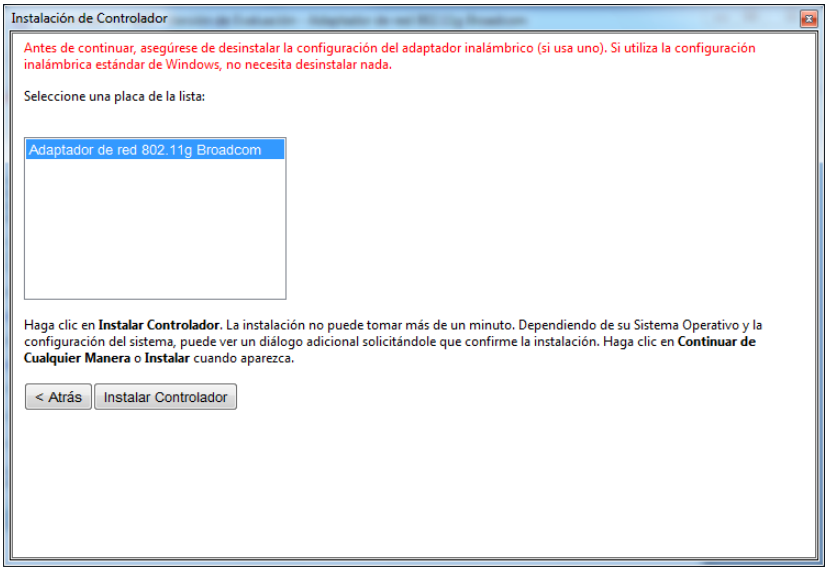


Figura 4.03 Ventana de adaptadores disponibles para su instalación

Fuente: Software CommView for WiFi

- Realizamos lo indicado y luego damos clic en *Instalar controlador* y luego en la siguiente ventana damos clic en *Finalizar*, se reiniciará la aplicación.

Antes de la captura de tráfico, es posible realizar algunos cambios en los datos por defecto del programa. Damos clic en la pestaña Registro y cambiamos los valores *de Tamaño máximo del directorio, MBytes* a 50000 y *Tam. Promedio de arch. Reg., MBytes* a 100; los valores cambiados permitirán capturar el mayor tráfico de datos posible.

Se puede cambiar también la opción *Guardar registros en:* al escritorio o carpeta en la que se desee almacenar la información que se va a obtener de la captura de tráfico de la red.

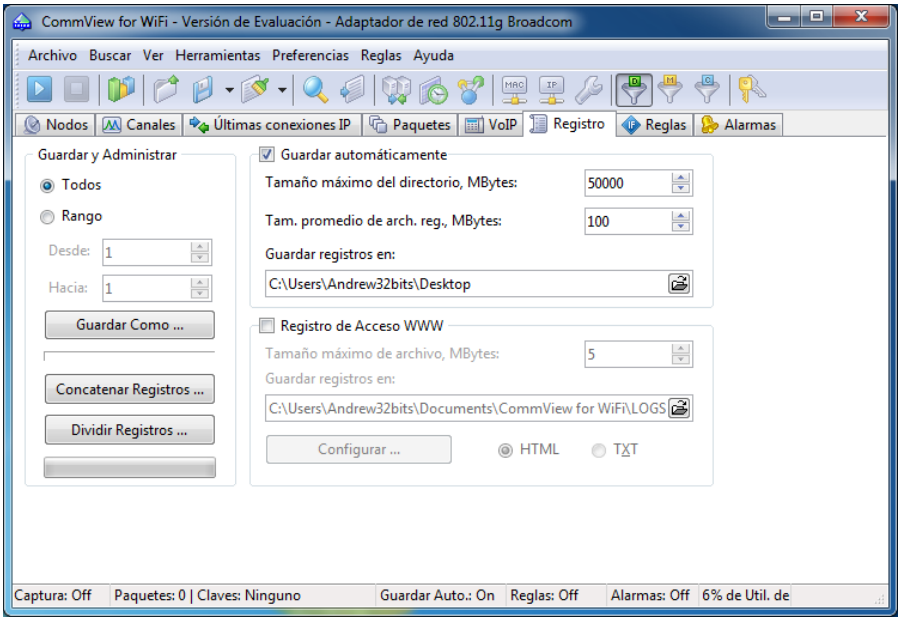


Figura 4.04 Configuración inicial CommView for WiFi

Fuente: Software CommView for WiFi

Igualmente, de la pestaña *Reglas*, se seleccionan las opciones *Capturar Paquetes de Datos* e *Ignorar Beacons*, esto permitirá solamente capturar el tráfico de datos óptimo necesario.

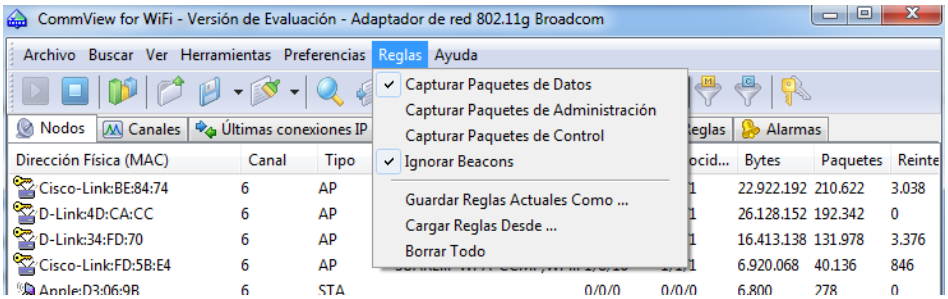


Figura 4.05 Configuración Reglas CommView for WiFi

Fuente: Software CommView for WiFi

- Iniciamos la captura de tráfico dando un clic en el botón *Iniciar Captura* , aparecerá la ventana *Explorador*. Con la captura de tráfico activada se podrá comenzar la exploración de los canales WiFi accesibles.

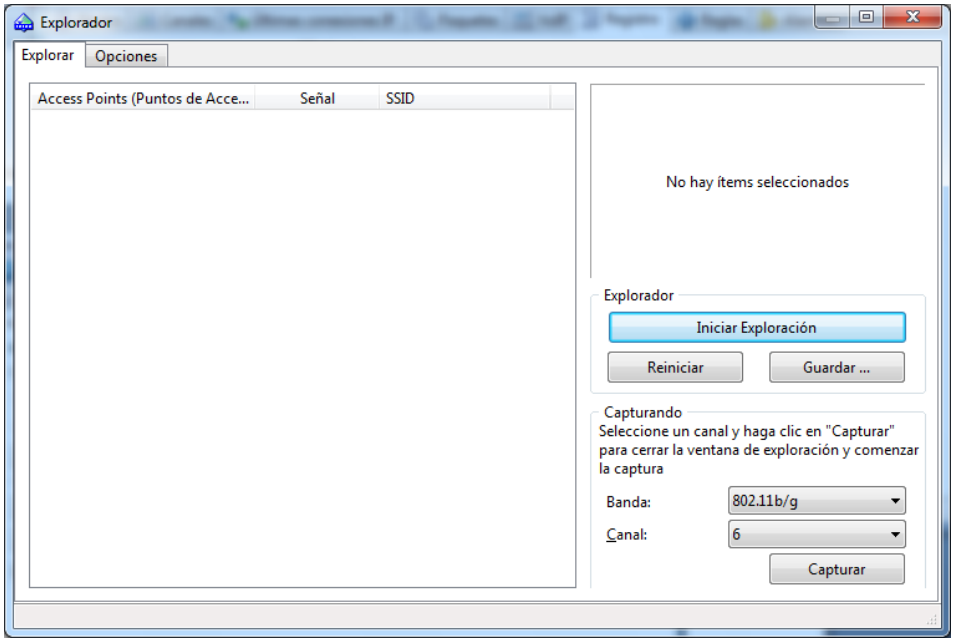


Figura 4.06 Explorador de redes WiFi

Fuente: Software CommView for WiFi

- Se da clic en *Iniciar Exploración*, se mostrará todas las redes disponibles en todos los canales ofreciendo una visión global del espacio WiFi del área.

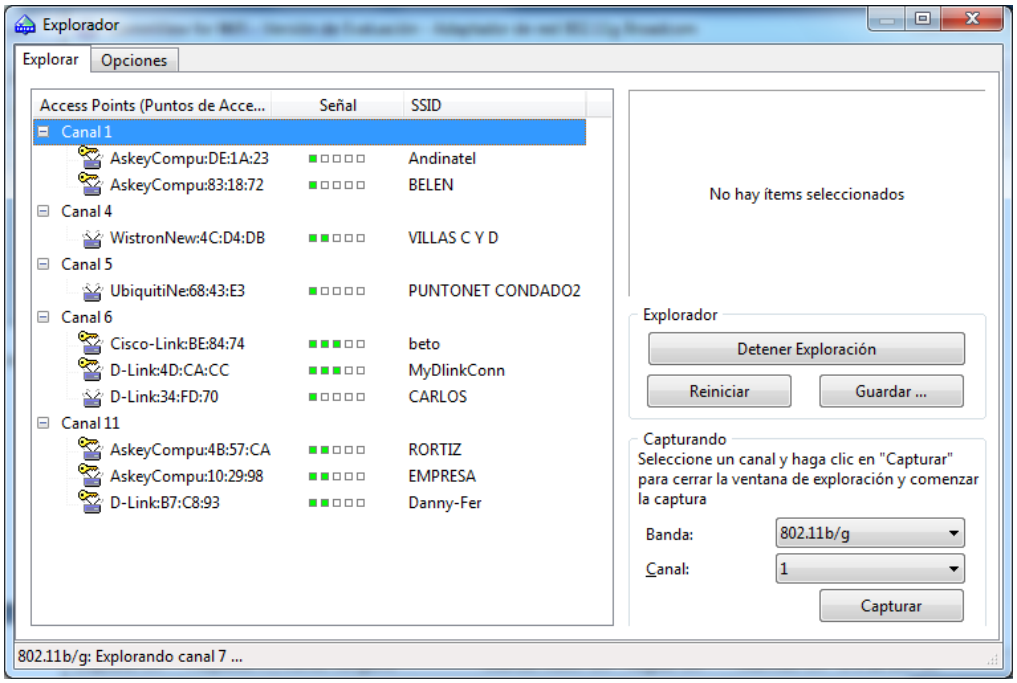


Figura 4.07 Redes WiFi encontradas

Fuente: Software CommView for WiFi

- Se escoge el punto de acceso requerido; para activar la captura de paquetes de esa red, se da clic en el botón de *Capturar* que se encuentra en el panel de opciones de la derecha.

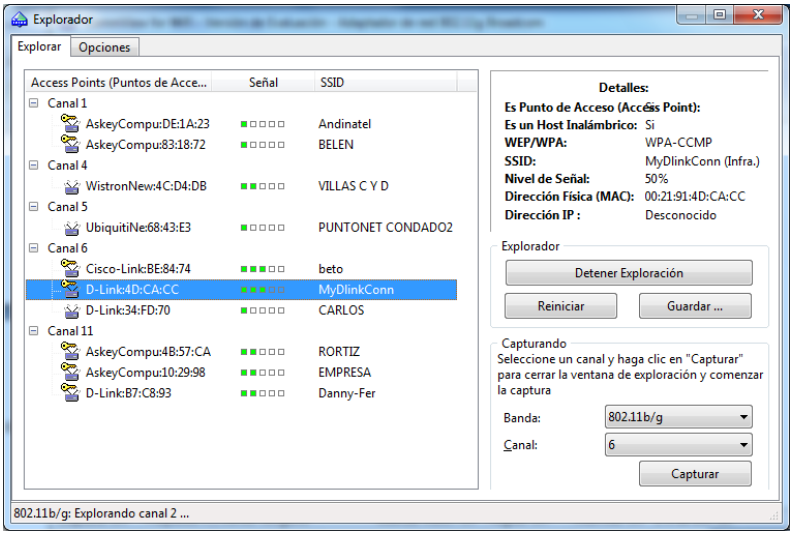


Figura 4.08 Selección red WiFi

Fuente: Software CommView for WiFi

- *CommView* empezará a realizar la captura de tráfico de la red seleccionada; inicialmente aparecerá en la pestaña *Nodos*, los puntos de acceso y clientes asociados que usan el canal en un determinado instante.

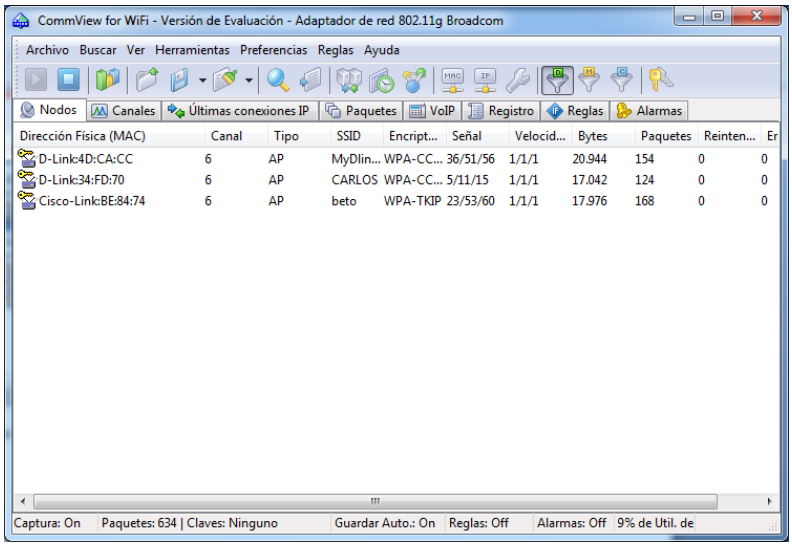


Figura 4.09 Captura de tráfico de la red seleccionada

Fuente: Software CommView for WiFi

- Con las configuraciones de la pestaña Registro, se creará un archivo en el Escritorio o en la carpeta seleccionada de almacenamiento de la captura.

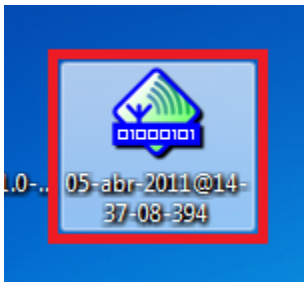
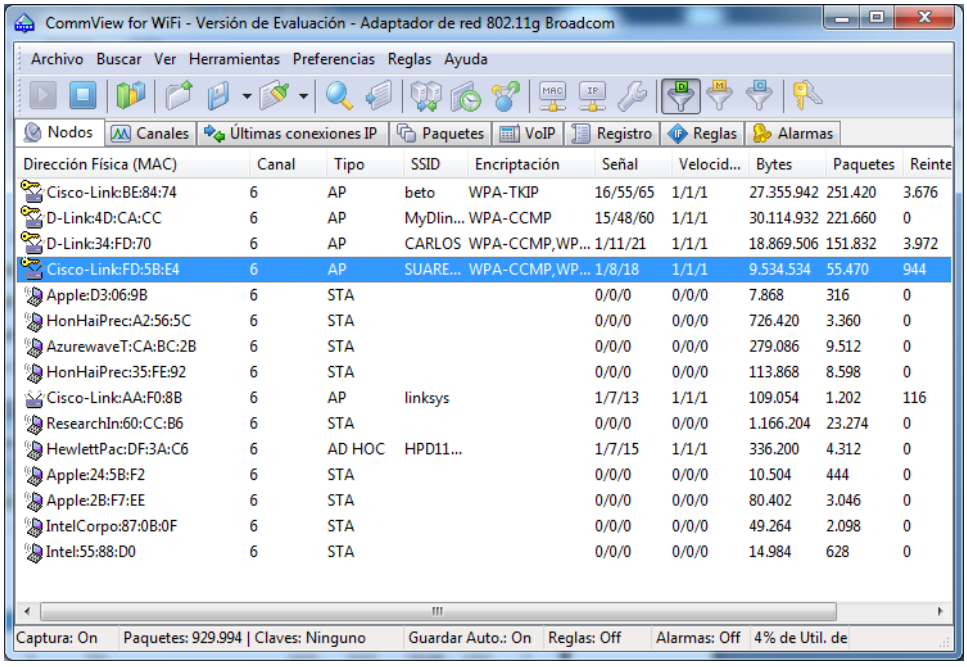


Figura 4.10 Creación de archivo de captura de paquetes

Fuente: Software CommView for WiFi

- Al seleccionar la pestaña *Nodos*, se observan los diferentes puntos de acceso que usan WPA2-PSK con cifrado CCMP y WPA-PSK, como también los clientes que se encuentran asociados a la redes. Los datos que se capturan son todos los paquetes que circulan por el canal.



Dirección Física (MAC)	Canal	Tipo	SSID	Encriptación	Señal	Velocid...	Bytes	Paquetes	Reinte
Cisco-Link:BE:84:74	6	AP	beto	WPA-TKIP	16/55/65	1/1/1	27.355.942	251.420	3.676
D-Link:4D:CA:CC	6	AP	MyDlin...	WPA-CCMP	15/48/60	1/1/1	30.114.932	221.660	0
D-Link:34:FD:70	6	AP	CARLOS	WPA-CCMP,WP...	1/11/21	1/1/1	18.869.506	151.832	3.972
Cisco-Link:FD:5B:E4	6	AP	SUARE...	WPA-CCMP,WP...	1/8/18	1/1/1	9.534.534	55.470	944
Apple:D3:06:9B	6	STA			0/0/0	0/0/0	7.868	316	0
HonHaiPrec:A2:56:5C	6	STA			0/0/0	0/0/0	726.420	3.360	0
AzurewaveT:CA:BC:2B	6	STA			0/0/0	0/0/0	279.086	9.512	0
HonHaiPrec:35:FE:92	6	STA			0/0/0	0/0/0	113.868	8.598	0
Cisco-Link:AA:F0:8B	6	AP	linksys		1/7/13	1/1/1	109.054	1.202	116
ResearchIn:60:CC:B6	6	STA			0/0/0	0/0/0	1.166.204	23.274	0
HewlettPac:DF:3A:C6	6	AD HOC	HPD11...		1/7/15	1/1/1	336.200	4.312	0
Apple:24:5B:F2	6	STA			0/0/0	0/0/0	10.504	444	0
Apple:2B:F7:EE	6	STA			0/0/0	0/0/0	80.402	3.046	0
IntelCorpo:87:0B:0F	6	STA			0/0/0	0/0/0	49.264	2.098	0
Intel:55:88:D0	6	STA			0/0/0	0/0/0	14.984	628	0

Figura 4.11 Access Point encontrados con sus clientes asociados

Fuente: Software CommView for WiFi

- Al registro creado lo abrimos dando doble clic, o de la ventana del *CommView* se puede desplegar el menú *Archivo*, damos clic en *Visor de Registros* y aparecerá la ventana del visor, de ahí se necesitará solamente buscar el archivo creado necesario.

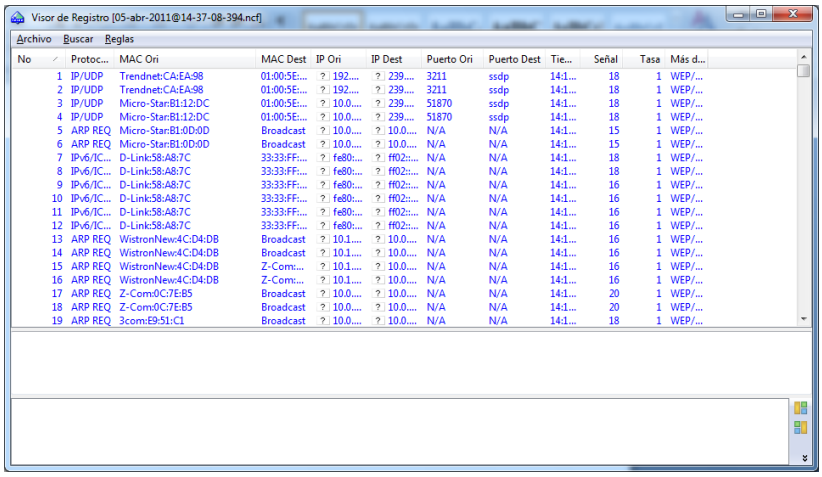


Figura 4.12 Visor de Registros CommView for WiFi

Fuente: Software CommView for WiFi

- En la ventana se cargarán todos los paquetes que se haya capturado en el fichero, ya sean éstos buenos o malos, por eso se puede tener un cierto número de IVs válidos, lo cuales con aplicaciones como Aircrack-ng se puede comprobar su validez o hasta es posible que presente errores.

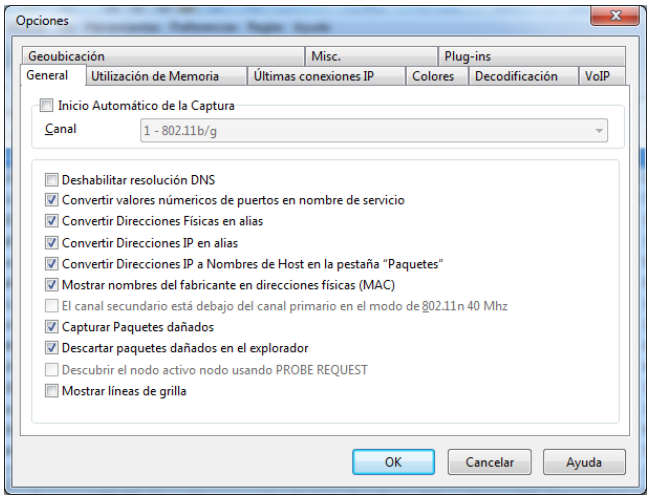


Figura 4.13 Configuración de Opciones Generales

Fuente: Software CommView for WiFi

- Cuando se encuentren los datos cargados correctamente en dicho visor, se procede a convertir el formato a .CAP. Se abre el menú *Archivo*, se dirige hacia *Exportar Registros*, se selecciona la opción *Wireshark/Tcpdump (es el último de la lista)*, lo ponemos un nombre y lo guardamos.

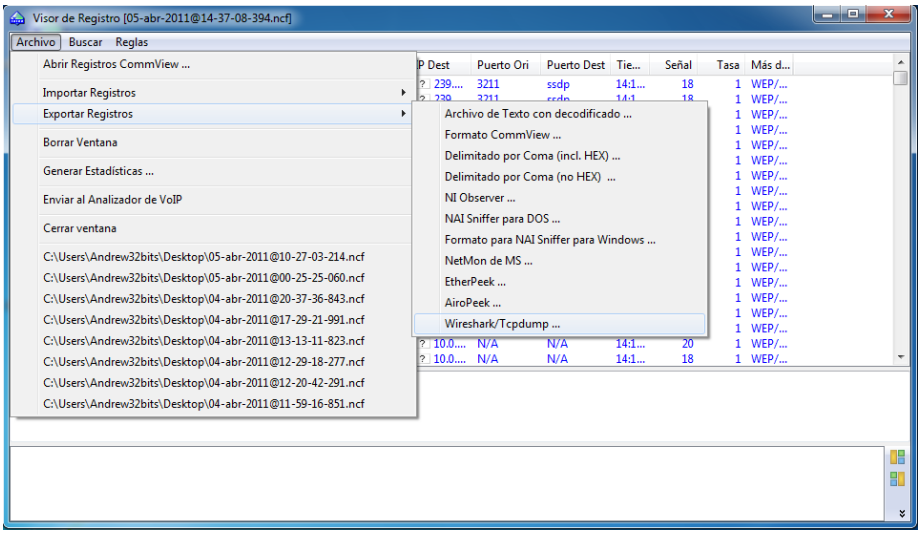


Figura 4.14 Exportar registros

Fuente: Software CommView for WiFi

Figura 4.15 Creación de archivo con extensión .CAP

Fuente: Software CommView for WiFi

Capturados los paquetes de datos necesarios, seguimos con la herramienta Aircrack-ng para encontrar las contraseñas necesarias de las redes que se van a tratar de vulnerar su seguridad.

4.2 Suite Aircrack-ng

La suite Aircrack-ng es una herramienta que permite el crackeo de redes WIFI. Con esta herramienta se pueden lanzar una gran cantidad de ataques sobre los protocolos WEP, WPA/WPA2-PSK. En el suite se incluyen otras herramientas adicionales que proporcionan un ataque complejo sobre las redes que se elijan, entre ellas están: Airodump-ng, Aireplay-ng y Aircrack-ng.

El paquete Aircrack-ng se lo puede descargar de la página web:
http://www.aircrack-ng.org/

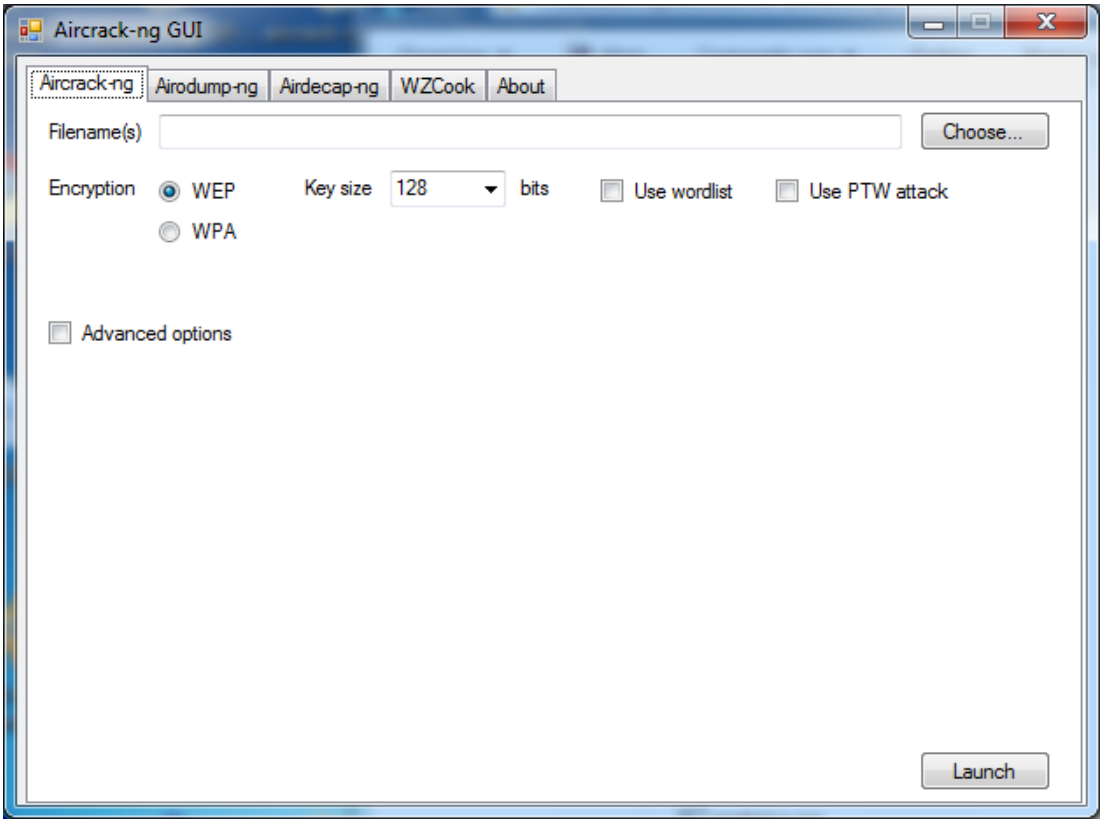


Figura 4.16 Aircrack-ng en modo gráfico

Fuente: Software Aircrack-ng GUI

El Suite Aircrack-ng puede funcionar en modo GUI o en el procesador de comandos de Windows.

4.2.1 Airodump-ng

Esta herramienta es la encargada de monitorizar el tráfico WIFI, capturando los paquetes 802.11 que circulan por la red de forma pasiva. La captura permitirá mediante la herramienta Aircrack-ng descifrar la clave, gracias a la recopilación de todos los IVs que contienen dichos paquetes.

Airodump-ng trabaja parecido a la herramienta CommView for WiFi.

4.2.1.1 Uso de la herramienta

Primeramente se debe iniciar el script Airmon-ng para que se muestren los dispositivos wireless que posees y para activar el modo monitor.

En el procesador de comandos, se debe ingresar a la carpeta donde se encuentra el Suite Aircrack-ng y se coloca los parámetros como se muestra a continuación:

C:\….\….\aircrack-ng-1.0-win\bin>airodump-ng [opciones] <dispositivo>

Las opciones que se tienen dentro de la herramienta airodump-ng:

--ivs: captura solo ivs

--gpsd: para usar un dispositivo gps

--write <nombre del archivo a guardar>: crea un archivo del nombre que le hallamos puestos y con la extensión (.cap ó .ivs) y empieza a capturar.

-w: es lo mismo que poner write.

--beacons: guarda los beacons, por defecto no los guarda.

Por defecto, airodump captura todos los canales que se encuentren dentro de la frecuencia 2,4GHz.

--channel: captura el canal especificado.

-c: lo mismo que escribir cannel.

-a: captura en la frecuencia de 5GHz

-abg: captura tanto en frecuencias de 2,4GHz como en 5GHz.

Ejemplos:

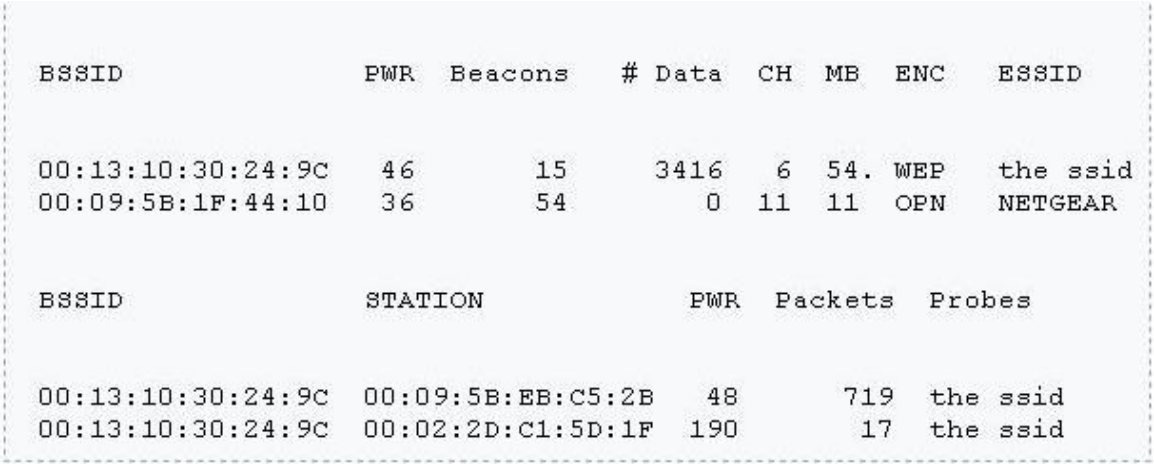
C:\….\….\aircrack-ng-1.0-win\bin>airodump-ng –ivs –w prueba –c 11 –abg ath0

capturaría solo ivs creando un archivo llamado prueba en el canal 11 tanto en a/b/g

C:\….\….\aircrack-ng-1.0-win\bin>airodump-ng –w prueba –c 11 –abg ath0

capturaría creando un archivo cap llamado prueba en el canal 11 tanto en a/b/g

Airodump-ng mostrará una lista con los puntos de acceso detectados, y también una lista de clientes conectados o estaciones ("stations").



```
BSSID              PWR  Beacons    # Data  CH  MB  ENC   ESSID

00:13:10:30:24:9C   46       15      3416   6  54. WEP   the ssid
00:09:5B:1F:44:10   36       54         0  11  11  OPN   NETGEAR

BSSID              STATION            PWR  Packets  Probes

00:13:10:30:24:9C  00:09:5B:EB:C5:2B   48      719  the ssid
00:13:10:30:24:9C  00:02:2D:C1:5D:1F  190       17  the ssid
```

Captura 4.01 Puntos de acceso encontrados con Airodump-ng

Fuente: Software Airdump-ng

Opción	Descripción
BSSID	Dirección MAC del punto de acceso
PWR	Nivel de señal reportado por la tarjeta. Su significado depende del controlador, pero conforme se acerca al punto de acceso o a la estación la señal aumenta. Si PWR==-1, el controlador no soporta reportar el nivel de señal.
Beacons	Número de paquetes-anuncio enviados por el AP. Cada punto de acceso envía unos diez Beacons por segundo al ritmo (rate) mínimo (1M), por lo que normalmente pueden ser recogidos desde muy lejos.
# Data	Número de paquetes de datos capturados (si es WEP, sólo cuenta IVs), incluyendo paquetes de datos de difusión general.
CH	Número de canal (obtenido de los paquetes beacon). Nota: algunas veces se capturan paquetes de datos de otros canales aunque no se esté alternando entre canales debido a las interferencias de radiofrecuencia.
MB	Velocidad máxima soportada por el AP. Si MB=11, entonces se trata de 802.11bm si MB=22 entonces es 802.11b+ y velocidades mayores son 802.11g. El punto (después de 54) indica que short preamble está soportado.
ENC	Algoritmo de encriptación en uso. OPN=sin encriptación, "WEP"?=WEP o mayor (no hay suficiente datos para distinguir entre WEP y WPA), WEP (sin la interrogación) indica WEP estática o dinámica, y WPA si TKIP o CCMP están presentes.
ESSID	Conocida como "SSID", puede estar vacía si el ocultamiento de SSID está activo. En este caso airodump tratará de recuperar el SSID de las respuestas a escaneos y las peticiones de asociación.
STATION	Dirección MAC de cada estación asociada.

Cuadro 4.01 Opciones Airodump-ng

Autor: Andrés Serrano Flores

4.2.2 Airdecap-ng

Esta herramienta sirve para desencriptar los paquetes capturados una vez obtenida la clave, ya sea WEP o WPA.

4.2.2.1 Uso de la herramienta

En el procesador de comandos, se debe ingresar a la carpeta donde se encuentra el Suite Aircrack-ng y se coloca los parámetros como se muestra a continuación:

C:\….\….\aircrack-ng-1.0-win\bin>airdecap-ng [opciones] <archivo .cap>

Opción	Parámetro	Descripción
-l		No elimina la cabecera del 802.11
-b	bssid	Filtro de dirección MAC del punto de acceso
-k	pmk	WPA Pairwise Master Key en hex
-e	essid	Identificador en ascii de la red escogida
-p	pass	Contraseña WPA de la red escogida
-w	key	Clave WEP de la red escogida en hex

Cuadro 4.02 Opciones Airdecap-ng

Autor: Andrés Serrano Flores

Ejemplos:

C:\….\….\aircrack-ng-1.0-win\bin>airdecap-ng -b 00:09:5B:10:BC:5A wpa.cap

C:\….\….\aircrack-ng-1.0-win\bin>airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap

C:\….\….\aircrack-ng-1.0-win\bin>airdecap-ng -e RedWiFi -p passphrase captura.cap

4.2.3 WZCook

Sirve para recuperar las claves WEP de la utilidad de XP Wireless Zero Configuration. Este es un software experimental, por lo que puede que funcione y puede que no, dependiendo del nivel de Service Pack que se tenga.

4.2.4 Aircrack-ng

Esta es la principal herramienta de criptoanálisis que permite recuperar la clave a partir de la captura mediante airodump-ng o de CommView for WiFi de paquetes cifrados, (este último utilizado para la elaboración de la presente disertación de grado), combinando ataques estadísticos con ataques de fuerza bruta.

Para el caso de las claves WPA y WPA2-PSK es necesario un diccionario de datos o de palabras claves.

4.2.4.1 Uso de la herramienta

Para el uso de la herramienta, se puede ingresar ya sea por la aplicación GUI o mediante el procesador de comandos de Windows.

Al iniciar mediante el modo GUI, aparecerá la pantalla que se muestra:

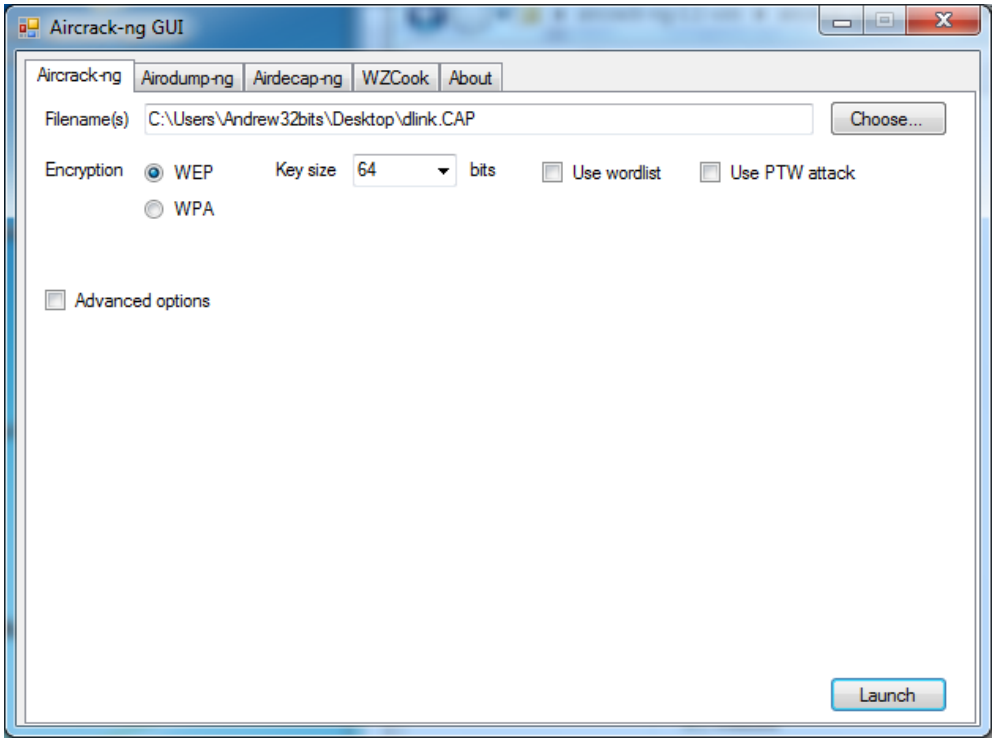


Figura 4.17 Aircrack-ng

Fuente: Software Aircrack-ng GUI

En *Filename(s)* se escogerá la captura de paquetes cifrados obtenido de Airodump-ng o de CommView.

- En cifrado WEP:

Si la clave a obtener de una red WiFi es de cifrado WEP, se debe dejar por defectos las opciones presentadas, lo único a cambiar sería el tamaño de clave:

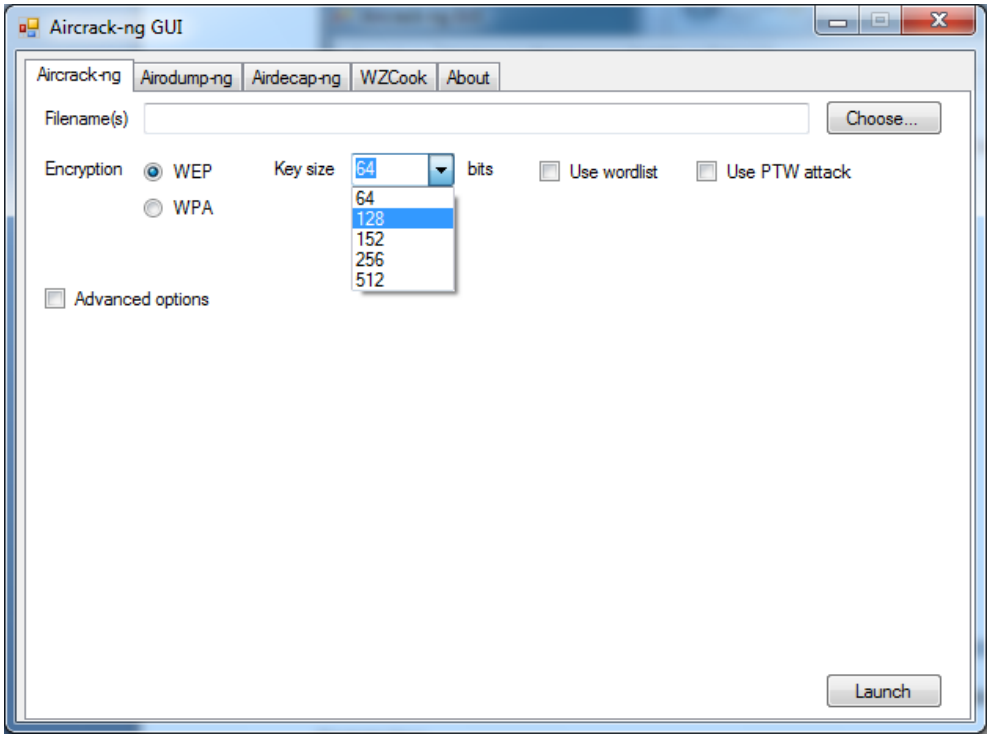
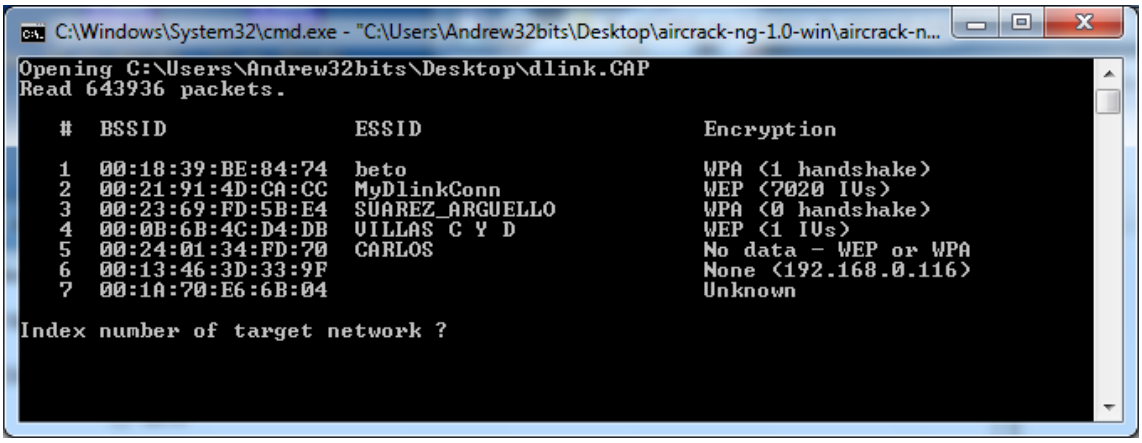


Figura 4.18 Obtención clave con cifrado WEP

Fuente: Software Aircrack-ng GUI

Al dar clic en el botón *Launch* aparecerá la siguiente pantalla:

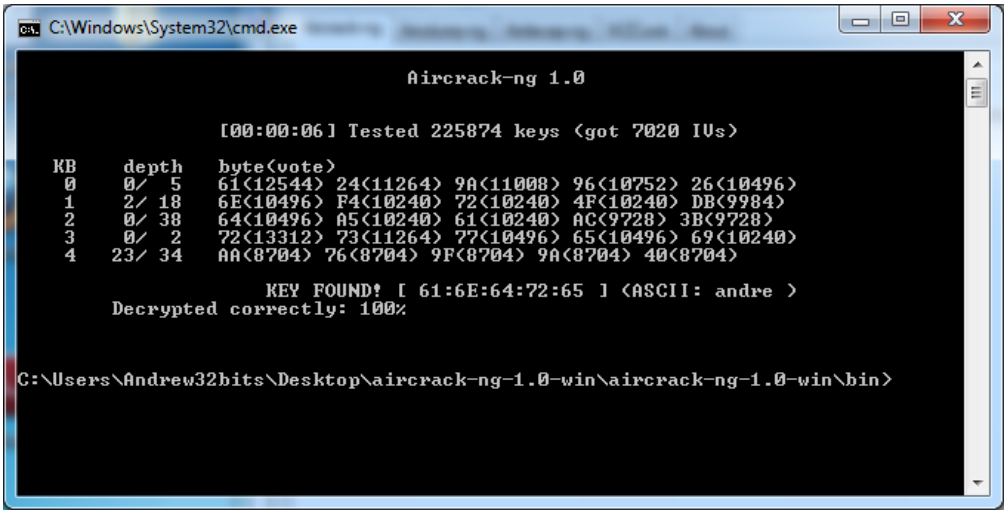


Captura 4.02 AP encontrados de la captura de registros .CAP

Fuente: Software Aircrack-ng MS-DOS

Se escogerá la red con encriptación WEP requerida (se debe tener en cuenta que el número de IVs optimo debe ser mayor a 5000 para que un paquete cifrado pueda ser decodificado).

Luego de un cierto tiempo, dependiendo del paquete capturado, se obtendrá la clave WEP:



Captura 4.03 Clave encontrada de red con cifrado WEP

Fuente: Software Aircrack-ng MS-DOS

- En cifrado WPA/WPA2

Para la decodificación de claves WPA/WPA2-PSK en necesario, además del paquete cifrado, de un diccionario de datos o una lista de palabras claves (Wordlist).

Varios de éstos Wordlist se pueden encontrar en la red, su extensión puede ser .lst o .txt, es posible también crear un Wordlist propio dependiendo de las claves a buscar.

A continuación se señalan algunas páginas donde se pueden obtener wordlist completos:

http://www.edadfutura.com/wordlist-diccionarios-para-crackear-wpa/
http://www.outpost9.com/files/WordLists.html
http://outworld.es/spdic.gz
http://comunidad.dragonjar.org/f182/diccionarios-para-wpa-9835/

http://www.gratistaringa.net/f131/diccionario-227-millones-de-palabras-wpa-wpa2-wifi-multilenguaje-4shared-1476636/
http://www.zonadd.net/viewtopic.php?t=4433

http://www.taringa.net/posts/linux/5687920/Diccionarios-competos-WPA_WPA2-Backtrack-4-WPA-CRACKER.html

http://www.taringa.net/posts/downloads/9348095/Mega-Diccionario-para-WPA_WPA2-227-millones-de-palabras-2Gb.html

También existe un programa que genera diccionarios por defecto según el router, se llama WiFiCripter y se lo puede obtener de la siguiente página web: **http://wificripter.blogspot.com/**

Aircrack-ng se puede iniciar en el modo GUI o mediante el procesador de comandos de Windows:

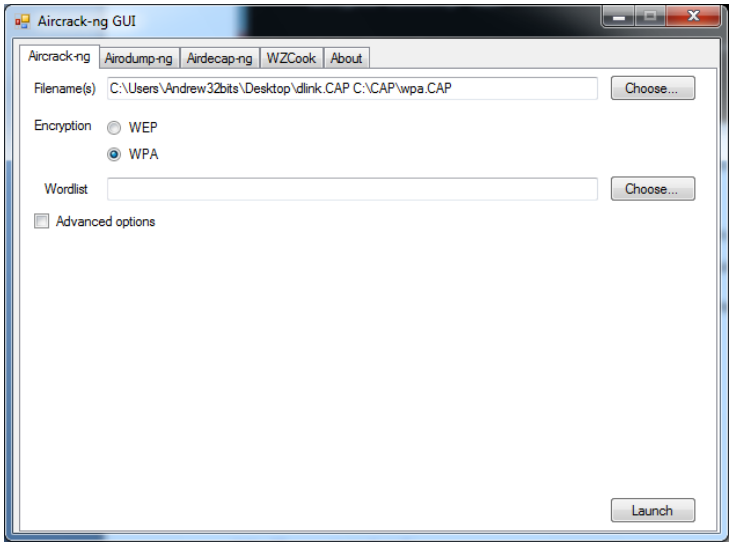
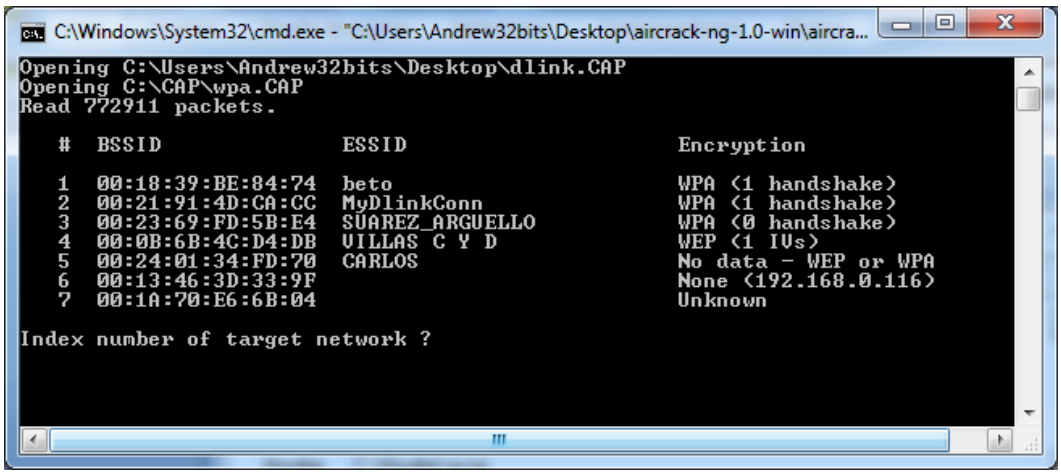


Figura 4.19 Obtención clave con cifrado WPA

Fuente: Software Aircrack-ng GUI

En éste caso se escogerá en *Encryption* la opción WPA; se debe escoger un Wordlist y posterior dar clic en el botón *Launch*. (Este proceso sirve para encontrar tanto claves con cifrado WPA como con cifrado WPA2)

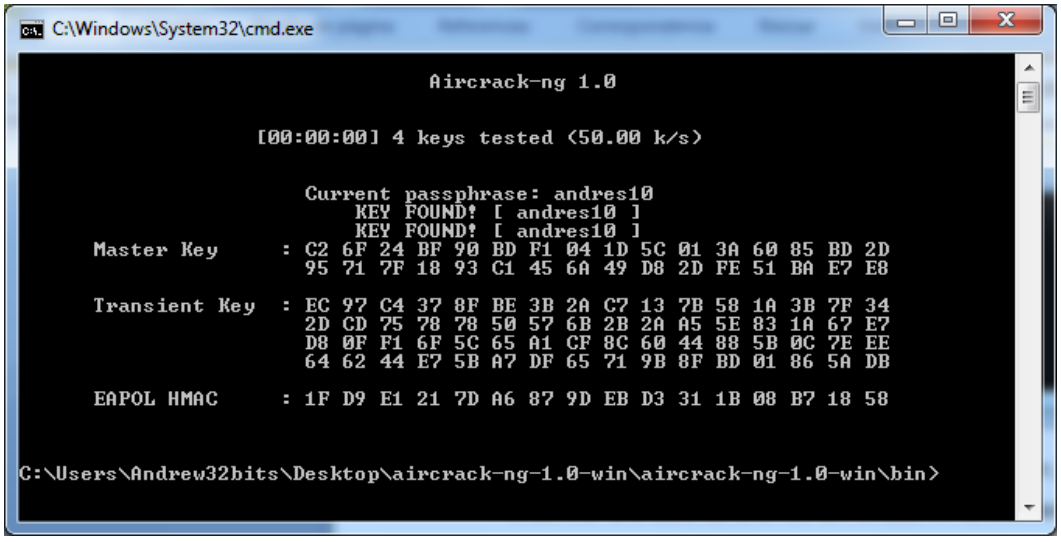


Captura 4.04 AP encontrados de la captura de registros .CAP

Fuente: Software Aircrack-ng MS-DOS

Igualmente aparecerá la información de redes a escoger, hay que tener en cuenta que para encontrar una clave de una red con cifrado WPA, ésta debe tener por lo menos un handshake.

Se selecciona la red cifrada WPA con por lo menos un handshake y luego de unos momentos (dependiendo si el diccionario de datos contiene una de las palabras de la clave), se obtendrá la clave necesaria.



Captura 4.05 Clave encontrada de red con cifrado WPA

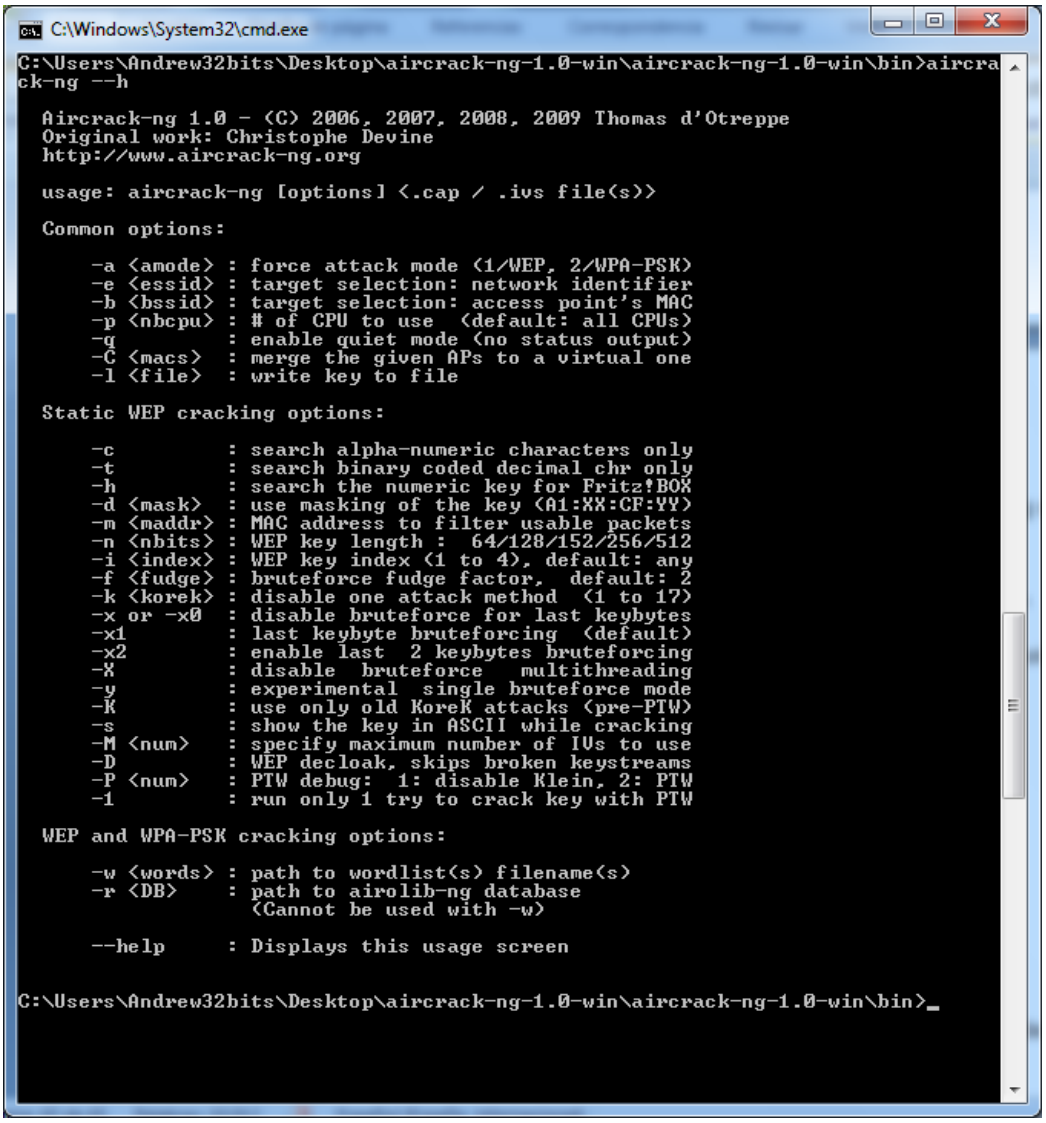
Fuente: Software Aircrack-ng MS-DOS

Es posible usar las diferentes opciones del Aircrack-ng en el procesador de comandos de Windows como se muestra a continuación:

C:\….\….\aircrack-ng-1.0-win\bin>aircrack-ng [opciones] <archivo(s) de captura >

Para obtener la información de ayuda de Aircrack-ng se coloca el siguiente comando:

C:\….\….\aircrack-ng-1.0-win\bin >aircrack-ng --h



Captura 4.06 Opciones Aircrack-ng

Fuente: Software Aircrack-ng MS-DOS

Ejemplos:

C:\....\....\aircrack-ng-1.0-win\bin>aircrack-ng -w C:\Wordlist\word.lst -b 00:21:91:4D:CA:CD -e MyDlinkConn C:\CAP\wpa.cap

C:\....\....\aircrack-ng-1.0-win\bin>aircrack-ng -w C:\Wordlist\as.txt -b 00:21:91:4D:CA:CD -e MyDlinkConn C:\CAP\1.cap

CAPÍTULO V

5. Estudio de Casos

Se realizará un estudio práctico de las herramientas analizadas en dos PYMES del Distrito Metropolitano de Quito.

Los dispositivos a utilizar en los PYMES tenemos:

Hardware

EQUIPO	CARACTERÍSTICAS
Computador Portátil Hewlett-Packard  **Figura 5.01 Computador Portátil HP** *Fuente: http:// www.**hp**.com/Notebooks-Pavilion*	✓ HP Pavilion Entertainment PC Dv4t-1000 ✓ Procesador: Intel Core 2 Duo 2.53GHz ✓ Memoria RAM: 3GB ✓ Disco Duro: 300GB ✓ Tarjeta de red: 802.11g Broadcom (integrada) ✓ MAC: 00-21-00-5A-75-B9 ✓ Sistema Operativo: Windows 7 Professional de 32 bits
Tarjeta inalámbrica adicional  **Figura 5.02 Tarjeta USB Linksys** ***Fuente:*** *http://www.linksysbycisco.com/ LATAM/es/products/WUSB54GC*	✓ Linksys Compact Wireless-G USB Adapter ✓ Modelo: WUSB54GC ✓ Banda de Frecuencia: 2.4GHz ✓ MAC: 00-18-39-12-52-86

Cuadro 5.01 Requerimientos de Hardware

Autor: Andrés Serrano Flores

Software

Los programas a utilizar son las herramientas revisadas:

- ✓ CommView for WiFi (sniffer)
- ✓ Suite Aircrack-ng (desencriptador)

5.1 Electrificaciones del Ecuador S.A. (Elecdor S.A.)

Electrificaciones del Ecuador S.A. es una empresa afiliada al grupo ELECNOR, organización española dedicada a la ingeniería, desarrollo y construcción a infraestructuras en los ámbitos de la energía, el medio ambiente, las tecnologías y sistemas de información y el espacio.

Figura 5.03 Logo Elecdor S.A.

Fuente: Electrificaciones del Ecuador ELECDOR S.A.

La empresa tiene su domicilio principal en la Ciudad de Quito, República del Ecuador. La actividad principal de la misma es la fabricación de postes de hormigón y estructuras para tendidos eléctricos. El segmento de mercado que está enfocada es principalmente a Empresas Eléctricas y personas naturales que principalmente están relacionados con temas de construcción.

5.1.1 Misión

“ELECDOR S.A. es una compañía que tiene por objeto garantizar la confiabilidad de los sistemas de Distribución, Subtrasmisión, Transmisión, y

Telecomunicaciones, teniendo como prioridad la Calidad, Seguridad y Eficiencia en el Servicio."

5.1.2 Visión

"Ser un equipo humano de trabajo que avale permanentemente productos y servicios Electromecánicos y de Telecomunicaciones competitivos de la más alta calidad, que estén acordes a las necesidades del cliente."

5.1.3 Valores

Al igual que su matriz Elecnor, Elecdor S.A. es una empresa dinámica e innovadora que cree en las personas y tiene la convicción de que la principal fuente de agregación de valor radica en los equipos profesionales que componen la empresa.

Los principales valores así como los principios básicos que Elecdor S.A. aplica para conseguir ser una empresa profesional ante el cliente y en los que cree firmemente son:

- ✓ **Orientación al cliente**
  Esfuerzo dirigido a la satisfacción del cliente, aportando soluciones competitivas y de calidad.
- ✓ **Orientación a resultados**
  Actividad orientada a la consecución de los objetivos del proyecto empresarial y de la rentabilidad de los accionistas, tratando de superar sus expectativas.
- ✓ **Prevención de riesgos laborales**
  Compromiso decidido con la seguridad y salud laboral promoviendo una cultura preventiva.
- ✓ **Responsabilidad Corporativa**
  Integración voluntaria de las preocupaciones sociales y medioambientales en sus operaciones comerciales y sus relaciones con sus interlocutores, canalizando a través de la Fundación Elecnor,

iniciativas en los ámbitos de infraestructura social, innovación tecnológica, formación y mecenazgo sociocultural.

- ✓ **Calidad y Medio Ambiente**
  Adaptación de la estrategia empresarial a la preservación del medio ambiente.
- ✓ **Compromiso con la organización**
  Implicación y compromiso con los objetivos empresariales, lealtad profesional y entrega al trabajo son señas de identidad de todas las personas que trabajan en el Grupo Elecnor heredadas de los propios socios fundadores.
- ✓ **Liderazgo**
  Esfuerzo continuo para ganar día a día la batalla de la competitividad, de la globalización de mercados, de la calidad y la capacidad tecnológica posicionándose como Grupo líder en sus distintas actividades.
- ✓ **Trabajo en equipo**
  Fomento de la participación de todos para lograr un objetivo común, compartiendo la información y los conocimientos.
- ✓ **Formación y desarrollo**
  Apuesta por el desarrollo profesional del capital humano mediante políticas de captación del talento, compensación, selección, formación y desarrollo.
- ✓ **Innovación**
  Promoción de la mejora continua y la innovación para alcanzar la máxima calidad desde criterios de rentabilidad.

La compañía Elecdor S.A. se encuentra ubicada en la Avenida Eloy Alfaro N32-650 y Bélgica. Dentro de ella se encuentra una red estructurada compuesta de 1 servidor y 9 computadores, todos ellos enlazados por un switch 3COM. El dispositivo wireless usado es marca Linksys, modelo WRT54G; éste dispositivo se ocupa al momento para compartir el Internet de la empresa y ocupar la impresora que se encuentra conectada en red.

A continuación se detalla el diagrama de red de la empresa Elecdor S.A.:

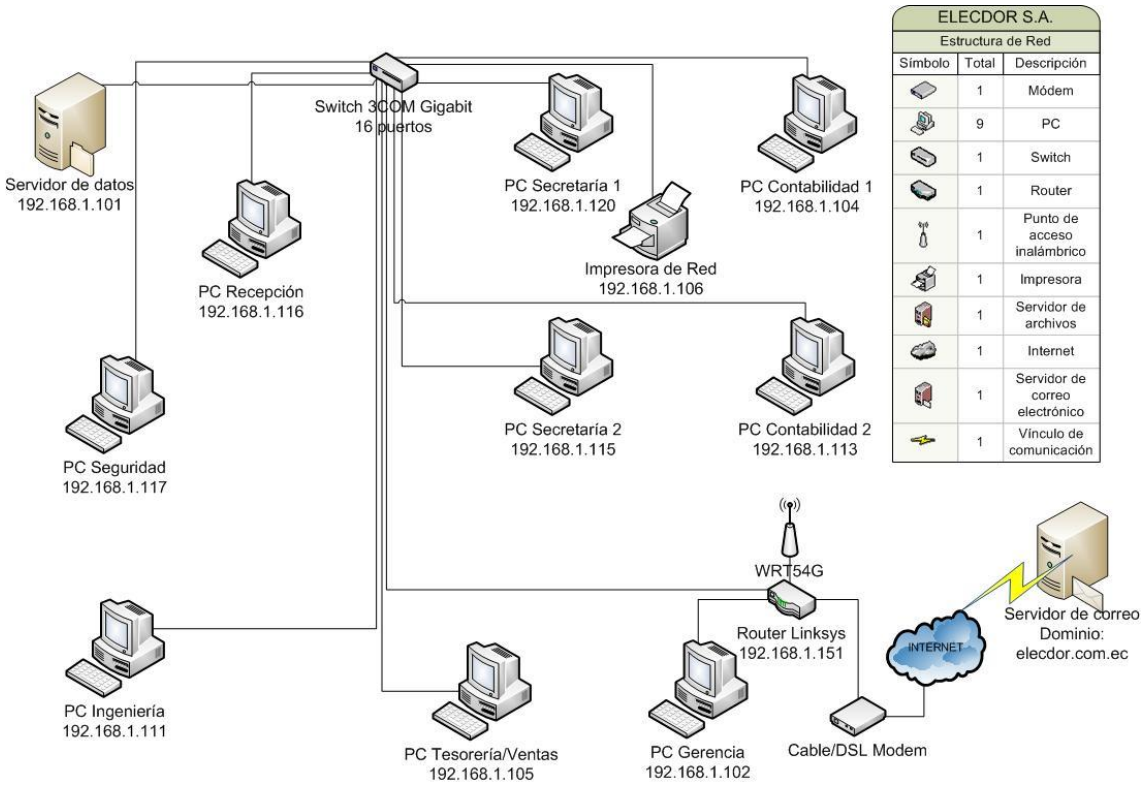


Figura 5.04 Red estructurada Elecdor S.A.

Autor: Andrés Serrano Flores

5.1.4 Atacando la red

Como se ha señalado, se necesita usar la herramienta CommView for WiFi para comenzar con la captura de los paquetes de datos que viaja a través de la red wireless dentro de la empresa.

Se necesita un tiempo de 6 a 8 horas para que la captura sea óptima y se obtenga una handshake que permita encontrar la clave de seguridad de la red WiFi.

El dispositivo wireless dentro de la empresa es el que se detalla a continuación; éste se encuentra conectado a un modem, el cual provee de Internet a toda la empresa:

EQUIPO	CARACTERÍSTICAS
Wireless Router / Access Point  **Figura 5.05 Router Linksys WRT54G** *Fuente: http://www.linksysbycisco.com/EU/es/support/WRT54G*	✓ Router Linksys Wireless-G WRT54G ✓ Estándares: IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b ✓ Banda de Frecuencia: 2.4GHz ✓ Velocidad: 54Mbps (Wireless), 10/100 Mbps (Ethernet) ✓ Tipo de puertos: 4 LAN RJ45, 1 WAN RJ45 ✓ MAC: 00-1C-10-A8-BB-D0 ✓ SSID: ElecdorLinksys

Cuadro 5.02 Router de la empresa Elecdor S.A.

Autor: Andrés Serrano Flores

PASOS

1. Se abre el programa CommView for WiFi y se lo configura correctamente, la conexión inalámbrica de la computadora portátil se establece en modo Monitor para poder empezar con la captura de datos.

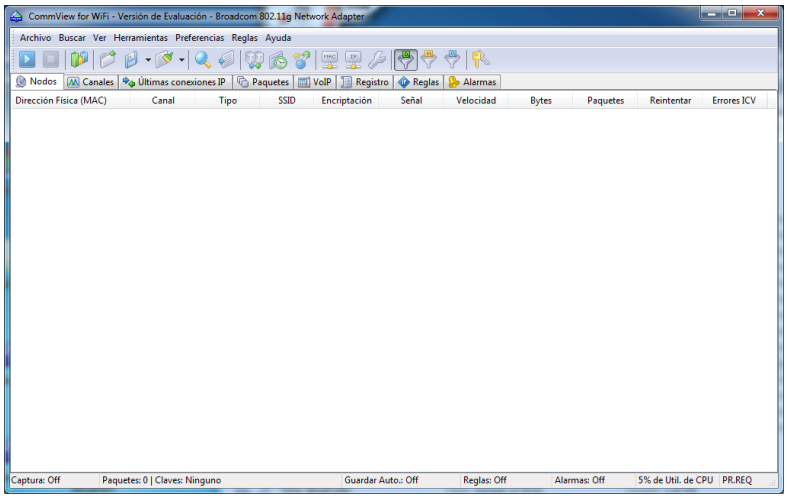


Figura 5.06 Configurando CommView for WiFi en Elecdor S.A.

Fuente: Software CommView for WiFi

2. Se da clic en el ícono Explorar para observar las redes inalámbricas disponibles, entre ellas la red inalámbrica de Elecdor S.A.

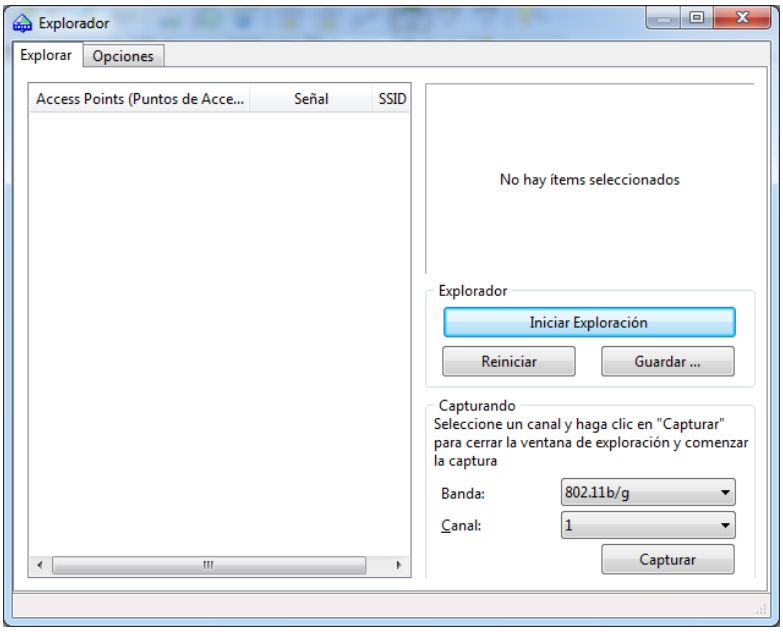


Figura 5.07 Explorador de redes WiFi

Fuente: Software CommView for WiFi

3. Se da clic en el botón Iniciar Exploración para que aparezcan todas las redes WiFi que encuentra el programa CommView.

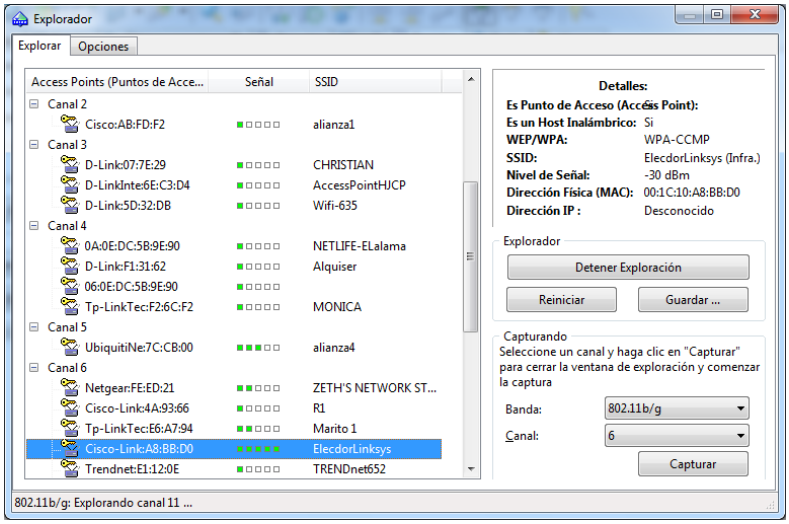


Figura 5.08 Selección de red WiFi

Fuente: Software CommView for WiFi

4. El nombre de identificación de la red es ElecdorLinksys, se señala la red respectiva para comenzar con la captura de los datos.

5. Se da clic en Capturar para empezar a obtener los paquetes de información del canal donde la red seleccionada se encuentra funcionando.

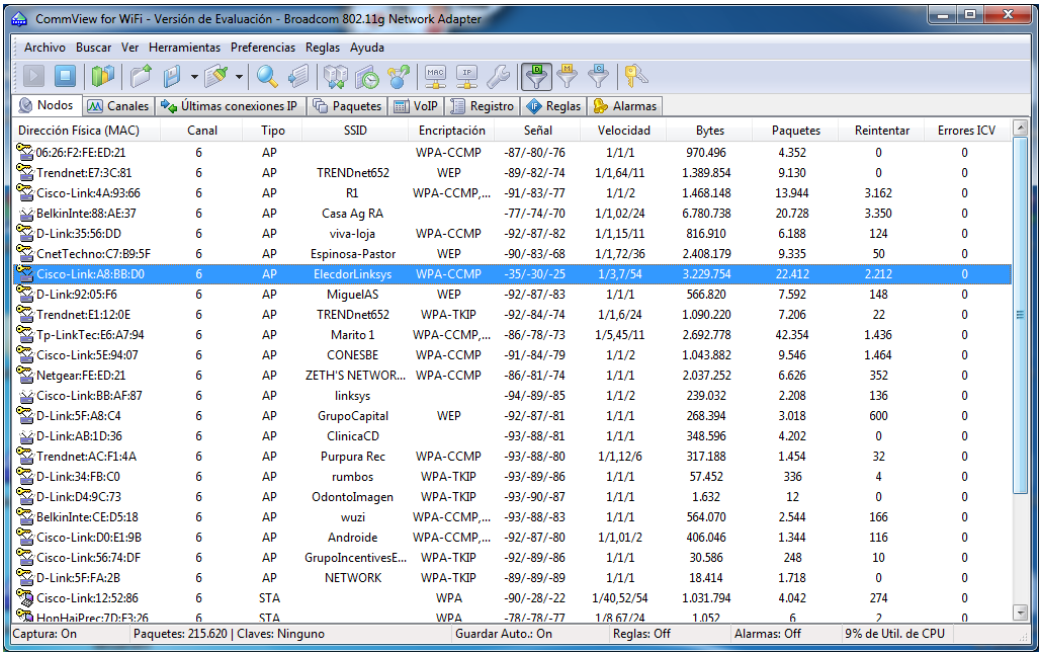


Figura 5.09 Captura de red WiFi

Fuente: Software CommView for WiFi

6. Luego de pasado un tiempo considerable, en el escritorio del equipo portátil aparecerá un archivo que contiene la captura de datos que se ha obtenido con la herramienta CommView.

Figura 5.10 Archivo CommView de captura de la red

Fuente: Software CommView for WiFi

7. Se abre con el Visor de Registros de CommView for WiFi la captura obtenida, y se lo guarda con un nombre cuya extensión es .CAP.

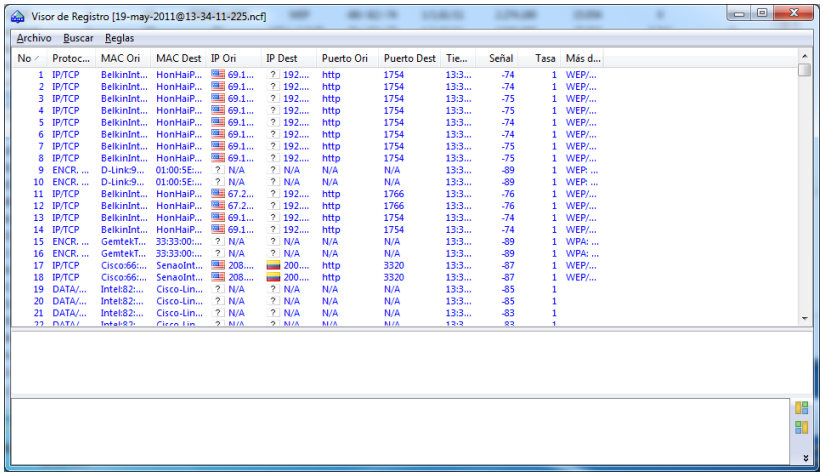


Figura 5.11 Visor de Registros de captura de datos

Fuente: Software CommView for WiFi

8. Para guardar con la extensión deseada, se abre el menú Archivo, seleccionamos Exportar Registros y se da clic en Wireshark/Tspdump.

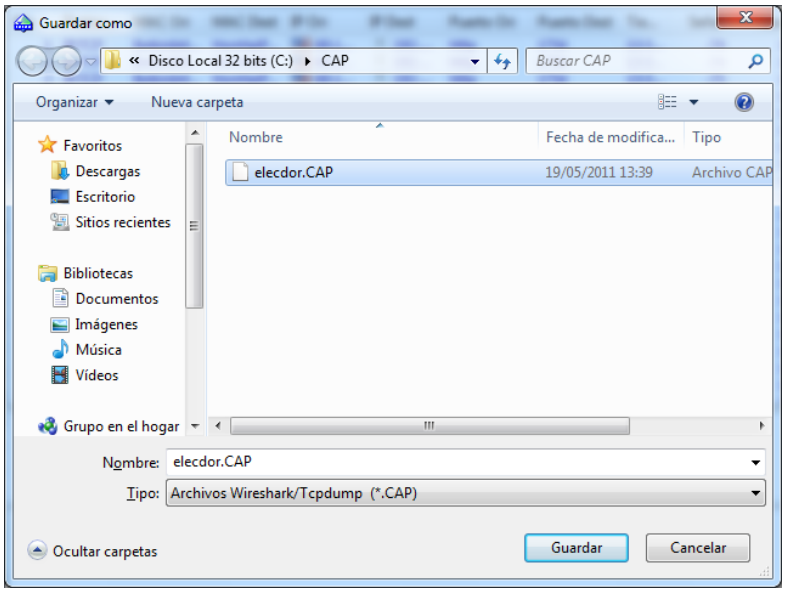


Figura 5.12 Guardando captura obtenida

Fuente: Software CommView for WiFi

9. Se da clic en Guardar y posteriormente se abre la herramienta Aircrack-ng.

Hay que tener en cuenta que el programa Aircrack-ng no distingue entre clave con cifrado WPA personal o WPA2 personal, pero se conoce que dentro de la empresa el cifrado de protección utilizado es WPA2 personal.

Con la herramienta Aircrack-ng, se selecciona el archivo .CAP seleccionado, se escoge la opción WPA y se selecciona un Wordlist. Para ésta ocasión, se personalizó un Wordlist de Internet con más palabras asociadas a la empresa.

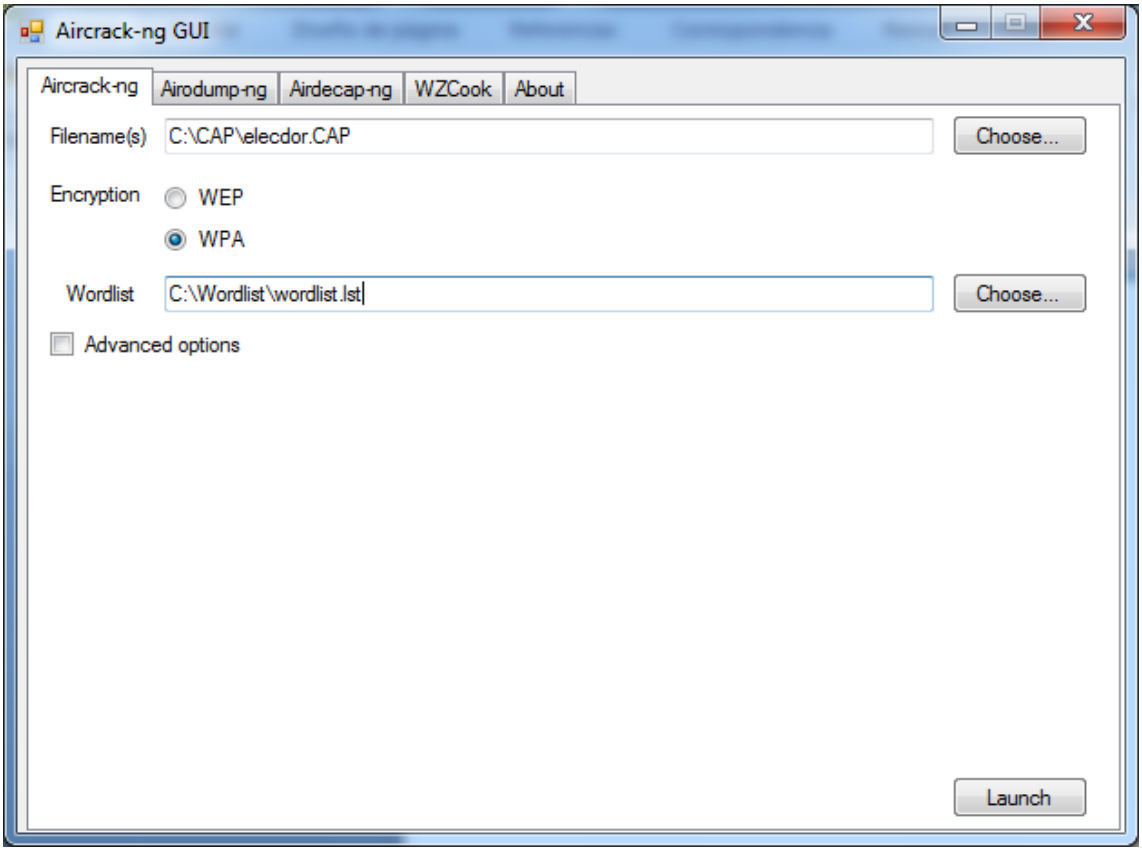
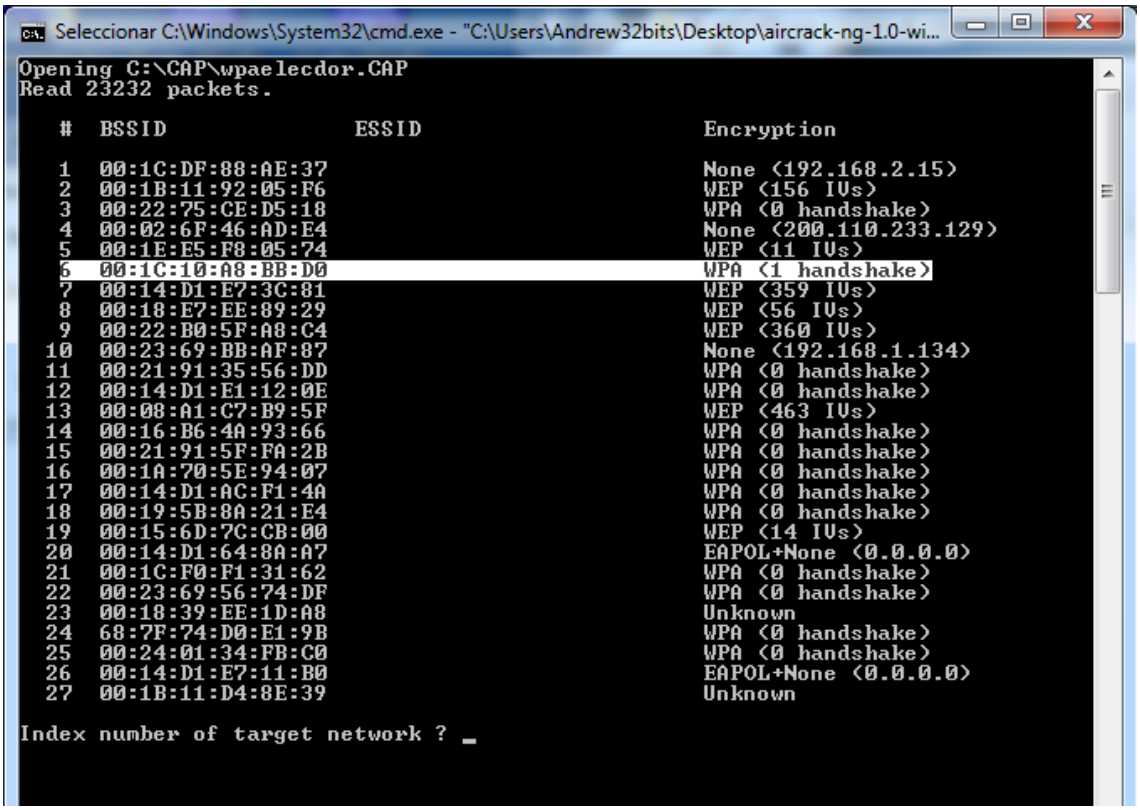


Figura 5.13 Usando Aircrack-ng

Fuente: Software Aircrack-ng GUI

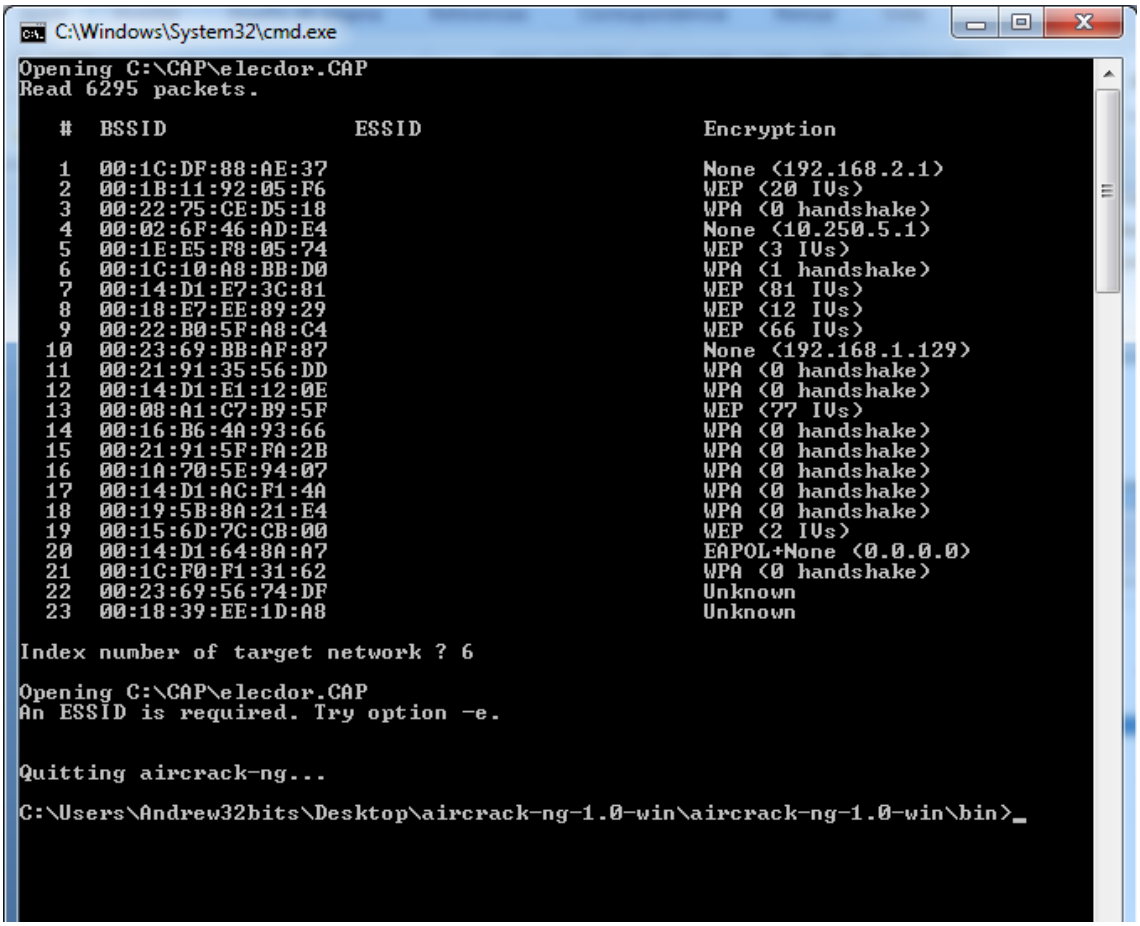
10. Luego de seleccionar la captura obtenida y seleccionando la lista de palabras, se procede a dar clic en Launch para comenzar con la desencriptación de la contraseña WiFi.



Captura 5.01 Redes encontradas durante la captura de paquetes de datos

Fuente: Software Aircrack-ng MS-DOS

11. La captura de datos muestra todas las redes encontradas en el canal dónde también trabaja la red WiFi de la empresa Elecdor S.A. Según la dirección MAC del router WRT54G de la empresa, seleccionamos el número de la red que corresponde a esa MAC: 00-1C-10-A8-BB-D0; se puede observar que se ha obtenido 1 handshake lo que sirve para poder encontrar efectivamente la clave de la red inalámbrica.



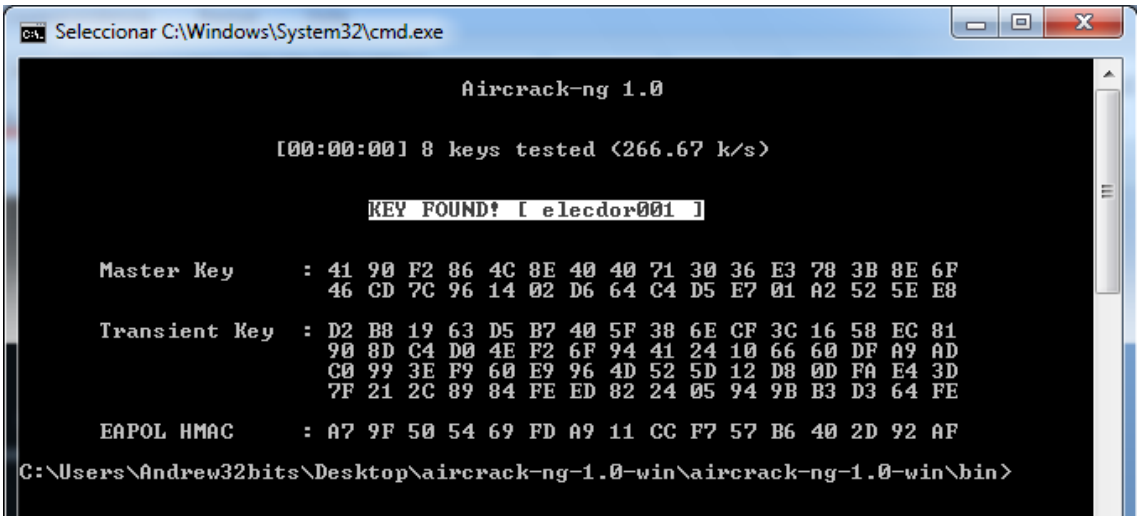
Captura 5.02 Selección de red a descifrar

Fuente: Software Aircrack-ng MS-DOS

12. Se escribe la red que se necesita encontrar la clave cifrada, el programa nos indica que se requiere especificar el nombre de la red, se escribe manualmente las opciones de ejecución:

C:\Users\Andrew32bits\Desktop\aircrack-ng-1.0-win\aircrack-ng-1.0-win\bin>aircrack-ng –w C:\Wordlist\as.txt -b 00:1C:10:A8:BB:D0 -e ElecdorLinksys C:\CAP\elecdor.cap

13. Luego de varios minutos y si dentro del diccionario de palabras se encuentra la clave necesaria, el programa indica que se ha encontrado la clave de la red solicitada.



Captura 5.03 Clave encontrada de la red WiFi de Elecdor S.A.

Fuente: Software Aircrack-ng MS-DOS

14. Para comprobar que efectivamente la clave encontrada es la indicada por el programa Aircrack-ng, tratamos de buscar el nombre de la red usando la tarjeta inalámbrica usd Linksys.

Figura 5.14 Red de la empresa usando la tarjeta inalámbrica USB

Fuente: Conectarse a una red de Windows

15. Nos pedirá la clave de seguridad de la red ElecdorLinksys, ingresamos la que se encontró con el programa de desencriptación. Se da clic en Aceptar y esperamos que se conecte a la red de la empresa.

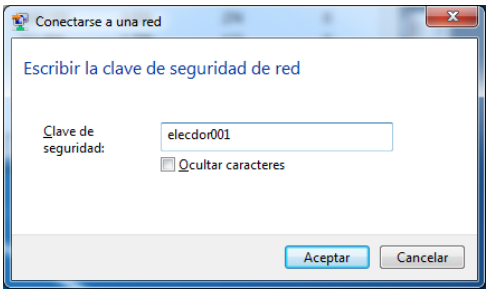


Figura 5.15 Ingreso de clave WiFi de la red

Fuente: Conectarse a una red de Windows

16. Realizamos pruebas conectándonos al Internet y navegamos por algunas páginas para comprobar que nos encontremos dentro de la red inalámbrica de la empresa Elecdor S.A.

17. Automáticamente se almacena la configuración de la red inalámbrica de la empresa Elecdor S.A., donde se observa que el tipo de cifrado de la contraseña es WPA2-personal.

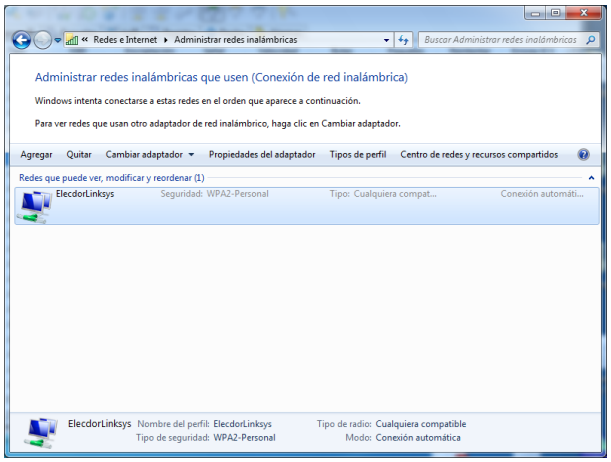


Figura 5.16 Se agrega automáticamente la red WiFi de la empresa

Fuente: Administrar redes inalámbricas de Windows

18. Podemos entrar en las propiedades de la red inalámbrica para observar el Tipo de Seguridad, el Tipo de Cifrado y la Clave de Seguridad de Red.

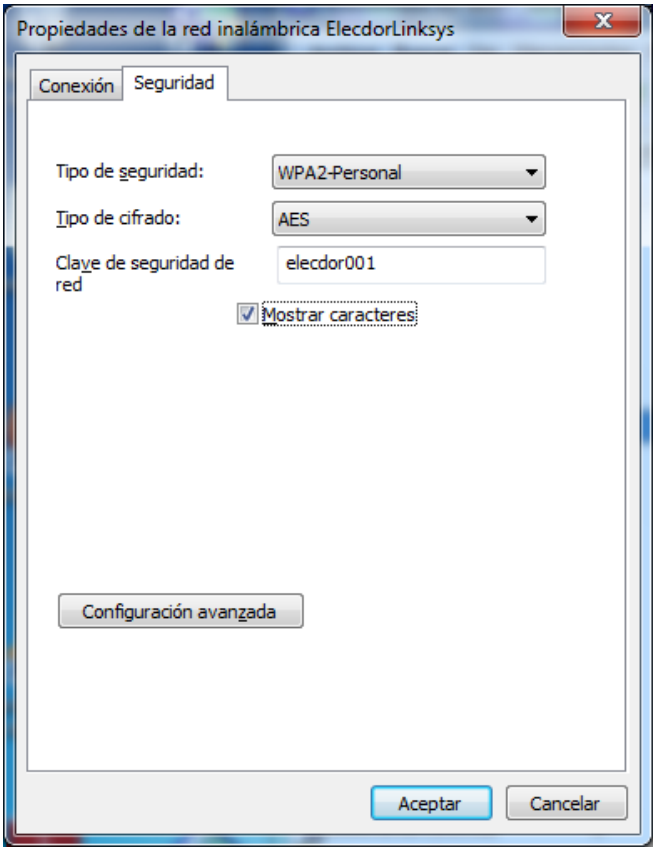


Figura 5.17 Propiedades de la red WiFi

Fuente: Propiedades de la red inalámbrica de WIndows

5.2 EN CAJAS Packing & Design

La empresa EN CAJAS produce cajas, empaques y embalajes para cualquier tipo de necesidad, se encuentra en la capacidad de usar diferentes materiales, siendo la especialidad el cartón micro corrugado personalizado, con la impresión del logotipo o cualquier otro elemento al igual que el color del fondo del cartón que puede ir desde el blanco y el kraf o cualquier otro color.

Figura 5.18 Logo EN CAJAS

Fuente: EN CAJAS

5.2.1 Misión

“Ofrecer un servicio personalizado, para analizar junto al cliente las necesidades y las soluciones que se puede brindar para satisfacerlo, tanto en características como en costos, almacenamiento, transporte, etcétera, porque sabemos que nuestro trabajo tiene la función de ser el valor agregado que va a tener su producto, y por lo tanto debe ser una inversión inteligente.”

5.2.2 Visión

“El resultado de la suma del diseño de la forma, la impresión, el material y el acabado le dará la mejor herramienta publicitaria para que su empresa, negocio, producto o servicio trascienda a través de una eficiente comunicación gráfica que seguro se posicionará rápidamente en el mercado y hará la diferencia con su competencia.”

5.2.3 Valores

Entre los principales valores y principios de la empresa EN CAJAS se tiene:

- ✓ Trabajar para la satisfacción del cliente
- ✓ Contribuir con el desarrollo socio-económico del país.

- ✓ Cuidar el medio ambiente.
- ✓ Trabajar dentro de un ambiente que priorice la seguridad.
- ✓ Respetar y cuidar los recursos de la empresa.

La empresa Encajas se encuentra ubicada en la Calle 6a N85-67 y Avenida Jaime Roldós, sector Mastodontes-Carcelén. En ella se encuentra una pequeña red de 5 computadores enlazados por un router wireless D-Link modelo DIR-280; éste dispositivo se ocupa para compartir el Internet de la empresa y realizar el enlace de todas las computadoras dentro de la misma.

Se detalla el diagrama de la red de la empresa EN CAJAS:

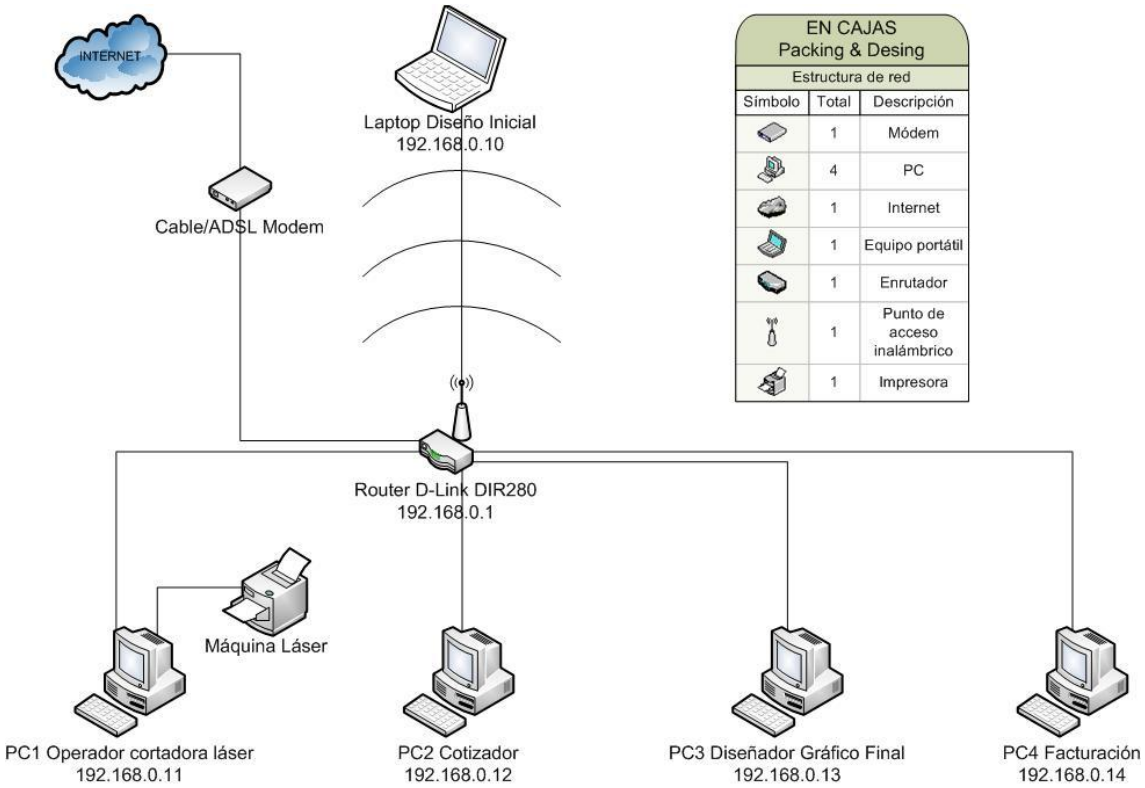


Figura 5.19 Red estructurada EN CAJAS

Autor: Andrés Serrano Flores

5.2.4 Atacando la red

Igualmente, se usa la herramienta CommView for WiFi para obtener los paquetes de datos que viaja a través de la red, que permitirá conseguir la contraseña de seguridad de la red wireless dentro de la empresa.

El dispositivo wireless dentro de la empresa es el que se detalla a continuación; éste se encuentra conectado a un modem, el cual provee de Internet a toda la empresa:

EQUIPO	CARACTERÍSTICAS
Wireless Router / Access Point  **Figura 5.20 Router D-Link DIR-280** *Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=1174*	✓ Wireless Router D-Link DIR-280 ✓ Firewall avanzado y control parental. Seguridad avanzada ✓ Estándares: IEEE 802.11g, compatible con IEEE 802.11b ✓ Banda de Frecuencia: 2.4GHz ✓ Velocidad: 54Mbps (Wireless), 10/100 Mbps (Ethernet) ✓ Tipo de puertos: 4 LAN RJ45, 1 WAN RJ45 ✓ Soporta VPN passthrough. Soporta encriptación WEP. WPA, WPA2 ✓ MAC: 00:21:91:4D:CA:CC ✓ SSID: EnCajas

Cuadro 5.03 Router de la empresa EN CAJAS

Autor: Andrés Serrano Flores

PASOS

1. Inicialmente, se captura el paquete de datos usando el programa CommView for WiFi; abrimos la aplicación, se configura los parámetros de inicio y se selecciona el Explorador.

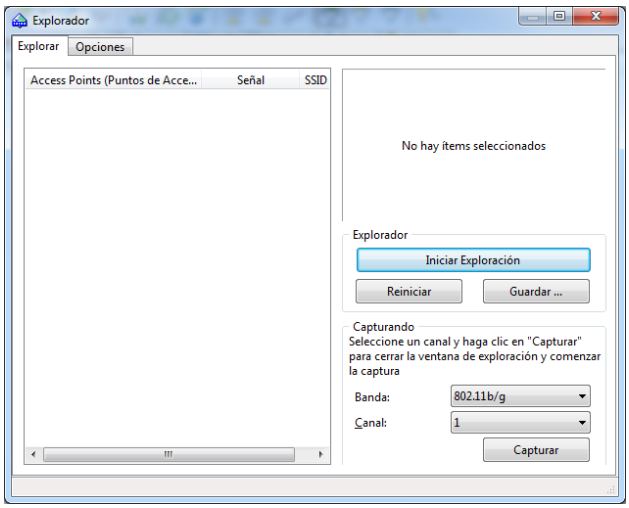


Figura 5.21 Explorador de redes WiFi

Fuente: Software CommView for WiFi

2. Se inicia la exploración y aparecerá la red wireless necesaria.

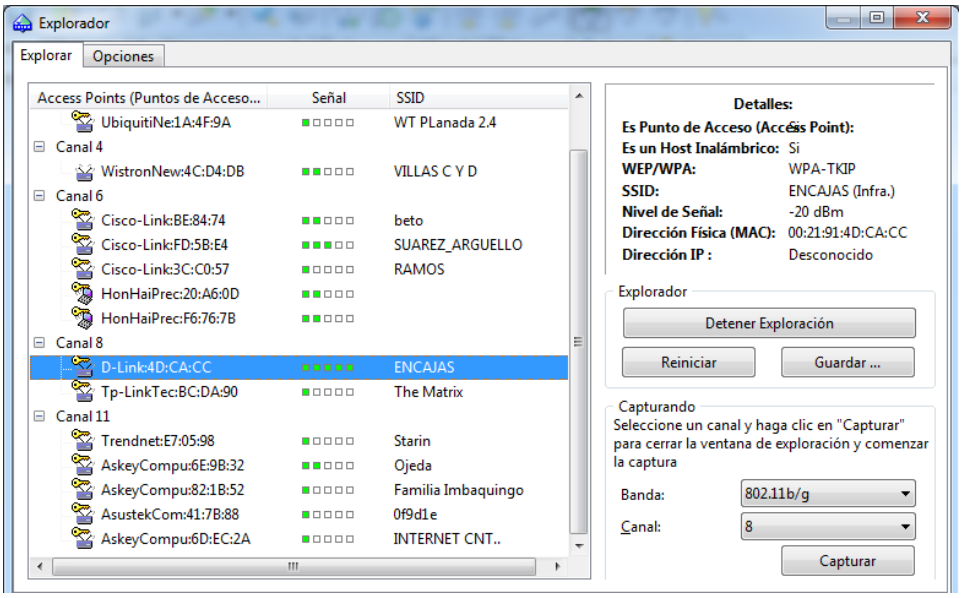


Figura 5.22 Selección de red WiFi

Fuente: Software CommView for WiFi

3. Se selecciona la red y se da clic en el botón Capturar, se empezará a generar la captura del paquete de datos.

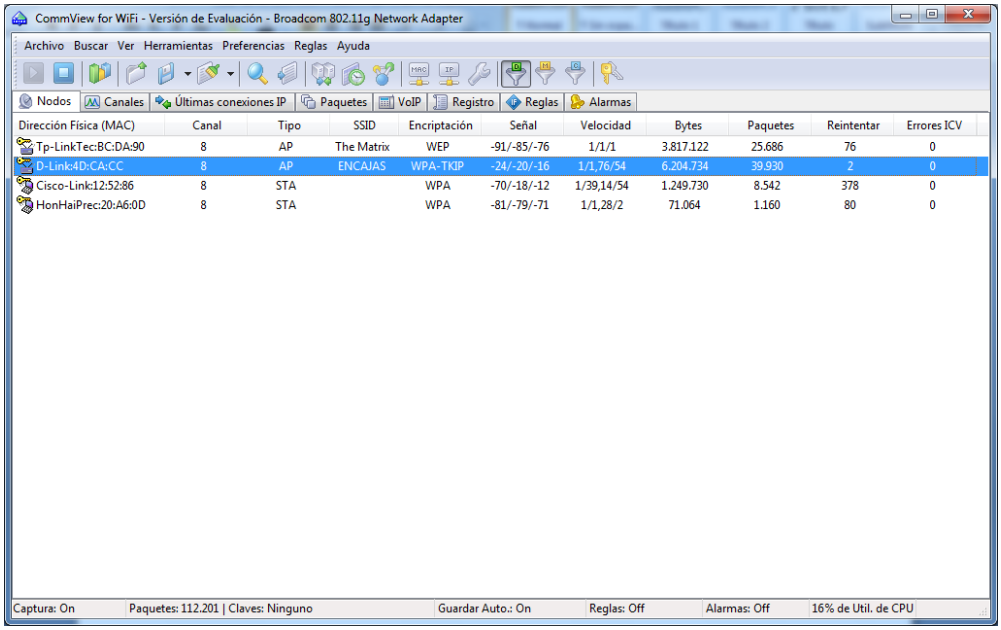


Figura 5.23 Captura de red WiFi

Fuente: Software CommView for WiFi

4. Luego de esperar un tiempo considerado, se procede a abrir el archivo que se crea mediante el Visor de Registro de CommView for WiFi.

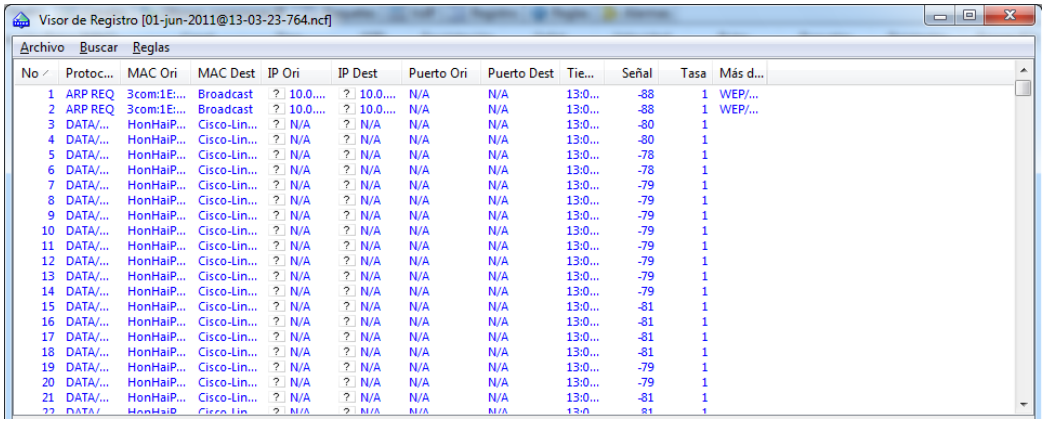


Figura 5.24 Visor de Registros de captura de datos

Fuente: Software CommView for WiFi

5. Se guarda al registro con el nombre encajas.CAP

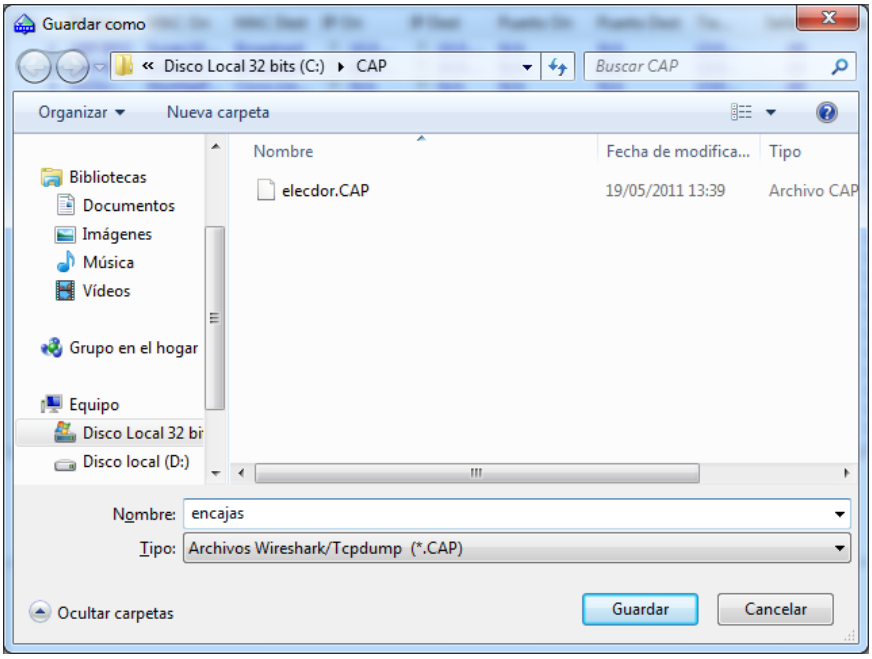


Figura 5.25 Guardando captura obtenida

Fuente: Software CommView for WiFi

6. Se abre el programa Aircrack-ng para proceder a encontrar la clave WiFi, se escoge el archivo de registro creado y se selecciona un diccionario de palabras.

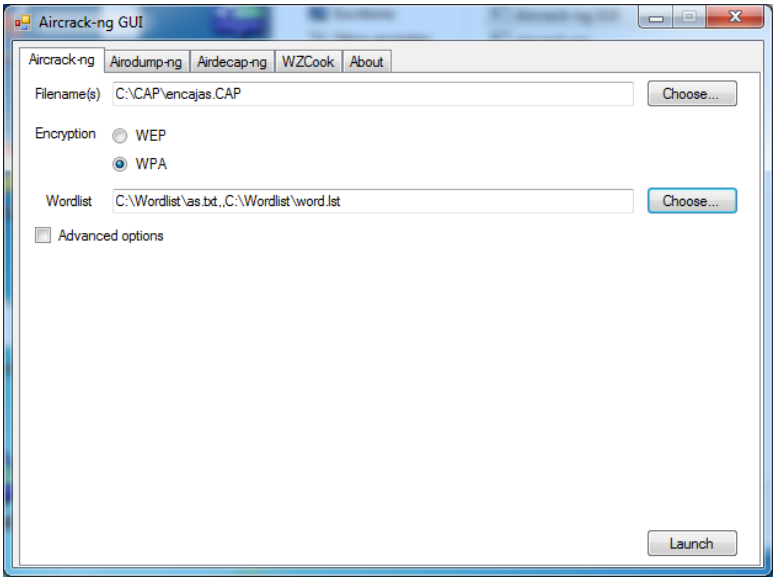
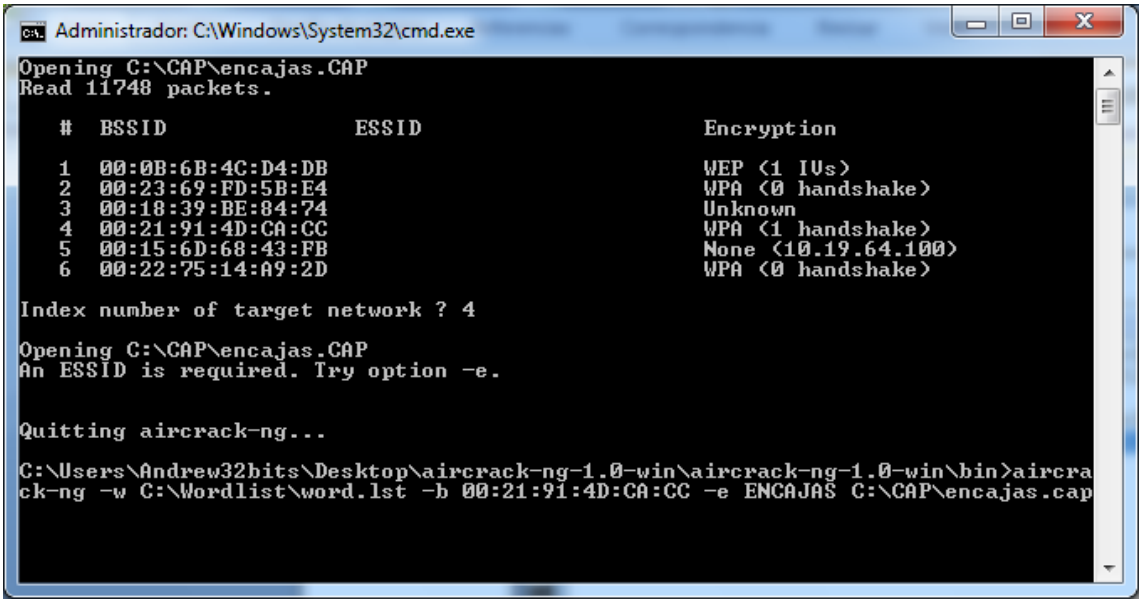


Figura 5.26 Usando Aircrack-ng

Fuente: Software Aircrack-ng GUI

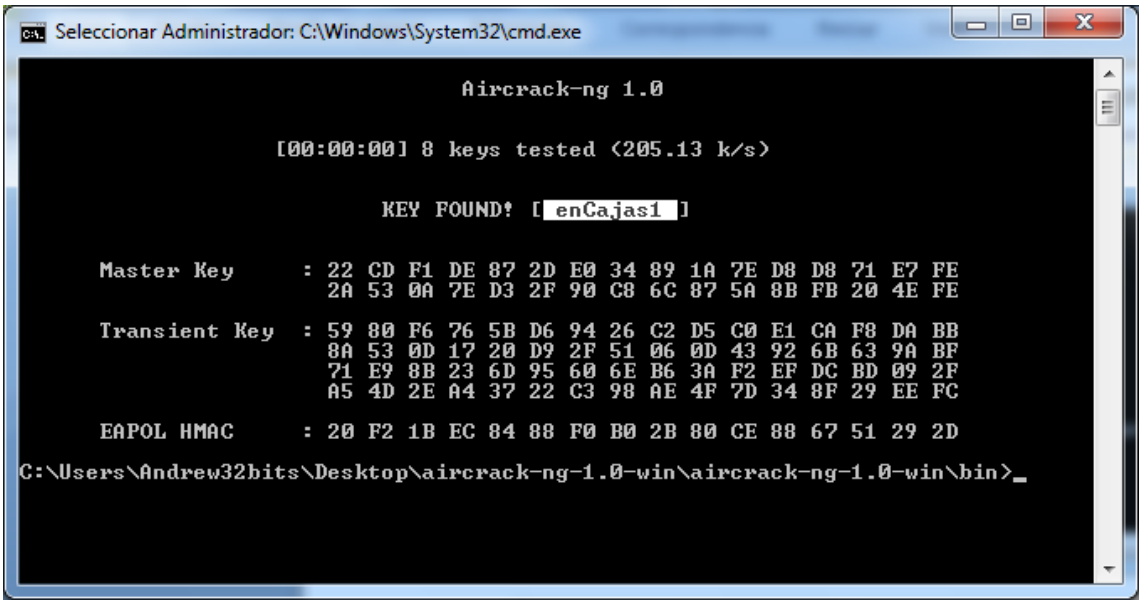
7. Aparecerá en modo DOS las redes capturadas en los paquetes de datos, se coloca el número según pertenezca la red wireless en la que se necesita encontrar la clave.



Captura 5.04 Selección de red a descifrar

Fuente: Software Aircrack-ng MS-DOS

8. Luego de un tiempo, aparecerá la clave wireless que se estaba buscando.



Captura 5.05 Clave encontrada de la red WiFi de EN CAJAS

Fuente: Software Aircrack-ng MS-DOS

9. Para comprobar que la clave encontrada es la de la red, se conecta una computadora vía wireless seleccionando la red y colocando la contraseña.

EMPRESA	TIEMPO DE ATAQUE	ATAQUE EFECTIVO	CONTRASEÑA DE SEGURIDAD
ELECDOR S.A.	6 horas	Si	elecdor001
ENCAJAS	8 horas	Si	enCajas1

Cuadro 5.04 Cuadro Resumen Ataques de Red

Fuente: Andrés Serrano Flores

5.3 Consejos básicos para que la red WiFi sea segura

Luego de observar lo sucedido con las redes inalámbricas y la relativa facilidad de descifrar las contraseñas con las herramientas que encontramos en el Internet, se va a indicar una serie de pasos o consejos orientados a mejorar la seguridad de las redes WiFi.

Muchos hogares y pequeñas empresas del DMQ cuentan en la actualidad con WiFi para la conexión a Internet, y varias empresas que dan servicio Internet incluyen en sus paquetes el modem y el Access Point, que permite compartir el Internet a varios dispositivos.

Uno de los principales consejos, y mientras sea posible, es la de utilizar la conexión mediante cable de red Ethernet a todos los dispositivos, especialmente si es dentro de una empresa, ya que es más estable y rápida que hacerla mediante una red inalámbrica, aunque en algunos casos, el disponer de una conexión WiFi ofrece más libertad y movilidad.

Si se tiene activada la conexión wireless, se debe pensar que además que en el entorno de la empresa, la señal WiFi puede llegar a otros usuarios y que mediante técnicas más o menos "sencillas/complicadas", podrían conectarse a la red, con el riesgo de seguridad que ello puede suponer o al menos por ver

reducidas las velocidades de descarga y subida, lo que va a traducirse en una navegación lenta e incluso nula.

Las diversas opciones de configuración dependerán de cada router o access point, que generalmente vienen con el manual de usuario, o bien buscando información sobre el mismo en webs especializadas.

5.3.1 Seguridades básicas

NOTA: Antes de empezar a modificar las opciones wireless del router o access point para asegurar la red, se debe tener en cuenta que todas las modificaciones tienen que hacerse conectado con cable de Ethernet, la razón por otra parte lógica, es casi seguro que al realizar algún cambio, se pierda la conexión al dispositivo. También se debe anotar todas las modificaciones que se hagan y el apartado que se encuentran.

A continuación se señalan algunos consejos básicos para mantener la red inalámbrica protegida:

- ✓ **Cambiar la contraseña que viene por defecto en el router o punto de acceso.** Todos los dispositivos suelen salir de fábrica con un password por defecto, la sencillez de encontrar páginas en Internet donde hay información de las contraseñas de cada marca de router y access point, hace que un intruso pueda "colgarse" de la red en cualquier momento, por eso una de las primeras medidas pasa por cambiarlo.
- ✓ **Modificar el SSID que viene configurado por defecto.** Es el nombre de la red WiFi, es un código de un máximo de 32 caracteres alfanuméricos, todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. Resulta conveniente cambiar estos nombres por otros mucho menos llamativos como: default, unknown, disconnected, empty, etc. Si el nombre no es sugerente para el atacante, quizá se decida por otros objetivos.
- ✓ **Cifrar la red usando WPA o si el modelo de router/access point lo permite WPA2.** En lugar de utilizar el cifrado WEP que en principio es

más sencillo de vulnerar, se recomienda en la medida de lo posible utilizar cifrados WPA y WPA2, usando contraseñas seguras. Si no queda otra opción que el cifrado WEP, es mejor de 128 bit que de 64 bit; igualmente las contraseñas con este tipo de cifrado es mejor cambiarlas cada dos semanas.

- ✓ **Desactivar el servidor DHCP.** Si se tiene esta opción activada en el dispositivo, cualquier ordenador que tenga su tarjeta de red configurada en *Obtener una IP automáticamente* y se encuentre dentro del área tendrá acceso a la red. Al desactivarlo, cada equipo que quiera conectarse, tendrá que introducir manualmente la información de la red. IP, puerta de enlace predeterminada, DNS, máscara de subred, etc.; de esta manera, sólo el personal calificado que tenga conocimiento de ésta información, será el único que pueda dar acceso a la red inalámbrica de la empresa, mejorando significativamente la seguridad de la misma.
- ✓ **Cambiar la clave de la red WiFi de forma regular.** Se debe cambiar la contraseña de red por lo menos 1 vez al mes, si es cifrado WPA o WPA2, para que de esta manera los usuarios no tengan acceso permanente a la red, ni que automáticamente se conecten los dispositivos wireless.
- ✓ **Cuando no se esté usando la red, apagar el router/access point.** Si no se depende del dispositivo inalámbrico para mantener la línea telefónica sería una buena opción apagar el router cuando no se lo utilice, o en su caso deshabilitar la red WiFi. De esta manera se lo deja nulo.
- ✓ **Limitar el número de equipos a conectarse.** Al delimitar los equipos, se está generando un "tope" en el número de equipos conectados al router o AP.

5.3.2 Consejos para contraseñas seguras

Una contraseña o Clave personal, también denominada con su anglicismo como Password, es un código o combinación de caracteres, utilizado como

medida de seguridad y cuyo objeto es el de proteger el *acceso no autorizado* a un recurso determinado.

Entre varias contraseñas de uso cotidiano tenemos las de las tarjetas de crédito, el pin y el puk del teléfono móvil, la alarma de casa o la oficina, la de bloqueo del televisor, etc., e informáticamente hablando, la de acceso al sistema operativo o a la sesión de usuario, la del Messenger, la de los correos electrónicos, a las cuentas bancarias, a dispositivos wireless como puntos de acceso y ruteadores, etc.

Como se observa, es algo bastante habitual en el día a día de cada persona o empresa y por tanto, hay que prestar una atención máxima, tanto en su empleo como en su elección, discreción y mantenimiento posterior.

Consejos para la elección y empleo de las contraseñas:

- ✓ Una contraseña será más segura cuanto mayor sea la dificultad para averiguarla, pero claro, a veces la elección de contraseñas con combinaciones muy rebuscadas y difíciles de recordar complican su empleo posterior, pero esto nunca debe ser motivo para obviar este aspecto. Existen además programas informáticos que nos permiten almacenarlas para utilizarlas cuando sea necesario.
- ✓ Es importante utilizar contraseñas que estén compuestas por una combinación de caracteres de al menos 8 cifras, compuesto por Letras (mayúsculas y minúsculas), Números (1,2,3,4,5) y Signos (& % $! = ? *· – /) Por ejemplo: Di5/4%$ext&.
- ✓ Dependiendo del recurso que se proteja algunas de estas contraseñas podrán ser en cierto modo más livianas, más cortas, etc., pero aún así, se debe utilizar siempre que sea posible las combinaciones expresadas anteriormente.
- ✓ Para generar las contraseñas, se debe obviar las palabras comunes, de uso habitual o que se encuentren en el diccionario, en lo posible, no utilizar alguna fecha de nacimiento o de familiares, matrícula del auto u otros datos relacionados, que alguien puede conocer y por tanto deducir.

- ✓ Por supuesto sobra decir que la contraseña es secreta y como tal debe tratarse. No se debe dejar al alcance de otras personas, poca validez puede tener por ejemplo la contraseña para arrancar nuestro equipo si la dejamos colocada en la pantalla con un Pos-it.
- ✓ Una buena práctica, es la de cambiar las contraseñas periódicamente, quizás no es necesario hacerlo todos los días pero si hay que hacerlo de vez en cuando y sobre todo, siempre cambiarlas tras aquellos supuestos en que el equipo haya estado comprometido (infectado por algún troyano, virus, etc.).
- ✓ No es aconsejable utilizar la opción que nos ofrecen determinados programas y navegadores web para guardar o recordar las contraseñas automáticamente, para que en accesos posteriores no se tenga que introducirla; siempre hay que pensar que otro usuario podrá acceder a ese programa o página web.
- ✓ Evitar en lo posible el utilizar la misma contraseña para todo.

5.3.3 Soluciones adicionales de protección

Además de los métodos y las opciones ya vistos que ofrecen los diferentes dispositivos wireless para garantizar la seguridad y confidencialidad en una WLAN, existen otros métodos que pueden ser utilizados, y no están directamente relacionados con la encriptación. Muchas de las soluciones requieren una configuración mínima en los equipos, los que les hace sencillas de implementar incluso por personal no profesional:

- ✓ **Filtrado de direcciones MAC:** se trata de una opción de autentificación adicional, que ofrecen muchos puntos de acceso y ruteadores, en el cual sólo se permite la conexión de ciertas tarjetas de red identificadas a partir de su dirección MAC. Esta es una medida muy fiable de identificar físicamente a los equipos, ya que es muy difícil que dos tarjetas de red tengan la misma MAC, de la misma manera resulta muy apta para entornos pequeños (pequeñas redes domésticas o de oficina). Sin embargo, si la red presenta un tamaño considerable y el número de equipos que acceden a ella es muy grande, se puede volver difícil de

gestionar. Igualmente, si se opta por este tipo de seguridad, una buena práctica es la de revisar cada cierto tiempo la lista de equipos (direcciones MAC) que hacen uso de la red.

- ✓ **Utilización de redes privadas virtuales (VPN):** se conoce que las VPN emplean tecnologías de cifrado para crear un canal virtual privado, de forma que aprovechan una infraestructura pública para simular una red privada. De este modo las VPN se pueden utilizar para proteger redes inalámbricas ya que proporcionan una doble funcionalidad. Por un lado se encarga de autentificar y autorizar a todos los clientes inalámbricos, y por otro lado se encargará de encriptar el tráfico desde y hacia esos clientes, mediante el empleo de IPSec, de este modo no será necesario hacer uso del débil cifrado WEP.
- ✓ **Limitar la potencia de emisión de los puntos de acceso o ruteadores:** se debe adecuar la potencia de emisión de las antenas de los AP o routers a las necesidades reales de la empresa. No resulta sensato, en lo que ha seguridad se refiere que nuestra antena de radio de cobertura de cientos de metros si solamente se pretende dar servicio en una pequeña red doméstica o de oficina. Si el AP o router tiene un radio de cobertura muy amplio, todo aquel que pretenda sacar provecho de la red WLAN, no necesitará ni siquiera acceder al recinto físico donde se encuentra ubicada, podrá llevar a cabos sus intentos de acceso ilegal cómodamente desde cualquier otro lugar sin que nadie sea advertido de ello.
- ✓ **Desactivar la difusión del nombre de la red (broadcast del SSID):** o lo que es lo mismo, que no haga público el nombre SSID (nombre de la red) que el router o access point difunde. La difusión de SSID permite que los nuevos equipos que quieran conectarse a la red inalámbrica identifiquen automáticamente los datos de la red, evitando así la configuración manual. Al desactivarlo, se tendrá que introducir manualmente el SSID en la configuración de cada nuevo equipo que se quiera conectar. Aunque el AP/router se encuentre funcionando en modo pasivo, resulta considerablemente sencillo averiguar el SSID analizando los paquetes de radio que circulan por la WLAN, pero no deja

de ser una medida adicional que dificulta la tarea a los posibles asaltantes.

- ✓ **Activar el cortafuegos (Firewall):** En la actualidad, los puntos de acceso y routers incluyen un sistema de cortafuegos que incorpora opciones predeterminadas. Se puede revisar la lista de puertos autorizados y bloqueados dentro de cada dispositivo wireless para configurarlos manualmente según las necesidades.
- ✓ **Usar cifrado AES en contraseñas WPA2:** un enrutador inalámbrico que soporte WPA/WPA2 generalmente usa dos tipos cifrado, AES y TKIP; el cifrado con TKIP es vulnerables a ataques de diccionario, así que lo mejor es usar WPA2 con cifrado AES ya que todavía no se ha encontrado forma de quebrantarlo.

CONCLUSIONES

Al terminar esta investigación, se tiene que los sistemas wireless no pretenden sustituir a las tradicionales redes cableadas, pero si pueden llegar a ser un complemento de éstas. Las redes inalámbricas proporcionan facilidades no disponibles en los sistemas cableados, lo que al juntar los dos sistemas se puede formar una red total con mayores beneficios. Por las ventajas que prestan las redes WiFi, éstas ya han sido implementadas en lugares públicos, instituciones públicas; pequeñas, medianas y grandes empresas, en universidades y colegios para entregar una mayor movilidad a sus usuarios.

Luego de haber revisado, investigado y obtenido resultados usando diferentes programas que se encuentran en Internet para capturar paquetes de datos de redes WiFi y para encontrar las claves de protección cifradas, se presentan las siguientes conclusiones:

- En base a la investigación realizada, y como parte principal de éste documento, se puede concluir que una de las desventajas y en la actualidad uno de los mayores problemas de las redes inalámbricas es su seguridad, ya que el medio de transmisión que se usa es el aire y es de fácil acceso para cualquier persona que se encuentre dentro del alcance de la red, y que teniendo el software necesario podría capturar la señal y decodificarla.

Los programas revisados en este trabajo (CommView for WiFi y Suite Aircrack.ng), son algunos de los varios más que se pueden encontrar en Internet, tanto para captura de tráfico como para decodificar las contraseñas de las redes WiFi, y es relativamente fácil la obtención y el uso de éstas herramientas.

- Si se desea implementar una red wireless en el hogar, oficina o institución, es necesario conocer a fondo el dispositivo wireless a adquirir, de manera que éste posea el último cifrado de seguridad conocido WPA2, y que permita además poder seleccionar el tipo de cifrado (TKIP, AES) y el tipo de modo (PSK, EAP).

Por defecto, en la mayoría de los dispositivos wireless a usar cuando se selecciona el tipo de seguridad WPA2 personal el cifrado es una combinación TKIP-PSK, lo que nos conlleva a que la contraseña deberá ser una palabra familiar, pero que no tenga mucho significado en un entorno externo, o a su vez una serie de letras y dígitos, en ambos casos, intercalando con letras mayúsculas.

- Otra de las conclusiones es que las redes inalámbricas revisadas, solamente usan los dispositivos wireless para compartir Internet, no se utiliza éste tipo de red para transmitir información importante de la empresa, ni para poder acceder a un programa, base de datos u otro software de un servidor o de un computador.

En la mayoría de lugares públicos o privados, los routers o APs se ocupan para compartir la conexión a Internet que se posea, convirtiéndose así en un servicio. Esto es beneficioso para la empresa u organización, pero también tiene su desventaja porque si existen varios dispositivos conectados a la red wireless, la velocidad de subida y bajada de Internet se vería afectada y ya no se sería un servicio óptimo.

- Se concluye también que el cifrado de seguridad WEP es fácilmente quebrantable, y que los cifrados WPA/WPA2 personal pueden ser vulnerados, siempre y cuando se tenga un diccionario de palabras que contenga la clave de la red WiFi y que dicha contraseña se haya configurado con el protocolo por defecto TKIP-PSK.

Se conoce que para configurar una clave de seguridad en modo EAP o con cifrado AES se necesita un servidor de autenticación externo, haciendo que la seguridad WPA y WPA2 se convierta en enterprise (empresarial), lo cual no es uno de los objetivos de estudio de ésta investigación.

- Se concluye además que los objetivos planteados en esta investigación se han cumplido en su totalidad, ya que se han investigado las diferentes tecnologías y protocolos existentes que se usan en las redes WiFi.

Con las prácticas realizadas en las empresas, se obtuvieron resultados que ayudaron a comprender las virtudes y las deficiencias de éstos protocolos, y ha

permitido sugerir varios consejos que sirven para mejorar las seguridades de las redes inalámbricas en general.

- Finalmente, como conclusión general, se puede decir que al implementar una red WiFi, se debe utilizar todas las herramientas disponibles en cada dispositivo, dependiendo de la necesidad de la organización, como es: configurar el nombre SSID, seleccionar el tipo de seguridad, usar DHCP o IPs fijas, utilizar filtrado MAC, generar contraseñas usando letras mayúsculas, minúsculas y dígitos, definir un rango de señal máximo, etc., que permitirá administrar de una mejor manera nuestra red.

RECOMENDACIONES

- Se recomienda tener mucho cuidado en la configuración de los equipos que servirán para capturar y descifrar los datos (computadores, laptops, tarjetas o adaptadores inalámbricos, etc.), ya que cualquier mala práctica puede ocasionar que dejen de funcionar correctamente, por lo que se sugiere seguir los pasos indicados en el presente trabajo tanto en la configuración de los adaptadores de red inalámbrica como de los programas CommView for WiFi y el suite Aircrack-ng.

- Se recomienda que al configurar el Access Point o el Router Inalámbrico de la empresa u organización para mejorar su seguridad, siempre se debe leer primero la documentación para conocer las demás herramientas que posee cada dispositivo, de manera que se pueda modificar las configuraciones de fábrica y otras adicionales.

- Si se va a instalar una red WiFi dentro de un entorno empresarial, se recomienda que el dispositivo inalámbrico, entre sus características, permita el cifrado WPA/WPA2 personal, ya que dichos cifrados son los más seguros en la actualidad; cabe recalcar que la contraseña a implementar debe contener letras mayúsculas, minúsculas y dígitos para que su seguridad sea mayor.

- A los usuarios de las empresas, se recomienda tener cuidado con las claves, no deben anotarlas en post-it, hojas sueltas, notas en el computador, etc. ya que personas ajenas a la organización podrían obtener esa información y de manera maliciosa podrían ingresar y alterar la configuración WiFi, provocando daños o haciendo que la red funcione de una manera incorrecta.

- La manipulación de los dispositivos WiFi, en el caso más básico, deberían ser administrados por personal capacitado o que posean conocimientos de Computación, un usuario sin conocimientos técnicos no debe ser la persona que administre los dispositivos o la red en sí.

- En la mayoría de los servicios de Internet, se ofrecen también conexión WiFi, la que es administrada por personal de dichas empresas; se recomienda sugerir que para la contraseña a configurar se use el cifrado WPA o WPA2 y

que tenga una complejidad de mediana a alta para mejorar su seguridad, en el caso en que la empresa no posea personal capacitado para esto.

- Las claves de seguridad de las empresas donde se realizó el estudio, se encuentran configuradas en cifrado WPA personal, se recomienda configurarlas en cifrado WPA2 personal y, en lo posible, deberán ser cambiadas unas 3 o 4 veces al año, de manera que si por alguna razón éstas han sido descifradas, en un corto tiempo volverán a ser seguras.

- Se recomienda a la Facultad de Ingeniería, en la Escuela de Sistemas, que se profundice más en lo referente a seguridades en dispositivos de Redes Informáticas, tanto los cifrados de seguridad como funciones adicionales de protección; ya que en la actualidad, éstos son usados comúnmente y en un futuro cercano llegarán a ser una parte fundamental de cualquier red estructurada que se vaya a implementar.

GLOSARIO DE TÉRMINOS

A

- **Ad-hoc:** una red wireless ad-hoc es un grupo de ordenadores, cada uno con un adaptador WLAN, conectados como una red inalámbrica independiente.
- **Algoritmo MD5:** (*Message-Digest Algorithm 5*, *Algoritmo de Resumen del Mensaje 5*) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado, representada típicamente como un número de 32 dígitos hexadecimal. El código MD5 fue diseñado por Ronald Rivest en 1991.
- **Algoritmo SHA1-HMAC:** es un tipo de algoritmo *hash en clave que se crea desde la *función hash SHA1 y se utiliza como HMAC o como código de autenticación de mensajes basado en hash. El proceso HMAC combina una clave secreta con los datos de mensaje, aplica el algoritmo hash a los resultados con la función hash, combina de nuevo ese valor hash con la clave secreta y, a continuación, aplica la función hash por segunda vez. El valor hash de salida tiene una longitud de 160 bits.

  ***hash:** es un algoritmo criptográfico para generar claves, es de orden unidireccional (sólo encripta, pero no desencripta), la misma cadena da el mismo resultado. Los hash son usados en la mayoría de las PC, cuando se introduce la clave de un usuario (y el usuario), ésta se convierte en una clave de números y caracteres (el hash se encarga de esto) y es comparada con la clave almacenada.

  ***función hash:** es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor.
- **AES:** (*Advanced Encryption Standard*) también conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.
- **AP:** *(Access Point*, *Punto de Acceso*) es un dispositivo repetidor de la señal para aumentar el alcance de una red inalámbrica.

B

- **Beacons:** número de paquete de datos o tramas que emiten los AP, o en su defecto routers inalámbricos, para que otros AP o tarjetas inalámbricas sepan que existe un AP activo por las cercanías.
- **Broadcast:** es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea.
- **Broadcast SSID:** es una configuración dentro del AP o router inalámbrico, el cual hace que el SSID sea público, es decir, que cualquiera que entre dentro del radio de acción del dispositivo, pueda ver el SSID.
- **BSS:** (*Basic Service Set*) una específica red ad-hoc es llamada como un BSS. Computadoras en un BSS deben ser configuradas con el mismo *BSSID.

  ***BSSID:** es la Dirección MAC del punto de acceso.

C

- **CCMP:** (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) es un protocolo que utiliza AES como algoritmo criptográfico y proporciona integridad y confidencialidad. Fue creado para reemplazar TKIP.
- **CMA/CA:** (*Múltiple Acceso de Portadora Evitando Colisiones*) protocolo de control de redes que se utiliza para prevenir colisiones entre los paquetes de datos.
- **Cisco:** Cisco Systems es una empresa líder en el ramo de las telecomunicaciones y tecnologías de la información, especializada principalmente en el networking o redes.
- **CRC:** *(Cyclic Redundancy Check*) es un algoritmo o código de redundancia cíclica que permite comprobar la fiabilidad y la no alternación de los datos.

- **CRC-32:** el algoritmo CRC-32 se utiliza para proteger la integridad de los datos al verificar que dichos datos no han sido alterados, comparando el CRC-32 de los datos enviados con el CRC-32 de los datos recibidos. Si se modifica aunque sea un punto de los datos iniciales, el resultado del CRC-32 es completamente diferente.

D

- **DHCP:** (*Dynamic Host Configuration Protocol*, *Protocolo Dinámico de Configuración de Puestos*) diseñado por Microsoft, su principal tarea consiste en asignar de manera automática las direcciones IP a los puestos de una red *TCP/IP.

  ***TCP/IP:** (acrónimo de *Transmission Control ProtocolInternet Protocol*) conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.
- **Dirección MAC:** (*Media Access Control Address*) es la identificación única de cada placa de red, también es conocida como dirección física MAC. Está compuesta de 48 bits en formato hexadecimal, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE, los primeros 24 bits y por el fabricante los últimos 24.
- **D-Link:** D-Link Corporation es una empresa electrónica que fabrica componentes de red, como tarjetas de red, puntos de acceso, routers, firewalls, etc.

E

- **EAP:** (*Extensible Authentication Protocol, Protocolo de Autenticación Extensible*) es una extensión del protocolo punto a punto que admite métodos de autenticación arbitrarios que utilizan intercambios de credenciales e información arbitrarias.
- **EAPOL:** *(EAP over LANs*) es el protocolo EAP en redes LAN.
- **ESS:** (*Extended Service Set*) es una extensión del modo de configuración BSS. Los nodos wireless y AP dentro de un ESS deben ser configurados en el mismo *ESSID y en el mismo canal (radio cannel).

  ***ESSID:** Conocida como SSID, puede estar vacía si el ocultamiento de SSID está activo.

- **Ethernet:** es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos.

G

- **GUI:** (*Graphical User Interface*) es un modo de interfaz de usuario basada en gráficas que incorpora iconos, menús despegables, imágenes, etc., los cuales representan funciones, acciones e información; se utiliza generalmente el puntero mouse.

H

- **Handshake:** es el protocolo de comienzo de comunicación entre dos máquinas o sistemas. Se genera cuando un cliente se asocia a la red inalámbrica, son los paquetes que se envían entre el AP y el cliente en el momento de la asociación. Para que poder empezar el ataque con diccionario en una red con cifrado WPA-PSK, se necesita haber capturado estos paquetes.
- **Hashing:** es una técnica que consta de datos de entrada, una función hash y una salida.

I

- **ICMP:** (*Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet*) es un subprotocolo de diagnóstico y notificación de errores del IP. Es utilizado para enviar mensajes de errores cuando un servicio no está disponible o cuando un host no puede ser encontrado, etc.
- **ICV:** (*Integrity Check Value*) es un valor de comprobación que permite a un sistema de tecnología de información detectar cambios o errores en los datos, así como asegurar la integridad de los datos.
- **IEEE:** (*Institute of Electrical and Electronics Engineers*) organización científica que define los estándares industriales y protocolos para el manejo de la tecnología. Sitio oficial: http://www.ieee.org/

- IP: (*Internet Protocol, Protocolo de Internet*) es un protocolo para la comunicación en una red a través de paquetes conmutados, es principalmente usado en Internet.
- IPsec: es un protocolo que está sobre la capa del protocolo de Internet (IP). Le permite a dos o más equipos comunicarse de forma segura (de ahí el nombre).
- **IV:** (*Vector de Inicialización*) es un bloque de bits requerido para lograr un cifrado en flujo o un cifrado por bloques, en uno de los modos de cifrado, con un resultado independiente de otros cifrados producidos por la misma clave. El tamaño del IV dependen del algoritmo de cifrado y del protocolo criptográfico y a menudo es tan largo como el tamaño de bloque o como el tamaño de la clave.

K

- **Keystream:** es una secuencia de caracteres pseudoaleatorios. El *keystream* lo produce el algoritmo RC4 en función de la clave (40 bits) y el IV (24 bits).

L

- **LAN:** (*Local Area Network*, *Red de Área Local*) es una red de comunicaciones que sirve a usuarios dentro de un área geográficamente limitada.
- **LDAP:** (*Lightweight Directory Access Protocol*) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
- **Linksys:** es una división de Cisco Systems que vende productos para redes domésticas y de pequeños negocios.

M

- **MIC:** (*Message Integrity Code*, *Código de Integridad de Mensaje* o *Michael*) es un código (algoritmo) que verifica la integridad de los datos de las tramas.

N

- **NIC:** (*Network Interface Card, Tarjeta de Interfaz de Redes*) es una tarjeta de circuito impresa que se conecta a una estación de trabajo o a un servidor, controla el intercambio de datos en una red.

O

- **OFDM:** (*Orthogonal Frequency Division Multiplexing*) Técnica de modulación *FDM que permite transmitir cantidades de datos digitales sobre una onda de radio. OFDM divide la señal de radio en varias sub-señales que se transmiten simultáneamente hacia el receptor en diferentes frecuencias. OFDM reduce la diafonía (efecto de cruce de líneas) durante la transmisión de la señal.

  ***FDM:** (*Frequency Division Multiplexing, Multiplexación por División de Frecuencia*) es un tipo de multiplexación utilizada generalmente en sistemas de transmisión analógicos.

P

- **PMK:** (*Pairwise Master Key, Clave Maestra en Pares*) es una "Llave Maestra" creada por un hash entre la passphrase (contraseña) y el SSID.
- **PRNG:** (*Pseudo-Random Number Generator*) es un algoritmo matemático que produce una sucesión indefinida de números aleatorios (pseudoaleatorios).
- **PSK:** (*Pre-Shared Key*) viene a significar Clave Compartida Previamente, está diseñado para uso doméstico y redes de oficinas pequeñas, en las cuales cada usuario basa su seguridad en una misma contraseña.

R

- **RADIUS:** (*Remote Authentication Dial-In User Service*) es un protocolo de autentificación y autorización para aplicaciones de acceso a red o movilidad IP.

- **RC4:** es un algoritmo de cifrado de flujo (funciona expandiendo una clave secreta) y es parte del protocolo de cifrado WEP.
- **RCP:** (*Remote Procedure Call, Llamada a Procedimiento Remoto*) es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.
- **Router:** es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
- **RSA Security:** es una empresa dedicada a la criptografía y al software de seguridad.
- **RTP:** (*Real Time Transport Protocol*) es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, generalmente define un formato de paquete estándar para el envío de audio y video sobre Internet.
- **RTCP:** (*Real Time Transport Control Protocol*) RTP y RTCP están ligados. RTP envía los datos y RTCP es utilizado para realimentación acerca de la calidad de servicio.

S

- **Seed:** es un valor secreto usado para inicializar una función u operación criptográfica, conocido también como "semilla".
- **Servidor AAA:** (*Authentication Authorization Accounting*) es un servidor configurado para desempeñar las tareas de autentificación, autorización y contabilidad.
- **SHA-1:** (*Secure Hash Algorithm*, *Algoritmo Hash Seguro*; también llamado SHS, *Secure Hash Standard*, *Estándar de Hash Seguro*) es un algoritmo hash criptográfico publicado por el gobierno de Estados Unidos. Genera un valor hash de 160 bits a partir de una cadena de longitud arbitraria.

- **Sniffer:** es una utilidad diseñada para capturar el tráfico (datos) que viaja por redes de tipología Ethernet o dentro de una red de cómputo.
- **Sniffing:** es la acción que permite al atacante "escuchar" las diversas comunicaciones que se establecen entre ordenadores a través de una red (física o inalámbrica) sin necesidad de acceder física ni virtualmente a un ordenador de la misma red, utilizando dispositivos y programas de computación.
- **SSID:** (*Service Set IDentifier*) es el identificador que tienen los puntos de acceso y que distinguen una red inalámbrica de otra.
- **SSL:** (*Secure Socket Layer*) es un protocolo que proporciona servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico.

T

- **TCP:** (*Transmission Control Protocol*) es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte.
- **TKIP:** (*Temporal Key Integrity Protocol*) es un protocolo de seguridad usado en WPA para mejorar el cifrado de datos en redes inalámbricas.

U

- **UDP:** (*User Datagram Protocol*) es un protocolo del nivel de transporte basado en el intercambio de datagramas y permite el envío de datagramas a través de la red sin que se haya establecido una conexión previa.

V

- **VPN:** (*Virtual Private Network*) tecnología que permite la transmisión de información privada sobre redes de uso público de manera segura, utilizando conexiones virtuales.

W

- **WECA:** (*Wireless Ethernet Compability Alliance, Alianza de Compatibilidad Ethernet Inalámbrica*) es el antiguo nombre formal de la Wi-Fi Alliance.
- **WEP:** (*Wired Equivalent Privacy*) es un sistema de encriptación incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite.
- **Wi-Fi Alliance:** Organización creada por líderes proveedores de software y equipos inalámbricos con la misión de certificar los productos basados en el 802.11. Sitio oficial: http://www.wi-fi.org/
- **WPA:** (*Wi-Fi Protected Access*) es un protocolo creado para solucionar los problemas de seguridad del WEP, basada en el protocolo de encriptación TKIP.
- **WPA2:** es una mejoría del protocolo WPA que utiliza el algoritmo de encriptación AES.
- **WLAN:** (*Wireless Local Area Network*) es una red de comunicaciones inalámbrica, utilizado como alternativa a las redes LAN cableadas.
- **WNIC:** (*Wireless Network Interface Card*) Tarjeta de Red Inalámbrica 2
- **Wordlist:** es un listado de palabras, almacenadas en un archivo con extensión .txt o .lst, que se utiliza para vulnerar las seguridades inalámbricas mediante "Fuerza Bruta".

X

- **XOR:** es una compuerta lógica que realiza la función booleana: A'B+AB

REFERENCIAS DE INTERNET

- Sitio Web de la Enciclopedia Libre Wikipedia en Español: http://es.wikipedia.org/
- Sitio Web de Microsoft: http://www.microsoft.com/
- Sitio Web de Wireless LANs: http://www.wirelesslans.org/
- Sitio Web de Seguridad en Redes: http://seguridadenredes.blogspot.com/
- Sitio web Wi-Fi Alliance: http://www.wi-fi.org
- Sitio web Institute of Electrical and Electronics Engineers: http://www.ieee.org
- Sitio web Normas de la IEEE: http://www.ieee802.org/11/
- Sitio web de la empresa Cisco – España que muestra la manera de proteger una red:
- http://www.cisco.com/web/ES/solutions/smb/products/security/security_primer.html
- Sitio web de la empresa Linksys – España que muestra las bondades de las herramientas de la empresa Linksys para proteger una red: http://www.linksysbycisco.com/EU/es/home
- Sitio web de la empresa D-Link: http://www.dlinkla.com/home/

- BORISOV, Nikita. GOLDBERG, Ian. WAGNER, David. Trabajo pionero en vulnerabilidades de WEP: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

- Comunidad Aircrack en Español sobre Seguridad Wireless: http://www.aircrack.es/

- Sitio web Suite Aircrack-ng: http://www.aircrack-ng.org/

- Sitio web TamoSoft: http://www.tamos.com/products/commwifi/

- Sitio web WiFiCripter: http://wificripter.blogspot.com/

- Páginas para descargar Wordlist:

  http://www.edadfutura.com/wordlist-diccionarios-para-crackear-wpa/
  http://www.outpost9.com/files/WordLists.html
  http://outworld.es/spdic.gz
  http://comunidad.dragonjar.org/f182/diccionarios-para-wpa-9835/
  http://www.gratistaringa.net/f131/diccionario-227-millones-de-palabras-wpa-wpa2-wifi-multilenguaje-4shared-1476636/
  http://www.zonadd.net/viewtopic.php?t=4433

  http://www.taringa.net/posts/linux/5687920/Diccionarios-completos-WPA_WPA2-Backtrack-4-WPA-CRACKER.html

  http://www.taringa.net/posts/downloads/9348095/Mega-Diccionario-para-WPA_WPA2-227-millones-de-palabras-2Gb.html

BIBLIOGRAFÍA

- ANDREU/PELLEJERO/LESTA**. Redes WLAN: Fundamentos y aplicaciones de seguridad.** Marcombo S.A.. 2006

- BARKEN, Lee. **Wireless Hacking**. Syngress. 2004

- CISCO SYSTEMS. **Fundamentos de redes inalámbricas**. Prentice Hall. 2006

- EDNEY, Jon; ARBAUGH, William. **Real 802.11 Security: Wi-Fi Protected Access and 802.11i.** Addison Wesley. 2004

- FLECK, Bob; POTTER, Bruce. **802.11 Security.** O'Reilly. 2002

- FLICKENGER, Rob. **Wireless Hacks.** O'Reilly. 2005

- GAST, Matthew. **802.11 Wireless Network.** O'Reilly. 2005

- HUIDOBRO, José;ROLDAN, David. **Comunicación en redes WLAN**. 2005

- LUCDENA, Manuel José. **Criptografía y seguridad en computadores**. 1999

- MILLER, Michael. Windows Vista. **Redes Inalámbricas**. Anaya Multimedia. 2008

- PANDA SOFTWARE INTERNACIONAL. **Seguridad de Redes Inalámbricas**. 2005

- MILLER, Stewart S. **Seguridad en WIFI**. McGraw Hill. 2004

- TANENBAUM, Andrew S. **Redes de Computadoras**. Prentice Hall. 1997

- VLADIMIROV, Andrew. **Hacking Wireless: Seguridad en redes inalámbricas.** Anaya Multimedia. 2004

ANEXOS

ANEXOS 1

Figuras

ANEXOS 2

Cuadros

ANEXOS 3

Empresas

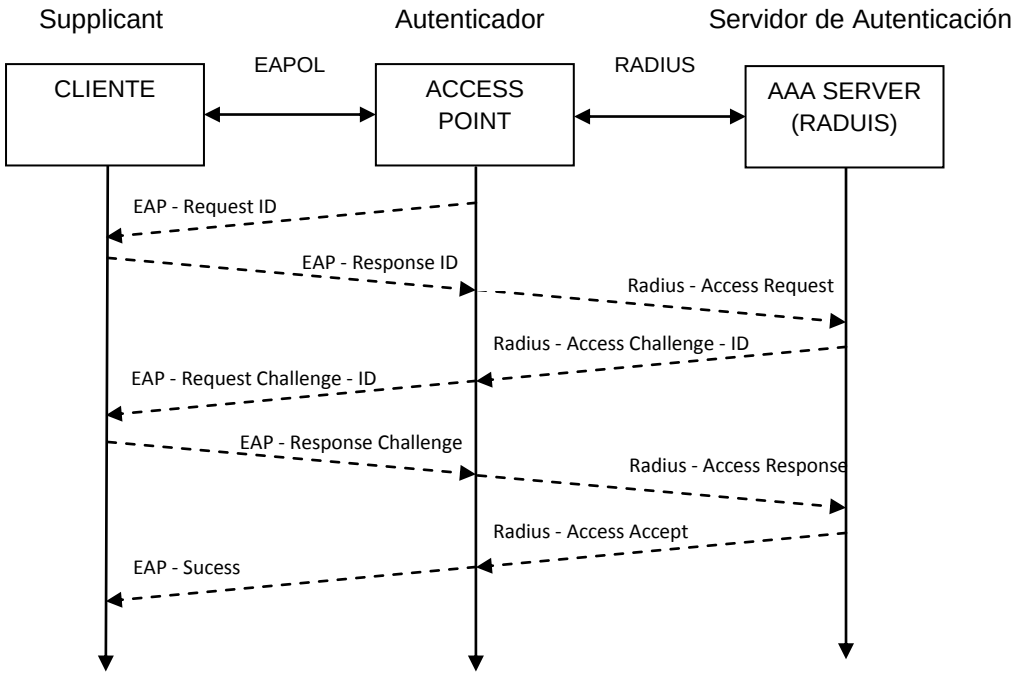
ANEXOS 4

Capturas

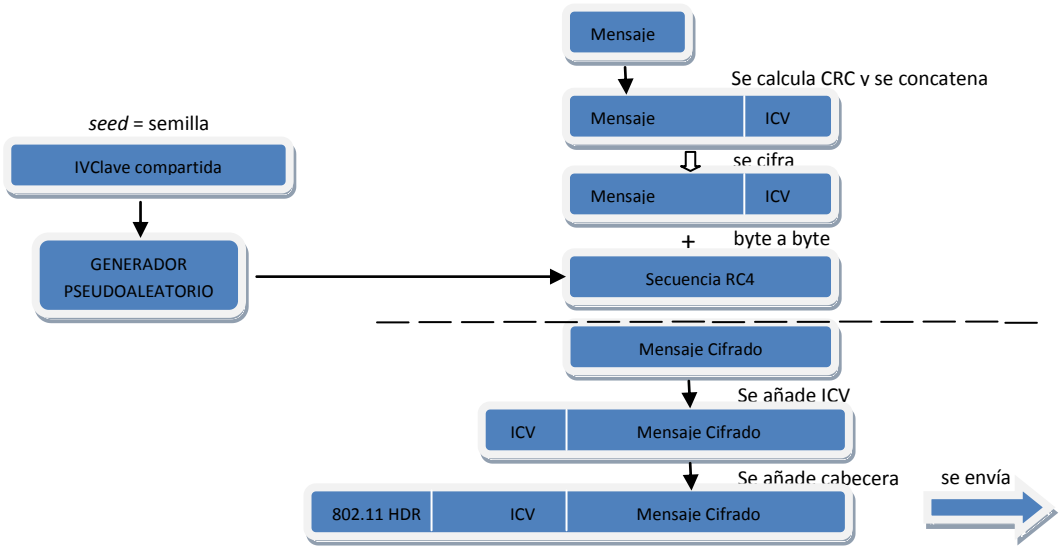
ANEXOS 1

Autor: Andrés Serrano Flores

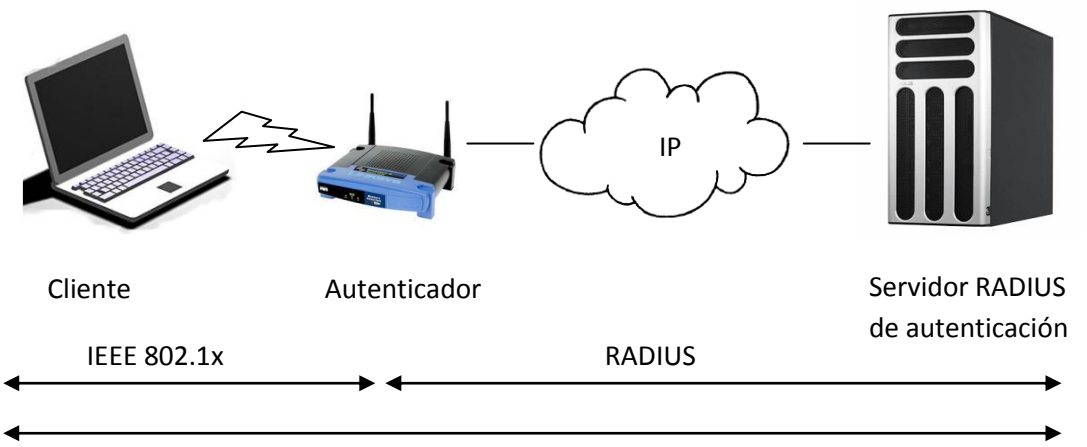
Autenticación EAP



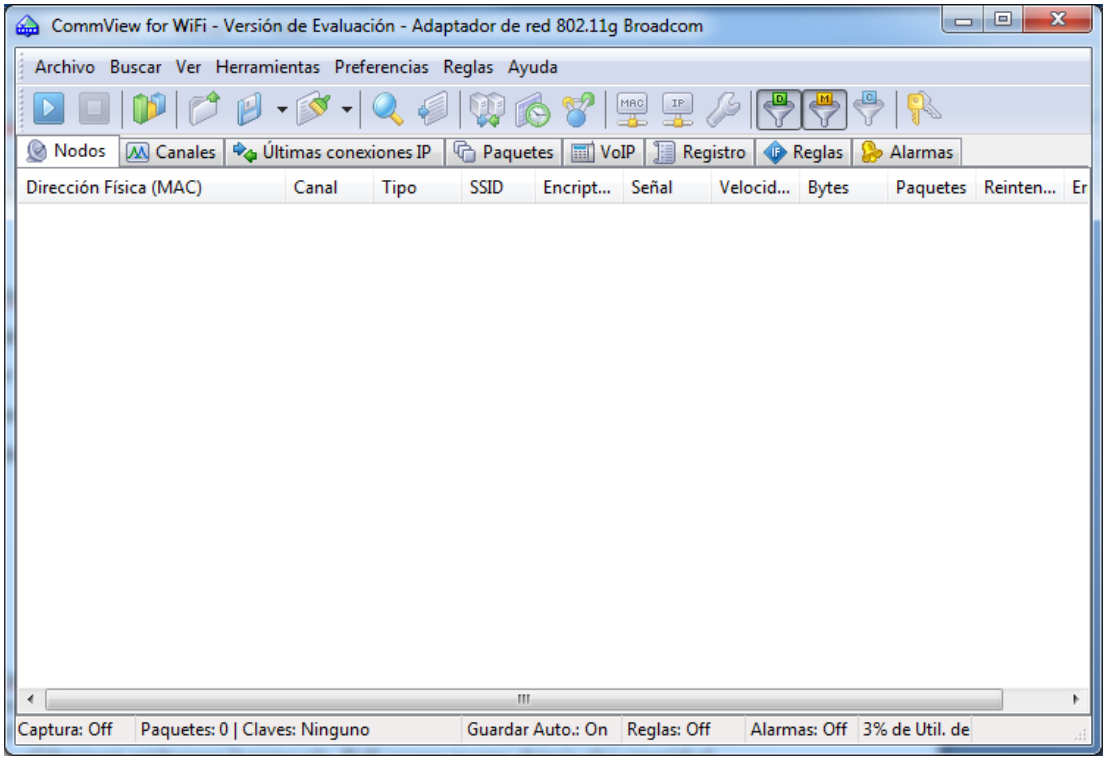
Cifrado WEP



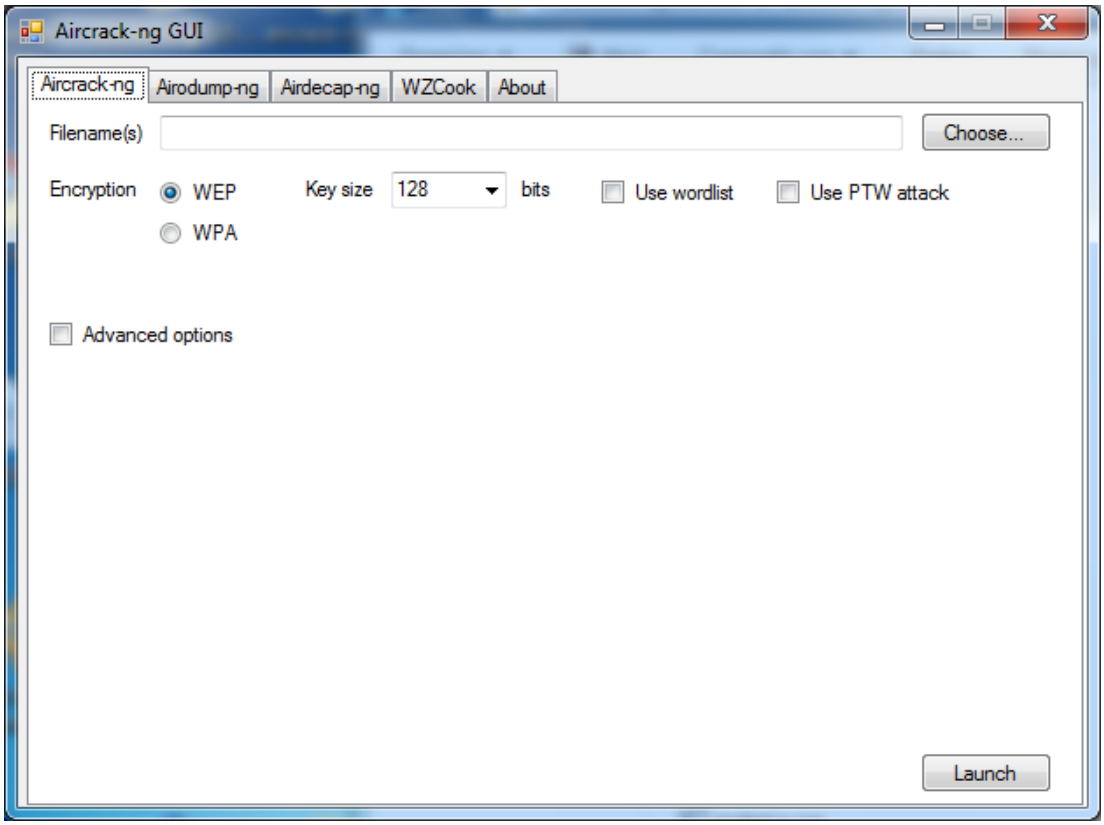
Arquitectura 802.1x/EAP



CommView for WiFi



Aircrack-ng en modo GUI



ANEXOS 2

Autor: Andrés Serrano Flores

Cuadro Comparativo: Principales Estándares 802.11

Protocolo	Año publicación	Frecuencia	Velocidad transmisión	Velocidad transmisión (Max)	Rango (interno)
802.11	1997	2.4-2.5 GHz	1 Mbit/s	2 Mbit/s	?
a	1999	5.15-5.35/5.47-7.725/5.725-5.875 GHz	25 Mbit/s	54 Mbit/s	30 m
b	1999	2.4-2.5 GHz	6.5 Mbit/s	11 Mbit/s	30 m
g	2003	2.4-2.5 GHz	25 Mbit/s	54 Mbit/s	30 m
n	2008	2.4 GHz o 5 GHz	200 Mbit/s	540 Mbit/s	50 m

Cuadro Comparativo: Nivel de Soluciones 802.1X/EAP

	EAP-MD5	LEAP (Cisco)	EAP-TLS (MS)	EAP-TTLS (Funk)	EAP-PEAP
Solución de seguridad	Estándar	Patente	Estándar	Estándar	Estándar
Certificados - Cliente	No	N/A	Sí	No (Opcional)	No (Opcional)
Certificados - Servidor	No	N/A	Sí	Sí	Sí
Credenciales de Seguridad	Ninguna	Deficiente	Buena	Buena	Buena
Soporta Autentificación de Base de Datos	Requiere borrar la base de datos	Active Directory, NT Domains	Active Directory	Active Directory, NT Domains, Token Systems, SQL, LDAP	Active Directory
Intercambio de llaves dinámicas	No	Sí	Sí	Sí	Sí
Autentificación Mutua	No	Sí	Sí	Sí	Sí

Tabla de verdad: Puerta XOR

Entrada A	Entrada B	Salida A ⊕ B
0	0	0
0	1	1
1	0	1
0	0	0

Tabla Comparativa: WPA vs WPA2

	WPA	**WPA2**
Modo Enterprise	Autentificación: 802.1x / EAP	Autentificación: 802.1x / EAP
	Encriptación: TKIP /MIC	Encriptación: AES-COMP
Modo Personal	Autentificación: PSK	Autentificación: PSK
	Encriptación: TKIP /MIC	Encriptación: AES-COMP

Opciones Airodump-ng

Opción	Descripción
BSSID	Dirección MAC del punto de acceso
PWR	Nivel de señal reportado por la tarjeta. Su significado depende del controlador, pero conforme se acerca al punto de acceso o a la estación la señal aumenta. Si PWR==-1, el controlador no soporta reportar el nivel de señal.
Beacons	Número de paquetes-anuncio enviados por el AP. Cada punto de acceso envía unos diez Beacons por segundo al ritmo (rate) mínimo (1M), por lo que normalmente pueden ser recogidos desde muy lejos.
# Data	Número de paquetes de datos capturados (si es WEP, sólo cuenta IVs), incluyendo

	paquetes de datos de difusión general.
CH	Número de canal (obtenido de los paquetes beacon). Nota: algunas veces se capturan paquetes de datos de otros canales aunque no se esté alternando entre canales debido a las interferencias de radiofrecuencia.
MB	Velocidad máxima soportada por el AP. Si MB=11, entonces se trata de 802.11bm si MB=22 entonces es 802.11b+ y velocidades mayores son 802.11g. El punto (después de 54) indica que short preamble está soportado.
ENC	Algoritmo de encriptación en uso. OPN=sin encriptación, "WEP"?=WEP o mayor (no hay suficiente datos para distinguir entre WEP y WPA), WEP (sin la interrogación) indica WEP estática o dinámica, y WPA si TKIP o CCMP están presentes.
ESSID	Conocida como "SSID", puede estar vacía si el ocultamiento de SSID está activo. En este caso airodump tratará de recuperar el SSID de las respuestas a escaneos y las peticiones de asociación.
STATION	Dirección MAC de cada estación asociada.

Opciones Airdecap-ng

Opción	Parámetro	Descripción
-l		No elimina la cabecera del 802.11
-b	bssid	Filtro de dirección MAC del punto de acceso
-k	pmk	WPA Pairwise Master Key en hex
-e	essid	Identificador en ascii de la red escogida
-p	pass	Contraseña WPA de la red escogida
-w	key	Clave WEP de la red escogida en hex

Requerimientos de Hardware

EQUIPO	CARACTERÍSTICAS
Computador Portátil Hewlett-Packard  **Computador Portátil HP**	✓ HP Pavilion Entertainment PC Dv4t-1000 ✓ Procesador: Intel Core 2 Duo 2.53GHz ✓ Memoria RAM: 3GB ✓ Disco Duro: 300GB ✓ Tarjeta de red: 802.11g Broadcom (integrada) ✓ MAC: 00-21-00-5A-75-B9 ✓ Sistema Operativo: Windows 7 Professional de 32 bits
Tarjeta inalámbrica adicional  **Tarjeta USB Linksys**	✓ Linksys Compact Wireless-G USB Adapter ✓ Modelo: WUSB54GC ✓ Banda de Frecuencia: 2.4GHz ✓ MAC: 00-18-39-12-52-86

Router de la empresa Elecdor S.A.

EQUIPO	CARACTERÍSTICAS
Wireless Router / Access Point  **Router Linksys WRT54G**	✓ Router Linksys Wireless-G WRT54G ✓ Estándares: IEEE 802.3, IEEE 802.3u, IEEE 802.11g, IEEE 802.11b ✓ Banda de Frecuencia: 2.4GHz ✓ Velocidad: 54Mbps (Wireless), 10/100 Mbps (Ethernet) ✓ Tipo de puertos: 4 LAN RJ45, 1 WAN RJ45 ✓ MAC: 00-1C-10-A8-BB-D0 ✓ SSID: ElecdorLinksys

Router de la empresa EN CAJAS

Wireless Router / Access Point  **Router D-Link DIR-280**	✓ Wireless Router D-Link DIR-280 ✓ Firewall avanzado y control parental. Seguridad avanzada ✓ Estándares: IEEE 802.11g, compatible con IEEE 802.11b ✓ Banda de Frecuencia: 2.4GHz ✓ Velocidad: 54Mbps (Wireless), 10/100 Mbps (Ethernet) ✓ Tipo de puertos: 4 LAN RJ45, 1 WAN RJ45 ✓ Soporta VPN passthrough. Soporta encriptación WEP. WPA, WPA2 ✓ MAC: 00:21:91:4D:CA:CC ✓ SSID: EnCajas

Cuadro Resumen Ataques de Red

EMPRESA	TIEMPO DE ATAQUE	ATAQUE EFECTIVO	CONTRASEÑA DE SEGURIDAD
ELECDOR S.A.	6 horas	Si	elecdor001
ENCAJAS	8 horas	Si	enCajas1

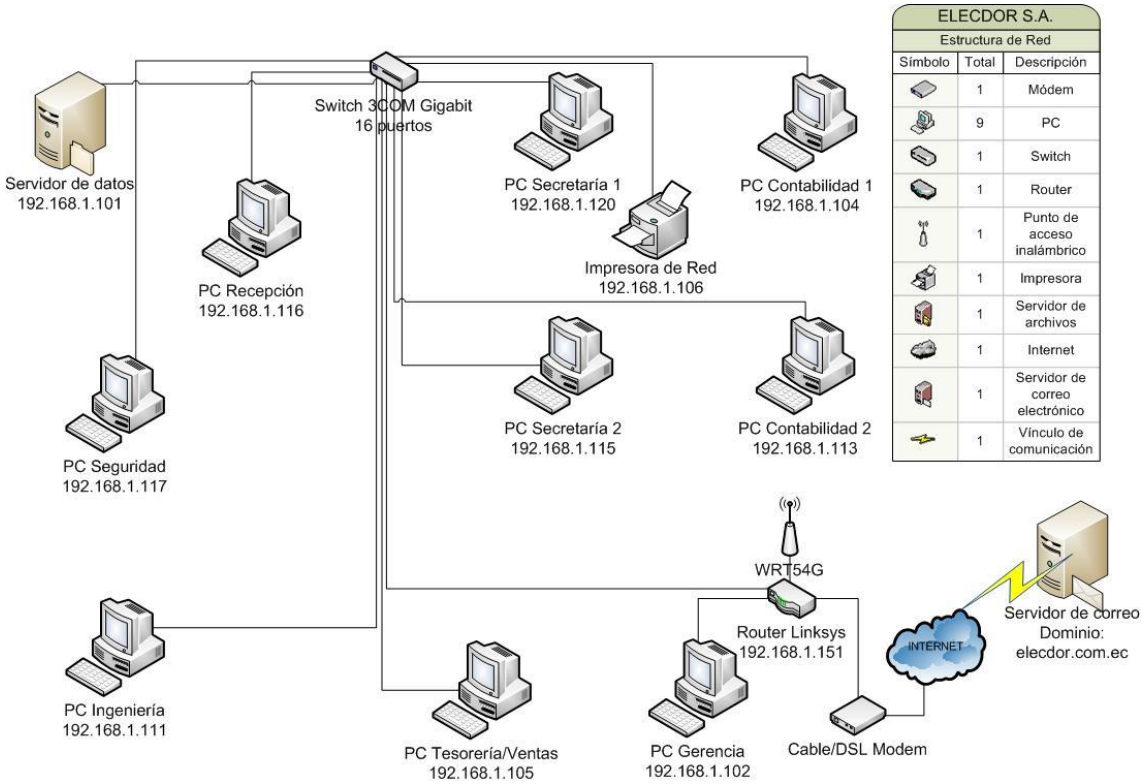
ANEXOS 3

Logo Elecdor S.A.

Fuente: Electrificaciones del Ecuador ELECDOR S.A.

Red estructurada Elecdor S.A.

Autor: Andrés Serrano Flores

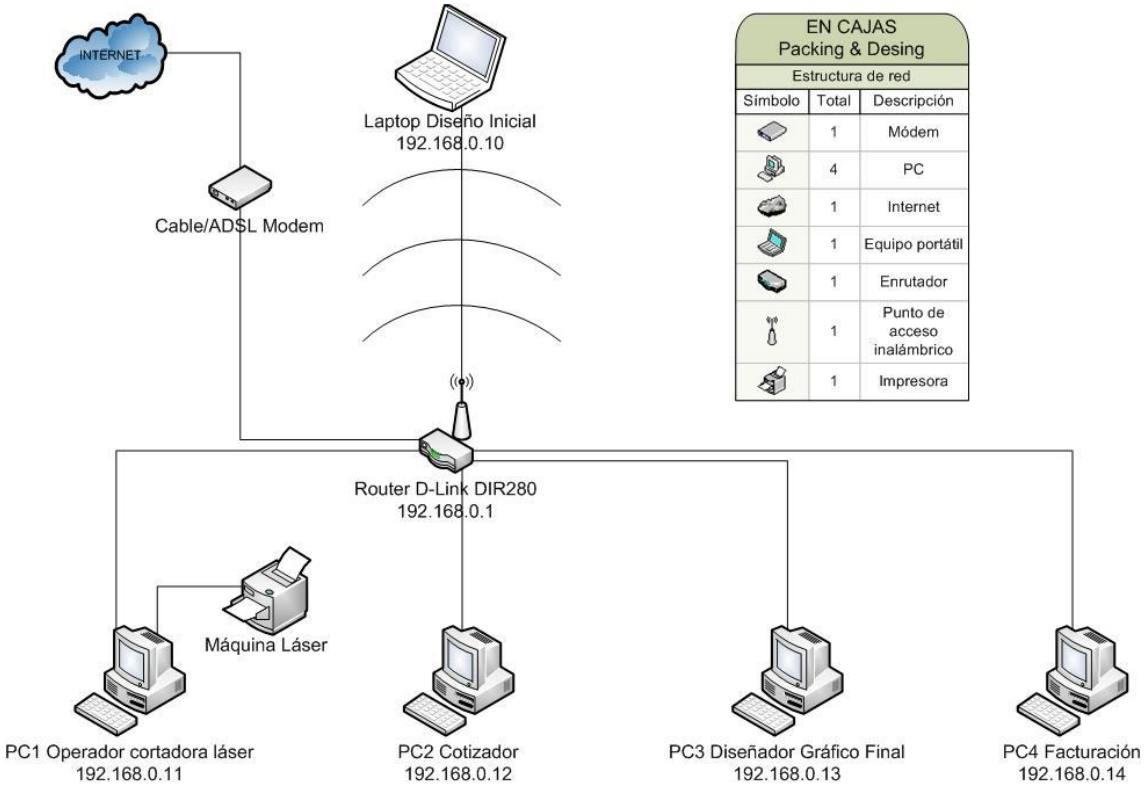


Logo EN CAJAS

Fuente: EN CAJAS

Red estructurada EN CAJAS

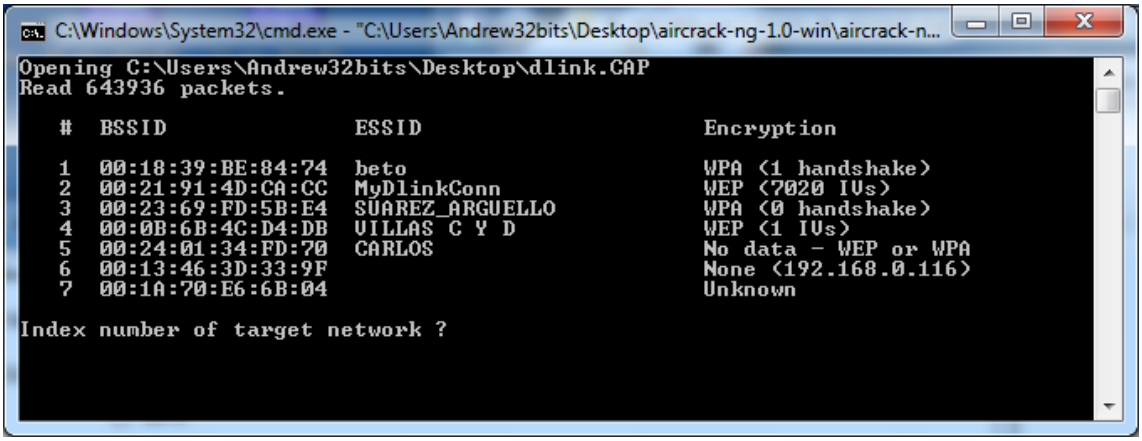
Autor: Andrés Serrano Flores



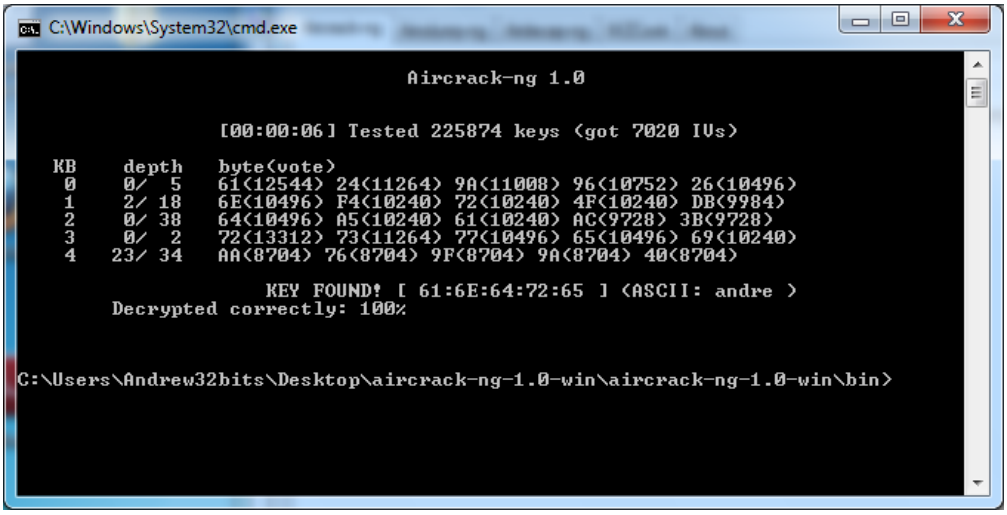
ANEXOS 4

Fuente: Software Aircrack-ng MS-DOS

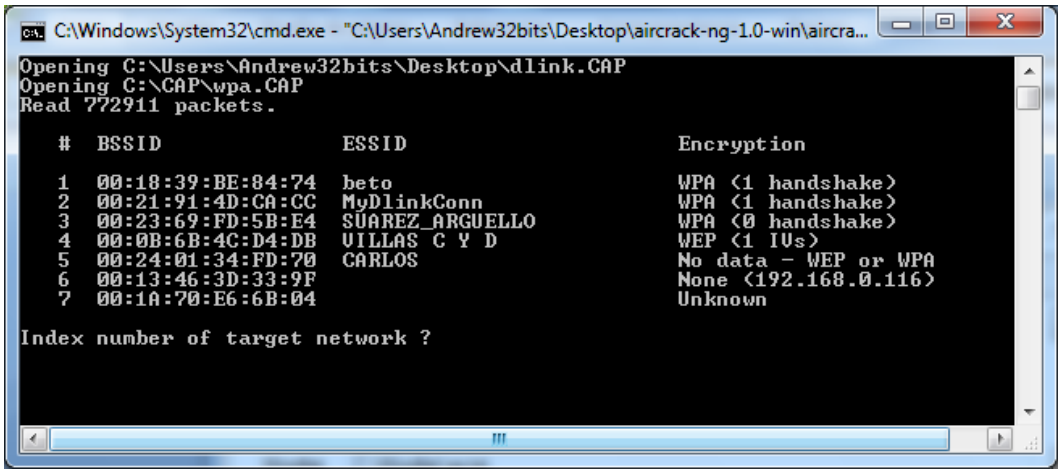
AP encontrados de la captura de registros .CAP



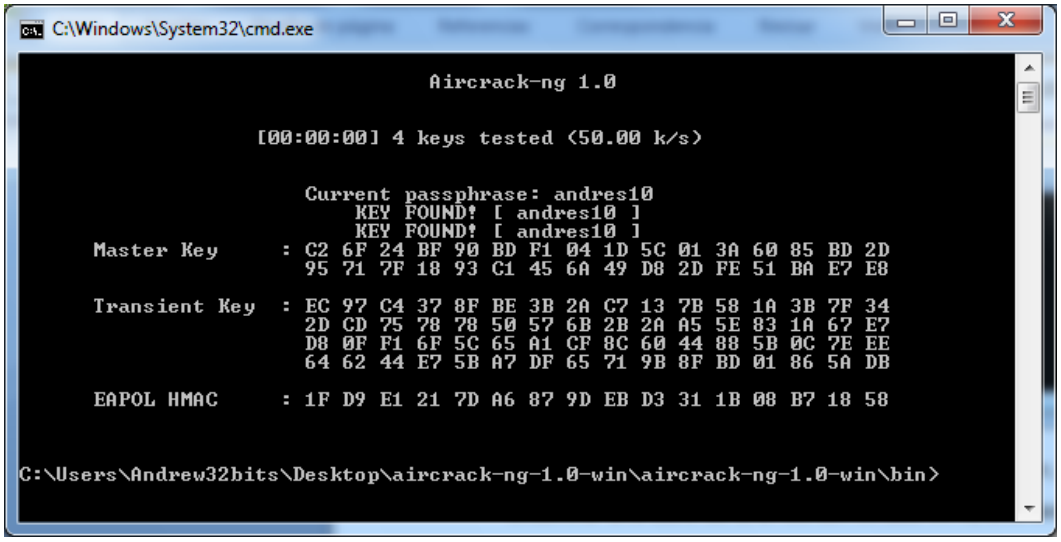
Clave encontrada de red con cifrado WEP



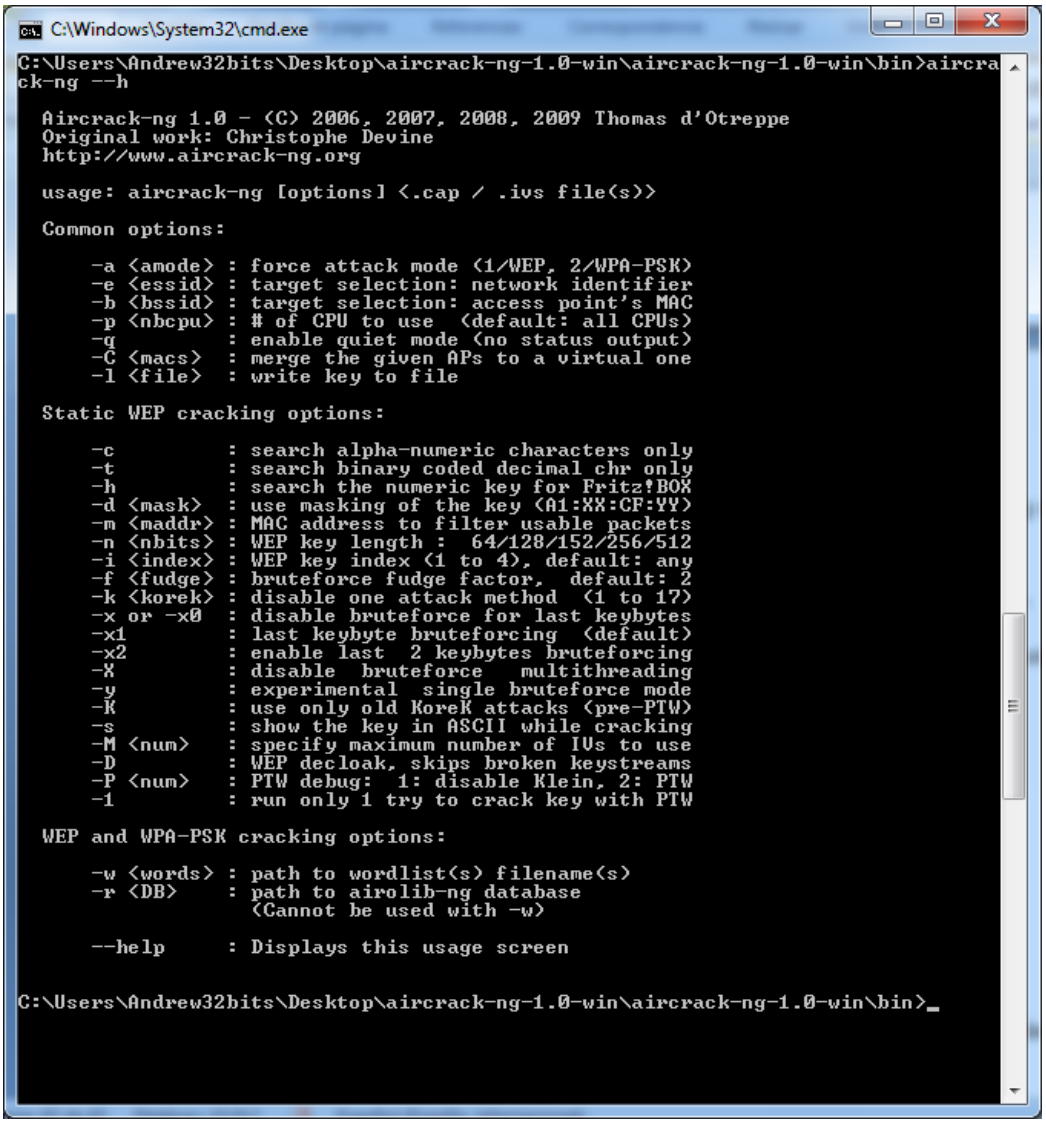
AP encontrados de la captura de registros .CAP



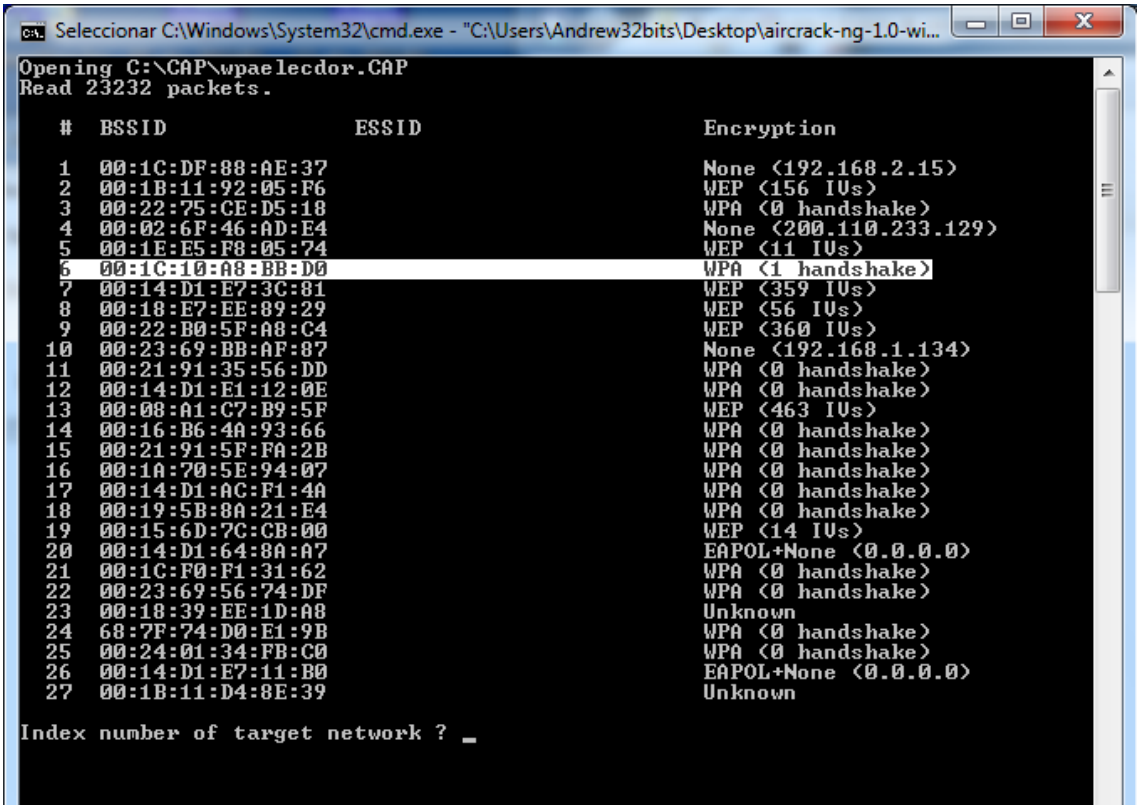
Clave encontrada de red con cifrado WPA



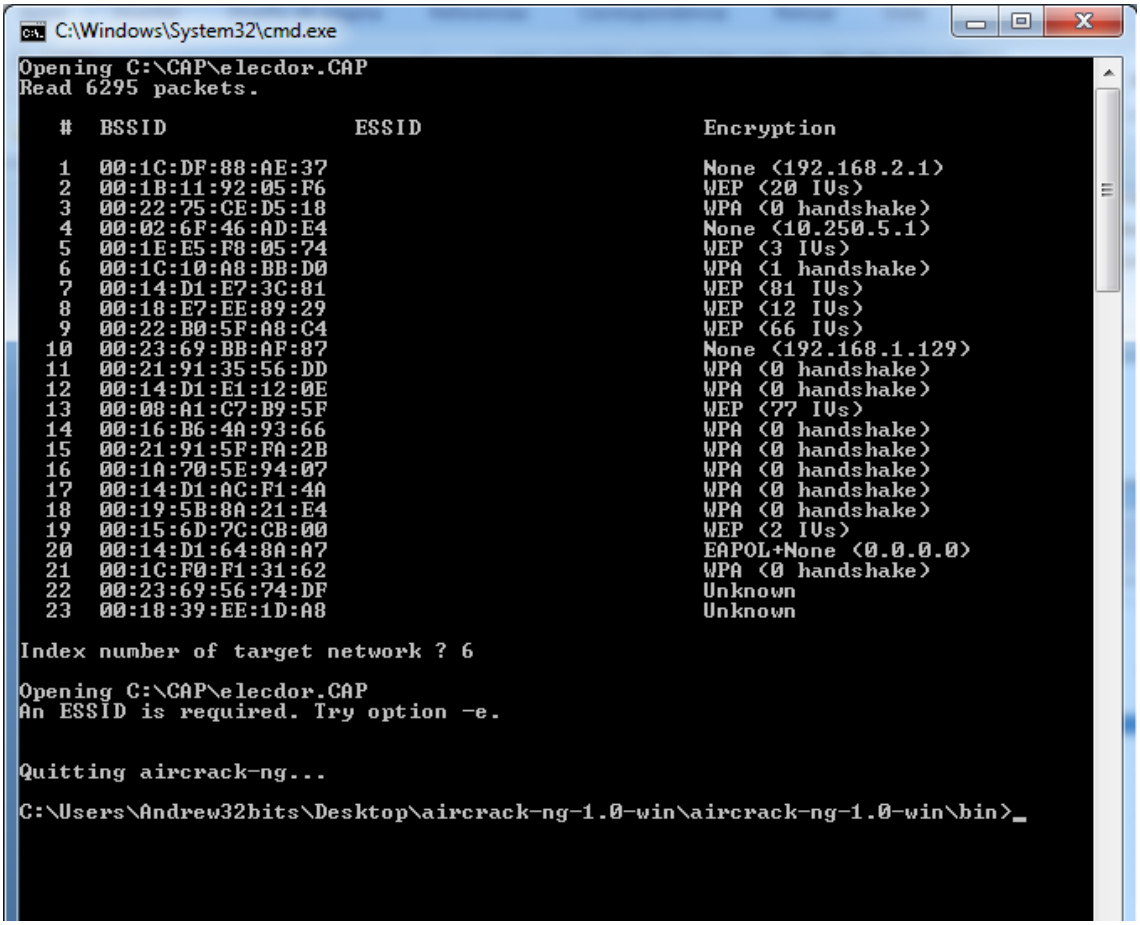
Opciones Aircrack-ng



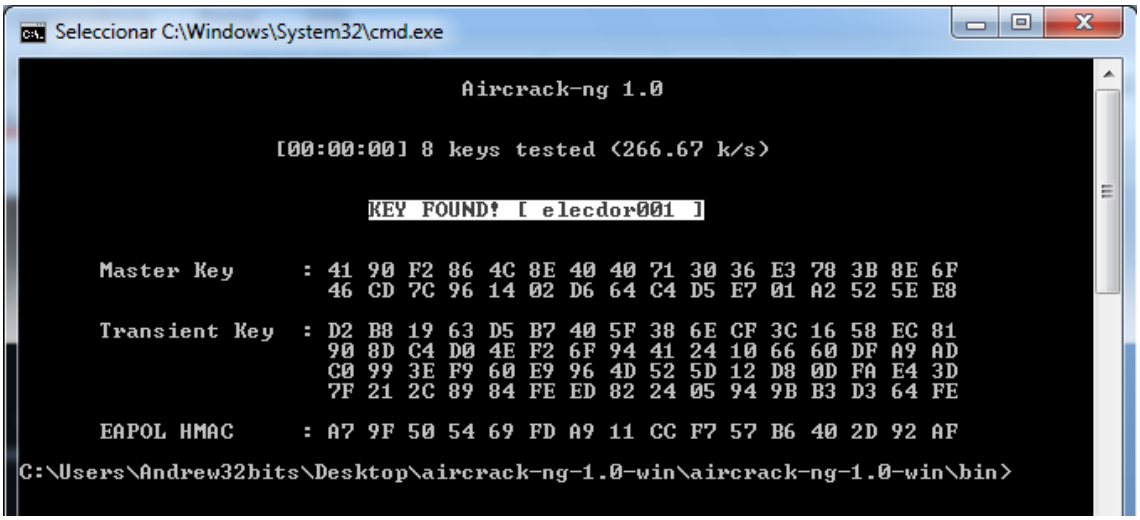
Información de las redes encontradas durante la captura de paquetes de datos Elecdor S.A.



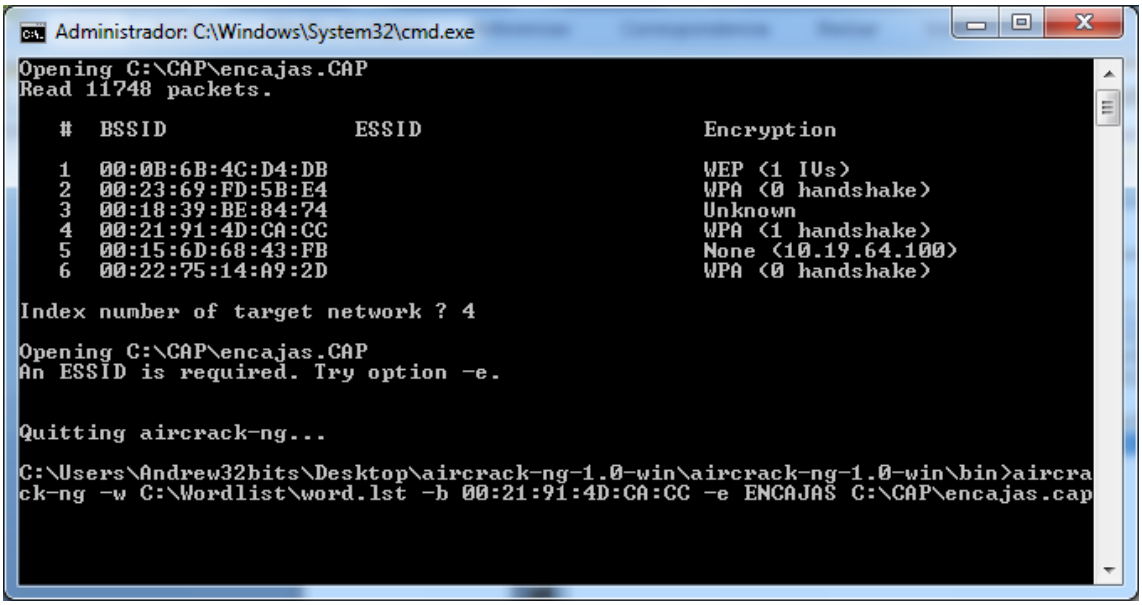
Selección de red a descifrar Elecdor S.A.



Clave encontrada de la red WiFi de Elecdor S.A.



Selección de red a descifrar EN CAJAS



Clave encontrada de la red WiFi de EN CAJAS